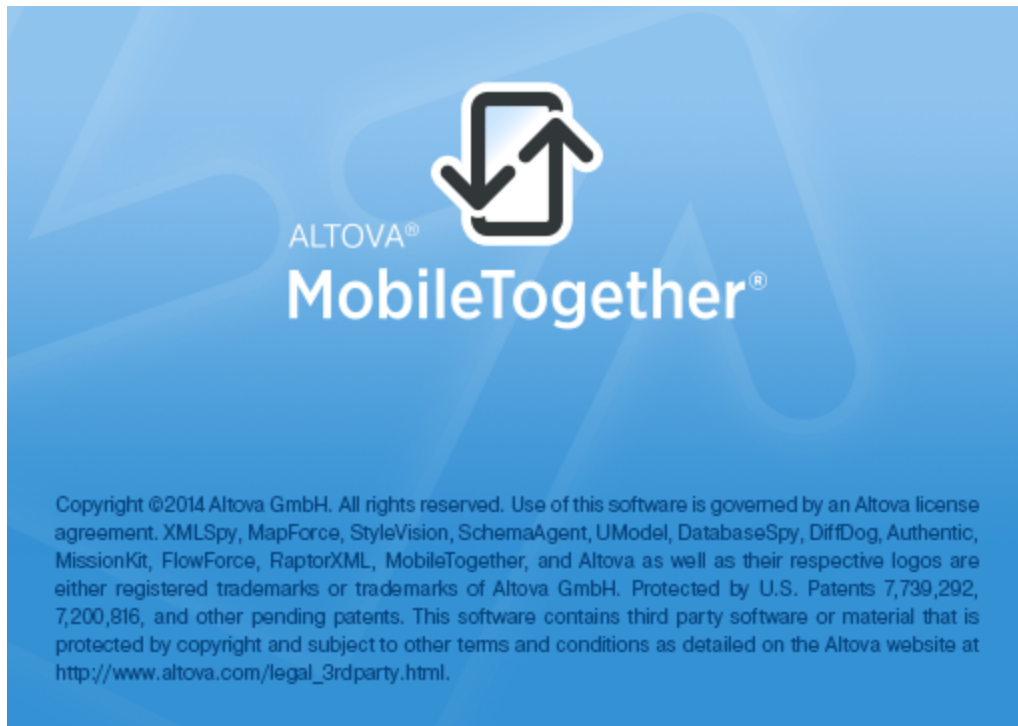


User and Reference Manual



Altova MobileTogether Server User & Reference Manual

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Published: 2014

© 2014 Altova GmbH

Table of Contents

1	Altova MobileTogether Server	3
2	Introduction	6
2.1	MobileTogether Overview	7
2.2	Using MobileTogether Server	9
3	Setting Up MobileTogether Server	12
3.1	Setup on Windows	13
3.1.1	Installation on Windows	14
3.1.2	Licensing on Windows	16
3.2	Setup on Linux	19
3.2.1	Installation on Linux	20
3.2.2	Licensing on Linux	23
3.2.3	Notes about Environment	26
3.3	Setup on Mac OS X	28
3.3.1	Installation on Mac OS X	29
3.3.2	Licensing on Mac OS X	32
3.3.3	Notes about Environment	34
3.4	Setting Up SSL Encryption	36
4	Server Procedures	42
4.1	Start Altova LicenseServer	43
4.2	Start MobileTogether Server	45
4.3	Set Up SSL Encryption	47
4.4	Set Administrator and Mobile Client Ports	52
4.5	Users and Roles	54
4.6	Available Privileges	56
4.7	Information for Clients	58
5	Web UI Reference	60

5.1	Workflows	62
5.2	Users and Roles	67
5.2.1	Users	70
5.2.2	Roles	74
5.2.3	Password Policies	77
5.2.4	Reports	79
5.3	User Licenses	80
5.4	Log	82
5.5	Cache	84
5.6	Settings	86

6 Altova LicenseServer 94

6.1	Network Information	96
6.2	Installation (Windows)	97
6.3	Installation (Linux)	98
6.4	Installation (Mac OS X)	100
6.5	Altova ServiceController	101
6.6	How to Assign Licenses	102
6.6.1	Start LicenseServer	103
6.6.2	Open LicenseServer's Config Page (Windows)	105
6.6.3	Open LicenseServer's Config Page (Linux)	108
6.6.4	Open LicenseServer's Config Page (Mac OS X)	111
6.6.5	Upload Licenses to LicenseServer	114
6.6.6	Register Product/s	118
	<i>Register FlowForce Server.....</i>	<i>119</i>
	<i>Register MapForce Server.....</i>	<i>124</i>
	<i>Register StyleVision Server.....</i>	<i>126</i>
	<i>Register RaptorXML(+XBRL) Server.....</i>	<i>128</i>
	<i>Register MobileTogether Server.....</i>	<i>130</i>
6.6.7	Assign Licenses to Registered Products	131
6.7	Configuration Page Reference	136
6.7.1	License Pool	137
6.7.2	Server Management	142
6.7.3	Server Monitoring	146
6.7.4	Settings	147
6.7.5	Messages, Log Out	151
6.8	Password Reset	152

Chapter 1

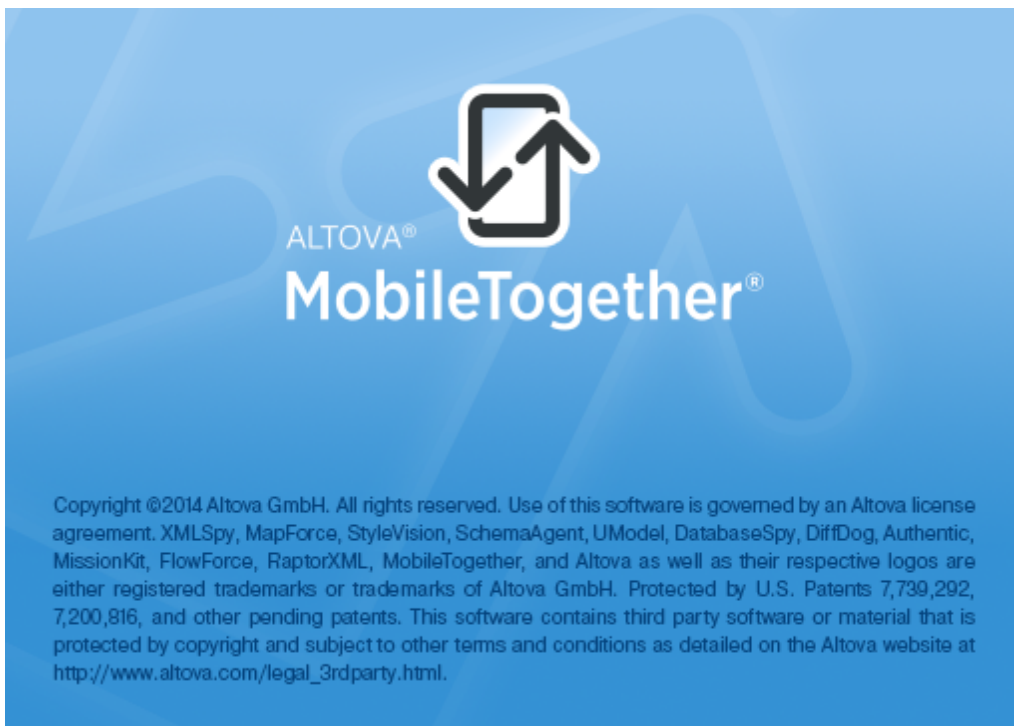
Altova MobileTogether Server

1 Altova MobileTogether Server

MobileTogether Server serves MobileTogether solutions to client mobile devices. It runs on MS Windows, Linux, and Mac OS X machines.

- MobileTogether solutions are created in Altova's MobileTogether Designer application and are deployed from MobileTogether Designer to MobileTogether Server.
- The MobileTogether Client app that is installed on client mobile devices then accesses MobileTogether solutions that are deployed on a MobileTogether Server.

MobileTogether Server has an easy-to-use Web UI that provides management of server processes and logs. This user manual describes how to set up MobileTogether Server and manage its processes.



This documentation

This documentation is organized into the following sections:

- [Introduction](#)
- [Setting Up MobileTogether Server](#)
- [Server Procedures](#)
- [Web UI Reference](#)
- [Altova LicenseServer](#)

Current version: 1.3

Last updated: 11-10-2014

Chapter 2

Introduction

2 Introduction

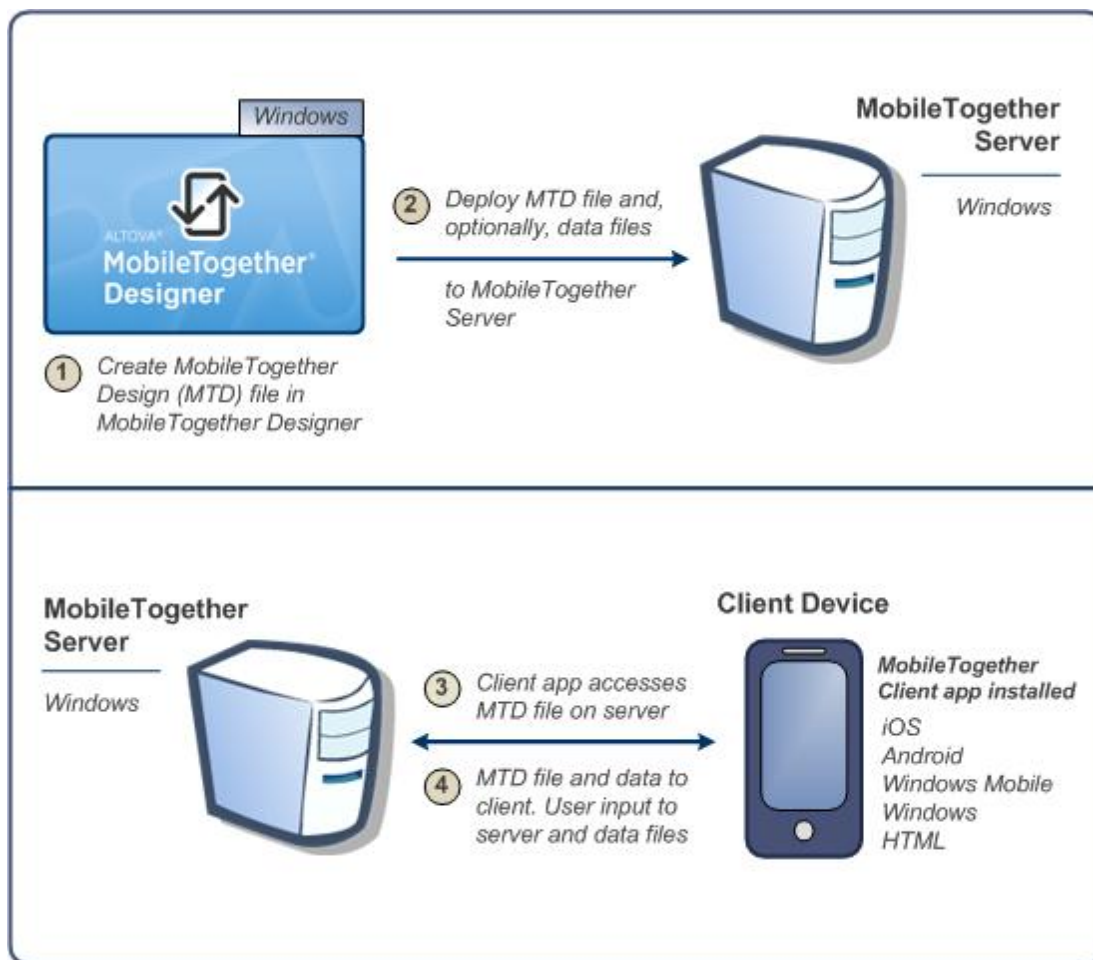
This introduction:

- [MobileTogether Overview](#), which describes the MobileTogether system and the place of MobileTogether Server within that system
- [Using MobileTogether Server](#) section, which lists the broad steps required to set up MobileTogether Server for use with MobileTogether Client apps

2.1 MobileTogether Overview

MobileTogether consists of the following modules:

- *MobileTogether Designer*. MobileTogether solutions for mobile clients are created and deployed to MobileTogether Server. See the [MobileTogether Designer user manual](#).
- *MobileTogether Server*. Serves MobileTogether solutions to MobileTogether Client apps installed on mobile devices. See the section, [Server Procedures](#), for descriptions of server administration tasks.
- *MobileTogether Client app (for mobile devices)*: Connects to a MobileTogether Server and accesses the MobileTogether solutions deployed on that server. See the [MobileTogether Client app user manual](#).



System requirements

▼ MobileTogether Designer

Windows	XP (SP2 for x64, SP3 for x86), Vista, 7, 8, or newer
Windows Server	2008 R2 or newer

▼ **MobileTogether Server**

Windows	XP (SP2 for x64, SP3 for x86), Vista, 7, 8, or newer
Windows Server	2008 R2 or newer
Linux	<ul style="list-style-type: none"> • CentOS 6 or newer • RedHat 6 or newer • Debian 6 or newer • Ubuntu 12.04 or newer
Mac OS X	10.7 or newer

▼ **MobileTogether Client**

iOS	iPhone, iPad
Android	Galaxy S, Nexus 7, Note 3, Sony Xperia U, and more
Windows Mobile	Windows Phone 8
Windows RT, Metro	For touch-enabled PCs and tablet computers
HTML	For any other mobile devices

2.2 Using MobileTogether Server

To set up MobileTogether Server for use with MobileTogether clients:

- Install and configure MobileTogether Server
 - Deploy MobileTogether solutions from MobileTogether Designer to MobileTogether Server
 - Configure MobileTogether Client apps (on mobile devices) to access solutions on a MobileTogether Server
-

The steps in more detail:

1. **Install MobileTogether Server**
MobileTogether Server runs on Windows, Linux, and Mac OS X systems. Before installing a new version of MobileTogether Server, de-install any previous version. See [Installation on Windows](#), [Installation on Linux](#), and [Installation on Mac OS X](#).
2. **License MobileTogether Server**
In order to license MobileTogether Server, it must be able to connect to a LicenseServer on your network. Start MobileTogether Server, register MobileTogether Server with LicenseServer, and assign a license to MobileTogether Server from LicenseServer. See [Licensing on Windows](#), [Licensing on Linux](#), and [Licensing on Mac OS X](#).
3. **Set up SSL encryption**
If you wish to encrypt server-client communication, you can set up SSL encryption for MobileTogether Server (see [Setting Up SSL Encryption](#)). Additionally, you will need to configure MobileTogether Client apps to communicate via SSL. See the [MobileTogether Client app user manual](#).
4. **Define basic settings**
Basic settings include [administrator and client ports](#), and other [communication settings and security settings](#).
5. **Set up user accounts**
MobileTogether Server is always accessed via a [user account](#), so user accounts have to be set up appropriately. There are two types of access:
 - *Administrator access:* Administrator access is via the Web UI and is used to carry out administrative tasks. Administrative actions include defining communication settings, security settings, and managing user accounts.
 - *End-user access:* End user access is via a mobile device and is used to download MobileTogether solutions to the client. Access to solutions on the server is determined by the user account the client logs in with.
6. **Deploy MobileTogether solutions to MobileTogether Server**

MobileTogether solutions are deployed from within the MobileTogether Designer application. See the [MobileTogether Designer user manual](#).

7. Configure MobileTogether Client apps to access MobileTogether Server
MobileTogether Client apps on mobile devices must be configured to connect to MobileTogether Server. The MobileTogether Server information that is required for configuring MobileTogether Client apps is listed in the section, [Information for Clients](#). Also see the [MobileTogether Client app user manual](#).

Chapter 3

Setting Up MobileTogether Server

3 **Setting Up MobileTogether Server**

This section describes installation, licensing and other setup procedures. It is organized into the following sections:

- [Installation on Windows](#)
- [Licensing on Windows](#)
- [Setup on Linux](#)
- [Setup on Mac OS X](#)
- [Setting Up SSL Encryption](#)

3.1 Setup on Windows

This section describes the [installation](#) and [licensing](#) of MobileTogether Server on Windows systems.

[Installation on Windows](#)

- [System requirements](#)
- [Installing MobileTogether Server](#)
- [Altova LicenseServer](#)
- [LicenseServer versions](#)
- [Trial license](#)
- [Application folder location](#)

[Licensing on Windows](#)

- [Start ServiceController](#)
- [Start LicenseServer](#)
- [Start MobileTogether Server](#)
- [Register MobileTogether Server](#)
- [Assign a license](#)

Installation on Windows

MobileTogether Server is available for installation on Windows systems. Its installation and setup procedure is described below.

▼ System requirements

▼ Windows

Windows XP (SP2 for x64; SP3 for x86), Windows Vista, Windows 7, Windows 8, or newer

▼ Windows Server

Windows Server 2008 R2 or newer

▼ Installing MobileTogether Server

MobileTogether Server can be installed on Windows systems as follows:

- As a separate standalone server product called MobileTogether Server. To install MobileTogether Server, download and run the MobileTogether Server installer. Follow the onscreen instructions.

The installers of both MobileTogether Server and [FlowForce Server](#) are available at the [Altova website](#) and will install the products with the necessary registrations. After installation, the MobileTogether Server executable will be located by default at:

```
<ProgramFilesFolder>\Altova\MobileTogetherServer1.3\bin  
\MobileTogetherServer.exe
```

▼ Altova LicenseServer

- In order for MobileTogether Server to work, it must be licensed via an [Altova LicenseServer](#) on your network.
- When you install MobileTogether Server on Windows systems, an option is available that allows you to download and install [Altova LicenseServer](#) together with MobileTogether Server.
- If an [Altova LicenseServer](#) is already installed on your network, you do not need to install another one—unless a newer version of [Altova LicenseServer](#) is required. (See *next point, LicenseServer versions*.)
- During the installation process of MobileTogether Server, check or uncheck the option for installing [Altova LicenseServer](#) as appropriate.

See the section, [Licensing on Windows](#), for more information about how to register and license MobileTogether Server with [Altova LicenseServer](#).

▼ LicenseServer versions

- Altova server products must be licensed either with the version of LicenseServer that is appropriate to the installed MobileTogether Server version, or with a later version of LicenseServer.
- The LicenseServer version that is appropriate for a particular version of MobileTogether Server is displayed during the installation of MobileTogether Server. You can install this version of LicenseServer along with MobileTogether Server, or you can install LicenseServer separately.
- Before installing a newer version of LicenseServer, any older one must be de-installed.

- The LicenseServer installer will do this automatically if it detects an older version.
- LicenseServer versions are backwards compatible. They will work with older versions of MobileTogether Server.
 - If you install a new version of MobileTogether Server and if your installed LicenseServer version is older than the appropriate LicenseServer, install the latest version available on the Altova website.
 - At the time of LicenseServer de-installation, all registration and licensing information held in the older version of LicenseServer will be saved to a database on your server machine. This data will be imported automatically into the newer version when the newer version is installed.
 - The version number of the currently installed LicenseServer is given at the bottom of the [LicenseServer configuration page](#) (all tabs).

Current version: 1.13

▼ Trial license

During the installation process, you will be given the option of requesting a 30-day trial license for MobileTogether Server. After submitting the request, a trial license will be sent to the email address you registered.

▼ Application folder location

The application will be installed in the following folder:

Windows XP	C:\Program Files\Altova\
Windows Vista, Windows 7/8	C:\Program Files\Altova\
32 bit Version on 64-bit OS	C:\Program Files (x86)\Altova\

Licensing on Windows

MobileTogether Server must be licensed with an Altova LicenseServer in order to run it. Licensing is a two-step process:

1. **Register MobileTogether Server** with LicenseServer. Registration is done from MobileTogether Server.
2. **Assign a license** to MobileTogether Server. License-assigning is done from LicenseServer.

The steps you need to carry out are given below.

▼ Start ServiceController

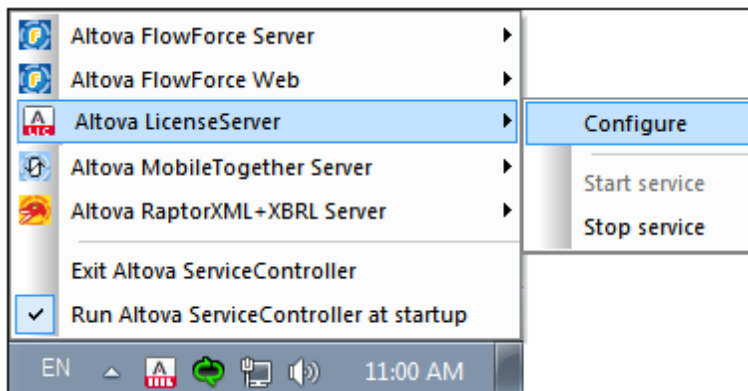
Altova ServiceController is started in order to start Altova LicenseServer and Altova MobileTogether Server.

Altova ServiceController (ServiceController for short) is an application for conveniently starting, stopping and configuring Altova services **on Windows systems**.

ServiceController is installed with Altova LicenseServer and with Altova server products that are installed as services (FlowForce Server, RaptorXML(+XBRL) Server, and Mobile Together Server). It can be started by clicking **Start | Altova LicenseServer | Altova ServiceController**. (This command is also available in the **Start** menu folders of Altova server products that are installed as services (FlowForce Server, RaptorXML(+XBRL) Server, and Mobile Together Server).) After ServiceController has been started, it can be accessed via the system tray (*screenshot below*).

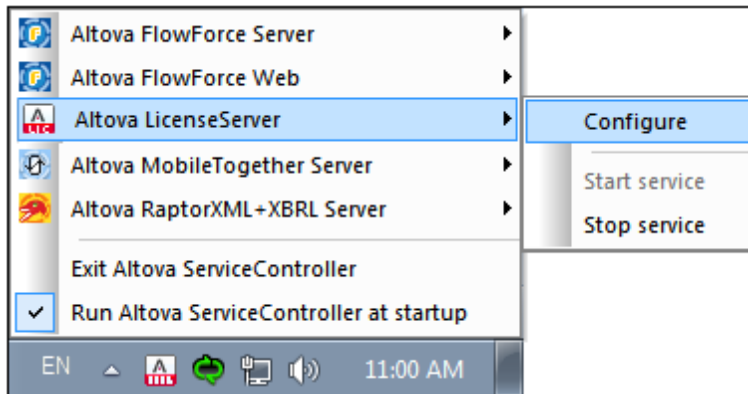


To specify that ServiceController starts automatically on logging in to the system, click the **ServiceController** icon in the system tray to display the **ServiceController** menu (*screenshot below*), and then toggle on the command **Run Altova ServiceController at Startup**. (This command is toggled on by default.) To exit ServiceController, click the **ServiceController** icon in the system tray and, in the menu that appears (*see screenshot below*), click **Exit Altova ServiceController**.



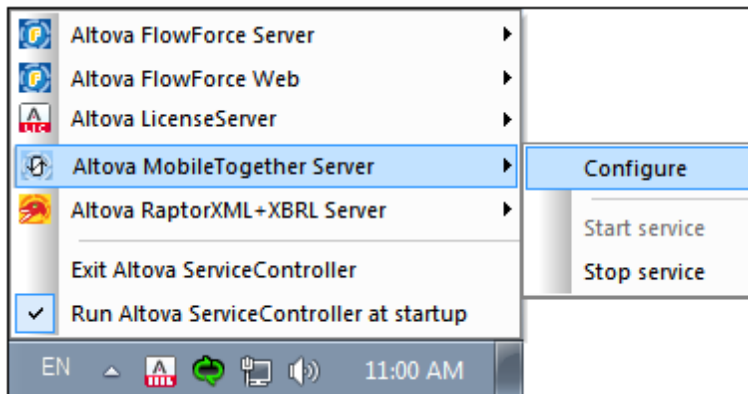
▼ Start LicenseServer

To start LicenseServer, click the **ServiceController** icon in the system tray, hover over **Altova LicenseServer** in the menu that pops up (see screenshot below), and then select **Start Service** from the LicenseServer submenu. If LicenseServer is already running, the *Start Service* option will be disabled.



▼ Start MobileTogether Server

To start MobileTogether Server, click the **ServiceController** icon in the system tray, hover over **Altova MobileTogether Server** in the menu that pops up (see screenshot below), and then select **Start Service** from the MobileTogether Server submenu. If MobileTogether Server is already running, the *Start Service* option will be disabled.



▼ Register MobileTogether Server

▣ *Register MobileTogether Server through FlowForce Server*

If MobileTogether Server was installed as part of a [FlowForce Server](#) installation, registering FlowForce Server with LicenseServer will automatically also register MobileTogether Server. How to register FlowForce Server is described in the [FlowForce Server documentation](#). Essentially: (i) Start Altova FlowForce Web as a service via ServiceController (see *previous point*); (ii) Enter your password to access the Setup page; (iii) Select the LicenseServer name or address and click **Register with LicenseServer**.

After successful registration, go to the [Server Management tab of LicenseServer's configuration page](#) to assign a license to MobileTogether Server.

☐ *Register a standalone MobileTogether Server*

Register MobileTogether Server via:

- its CLI, using the `licenseserver` command:

```
MobileTogetherServer licenseserver [options] ServerName-Or-IP-Address
```

For example, if `localhost` is the name of the server on which LicenseServer is installed:

```
MobileTogetherServer licenseserver localhost
```

- [the Settings tab of MobileTogether Server's Web UI](#). Essentially: (i) Start MobileTogether Server via ServiceController (see *previous point*); (ii) Enter your password to access the Setup page; (iii) Select the LicenseServer name or address, and click **Register with LicenseServer**.

After successful registration, go to the [Server Management tab of LicenseServer's configuration page](#) to assign a license to MobileTogether Server.

▼ Assign a license

After successfully registering MobileTogether Server, it will be listed in the [Server Management tab](#) of the configuration page of LicenseServer. Go [there](#) and [assign a license](#) to MobileTogether Server.

Note on cores and licenses

The licensing of Altova server products, *except MobileTogether Server*^{***}, is based on the number of processor cores available on the product machine. For example, a dual-core processor has two cores, a quad-core processor four cores, a hexa-core processor six cores, and so on. The number of cores licensed for a product on a particular server machine must be greater than or equal to the number of cores available on that server, whether it's a physical or virtual machine.

For example, if a server has eight cores (an octa-core processor), you must purchase at least an 8-core license. You can also combine licenses to achieve the core count. So, two 4-core licenses can also be used for an octa-core server instead of an 8-core license.

If you are using a computer server with a large number of CPU cores but only have a low volume to process, you may also create a virtual machine that is allocated a smaller number of cores, and purchase a license for that number. Such a deployment, of course, will have less processing speed than if all available cores on the server were utilized.

Note: Each license can be used for only one client machine at a time, even if it has unused licensing capacity. For example, if a 10-core license is used for a client machine that has 6 CPU cores, then the remaining 4 cores of the license cannot be used simultaneously for another client machine.

^{***} MobileTogether Server licenses are assigned on the basis of the number of users, that is, the number of client devices that connect to MobileTogether Server.

3.2 Setup on Linux

This section describes the [installation](#) and [licensing](#) of MobileTogether Server on Linux systems (Debian, Ubuntu, CentOS, RedHat).

[Installation on Linux](#)

- [System requirements](#)
- [Uninstall old versions of Altova server products](#)
- [Download the Linux package](#)
- [Install MobileTogether Server](#)
- [Altova LicenseServer](#)
- [LicenseServer versions](#)
- [Trial license](#)

[Licensing on Linux](#)

- [Start LicenseServer](#)
- [Start MobileTogether Server](#)
- [Register MobileTogether Server](#)
- [Assign a license](#)

[Notes about Environment](#)

Installation on Linux

MobileTogether Server is available for installation on Linux systems. Its installation and setup procedure is described below.

▼ System requirements

▼ *Linux*

- CentOS 6 or newer
- RedHat 6 or newer
- Debian 6 or newer
- Ubuntu 12.04 or newer

▼ FlowForce Server integration

If you are installing MobileTogether Server together with FlowForce Server, it is recommended to install FlowForce Server first. Otherwise, after having installed both MobileTogether Server and FlowForce Server, run the following command:

```
cp /opt/Altova/MobileTogetherServer1.3/etc/*.tool /opt/Altova/FlowForceServer2015/tools
```

This command copies the **.tool** file from **/etc** directory of MobileTogether Server to the FlowForce Server **/tools** directory. The **.tool** file is required by FlowForce Server; it contains the path to the MobileTogether Server executable. You do not need to run this command if you install FlowForce Server before installing MobileTogether Server.

▼ Uninstall old versions of Altova server products

If you need to uninstall a previous version, do this as follows. On the Linux command line interface (CLI), you can check which Altova server products are installed with the following command:

```
[Debian, Ubuntu]:  dpkg --get-selections | grep Altova
[CentOS, RedHat]:  rpm -qa | grep server
```

If MobileTogether Server is not installed, go ahead with the installation as documented below in *Installing MobileTogether Server*.

If MobileTogether Server is installed and you wish to install a newer version of MobileTogether Server, uninstall the old version with the command:

```
[Debian, Ubuntu]:  sudo dpkg --remove mobiletogetherserver
[CentOS, RedHat]:  sudo rpm -e mobiletogetherserver
```

If you need to uninstall an old version of Altova LicenseServer, do this with the following command:

```
[Debian, Ubuntu]:  sudo dpkg --remove licenseserver
[CentOS, RedHat]:  sudo rpm -e licenseserver
```

▼ Download the Linux package

MobileTogether Server installation packages for the following Linux systems are available on the [Altova website](#).

Distribution	Package extension
Debian 6 and higher	.deb
Ubuntu12.04 and higher	.deb
CentOS 6 and higher	.rpm
RedHat 6 and higher	.rpm

After downloading the Linux package, copy it to any directory on the Linux system. Since you will need an [Altova LicenseServer](#) in order to run MobileTogether Server, you may want to download LicenseServer from the [Altova website](#) at the same time as you download MobileTogether Server, rather than download it at a later time.

▼ Install MobileTogether Server

In a terminal window, switch to the directory where you have copied the Linux package. For example, if you copied it to a user directory called `MyAltova` (that is located, say, in the `/home/User` directory), then switch to this directory as follows:

```
cd /home/User/MyAltova
```

Install MobileTogether Server with the following command:

```
[Debian]:  sudo dpkg --install mobiletogetherserver-1.3-debian.deb
[Ubuntu]:  sudo dpkg --install mobiletogetherserver-1.3-ubuntu.deb
[CentOS]:  sudo rpm -ivh mobiletogetherserver-1.3-1.x86_64.rpm
[RedHat]:  sudo rpm -ivh mobiletogetherserver-1.3-1.x86_64.rpm
```

The MobileTogether Server package will be installed in the folder:

```
/opt/Altova/MobileTogetherServer1.3
```

▼ Altova LicenseServer

In order for any Altova Server product—including MobileTogether Server—to run, that server product must be licensed via an [Altova LicenseServer](#) on your network.

On Linux systems, [Altova LicenseServer](#) will need to be installed separately. Download LicenseServer from the [Altova website](#) and copy the package to any directory on the Linux system. Install it just like you installed MobileTogether Server (*see previous step*).

```
[Debian]:  sudo dpkg --install licenseserver-1.13-debian.deb
[Ubuntu]:  sudo dpkg --install licenseserver-1.13-ubuntu.deb
[CentOS]:  sudo rpm -ivh licenseserver-1.13-1.x86_64.rpm
[RedHat]:  sudo rpm -ivh licenseserver-1.13-1.x86_64.rpm
```

The LicenseServer package will be installed in:

```
/opt/Altova/LicenseServer
```

For information about how to register MobileTogether Server with [Altova LicenseServer](#) and license it, see the section, [Licensing on Linux](#).

▼ LicenseServer versions

- Altova server products must be licensed either with the version of LicenseServer that is appropriate to the installed MobileTogether Server version, or with a later version of LicenseServer.
- The LicenseServer version that is appropriate for a particular version of MobileTogether Server is displayed during the installation of MobileTogether Server. You can install this version of LicenseServer along with MobileTogether Server, or you can install LicenseServer separately.
- Before installing a newer version of LicenseServer, any older one must be de-installed. The LicenseServer installer will do this automatically if it detects an older version.
- LicenseServer versions are backwards compatible. They will work with older versions of MobileTogether Server.
- If you install a new version of MobileTogether Server and if your installed LicenseServer version is older than the appropriate LicenseServer, install the latest version available on the Altova website.
- At the time of LicenseServer de-installation, all registration and licensing information held in the older version of LicenseServer will be saved to a database on your server machine. This data will be imported automatically into the newer version when the newer version is installed.
- The version number of the currently installed LicenseServer is given at the bottom of the [LicenseServer configuration page](#) (all tabs).

Current version: 1.13

▼ Trial license

During the installation process, you will be given the option of requesting a 30-day trial license for MobileTogether Server. After submitting the request, a trial license will be sent to the email address you registered.

Licensing on Linux

MobileTogether Server must be licensed with an Altova LicenseServer in order to run it. Licensing is a two-step process:

1. **Register MobileTogether Server** with LicenseServer. Registration is done from MobileTogether Server.
2. **Assign a license** to MobileTogether Server. License-assigning is done from LicenseServer.

The steps you need to carry out are given below.

▼ Start LicenseServer

To correctly register and license MobileTogether Server with LicenseServer, LicenseServer must be running as a daemon on the network. Start LicenseServer as a daemon with the following command:

```
[Debian]:  sudo /etc/init.d/licenseserver start
[Ubuntu]:  sudo initctl start licenseserver
[CentOS]:  sudo initctl start licenseserver
[RedHat]:  sudo initctl start licenseserver
```

If at any time you need to stop LicenseServer, replace `start` with `stop` in the above command. For example:

```
sudo /etc/init.d/licenseserver stop
```

▼ Start MobileTogether Server

Start MobileTogether Server as a daemon with the following command:

```
[Debian]:  sudo /etc/init.d/mobiletogetherserver start
[Ubuntu]:  sudo initctl start mobiletogetherserver
[CentOS]:  sudo initctl start mobiletogetherserver
[RedHat]:  sudo initctl start mobiletogetherserver
```

When started for the first time, MobileTogether Server will start on a random port and open a Web UI (Setup) page.

If your web browser is on the same machine as MobileTogether Server, the URL of the Setup page is:

```
file:///var/opt/Altova/1.3/MobileTogetherweb.html
```

If your web browser is on a different machine than MobileTogether Server, extract the URL of the Setup page from the log file:

```
grep running /var/opt/Altova/1.3/data/mtweb.log
```

▼ Register MobileTogether Server

Register MobileTogether Server via:

- its CLI, using the `licenseserver` command:

```
sudo /opt/Altova/MobileTogetherServer1.3/bin/mobiletogetherserver
licenseserver [options] ServerName-Or-IP-Address
```

For example, if `localhost` is the name of the server on which LicenseServer is installed:

```
sudo /opt/Altova/MobileTogetherServer1.3/bin/mobiletogetherserver
licenseserver localhost
```

In the command above, `localhost` is the name of the server on which LicenseServer is installed. Notice also that the location of the MobileTogether Server executable is:

```
/opt/Altova/MobileTogetherServer1.3/bin/
```

- [the Settings tab of MobileTogether Server's Web UI](#). Essentially: (i) Start MobileTogether Server via ServiceController (see *previous point*); (ii) Enter your password to access the Setup page; (iii) Select the LicenseServer name or address, and click **Register with LicenseServer**.

After successful registration, go to the [Server Management tab of LicenseServer's configuration page](#) to assign a license to MobileTogether Server.

▼ Assign a license

After successfully registering MobileTogether Server, it will be listed in the [Server Management tab](#) of the configuration page of LicenseServer. Go [there](#) and [assign a license](#) to MobileTogether Server.

Note on cores and licenses

The licensing of Altova server products, *except MobileTogether Server*^{***}, is based on the number of processor cores available on the product machine. For example, a dual-core processor has two cores, a quad-core processor four cores, a hexa-core processor six cores, and so on. The number of cores licensed for a product on a particular server machine must be greater than or equal to the number of cores available on that server, whether it's a physical or virtual machine.

For example, if a server has eight cores (an octa-core processor), you must purchase at least an 8-core license. You can also combine licenses to achieve the core count. So, two 4-core licenses can also be used for an octa-core server instead of an 8-core license.

If you are using a computer server with a large number of CPU cores but only have a low volume to process, you may also create a virtual machine that is allocated a smaller number of cores, and purchase a license for that number. Such a deployment, of course, will have less processing speed than if all available cores on the server were utilized.

Note: Each license can be used for only one client machine at a time, even if it has unused licensing capacity. For example, if a 10-core license is used for a client machine that has 6 CPU cores, then the remaining 4 cores of the license cannot be used simultaneously for another client machine.

^{***} MobileTogether Server licenses are assigned on the basis of the number of users, that is, the number of client devices that connect to MobileTogether Server.

Notes about Environment

Folders

Given below is a list of important folders in your MobileTogether Server setup.

▣ *Installation root*

`/opt/Altova/MobileTogetherServer1.3/`

▣ *Database, License, and Solution Files*

`/var/opt/Altova/MobileTogetherServer`

▣ *Environment settings*

`/etc/profile.d/jdbc.sh`

The environment settings file must be defined according to your specific environment. The example path above serves only as a general guide.

Note: The environment settings file sets the variables for **all users** on the system.

File-based databases

File-based databases (such as SQLite databases) must reside in the folder defined in the Settings tab of MobileTogether Server as the [Server Side's Solutions Working Directory](#). By default, this folder is:

`/var/opt/Altova/MobileTogetherServer/SolutionFiles`

JDBC-Connections

Note the following points:

- The Java Runtime Environment or SDK must be installed.
- The JDBC-Connects for the target database must be installed.
- The following environment variables must be set correctly for your environment:
 - CLASSPATH: to find the jar-files
 - PATH: to find the JRE, but might not be necessary depending on the installation
 - JAVA_HOME: if necessary, depending on the installation.

Note

On Linux servers, the only database connections supported are JDBC.

Listing of important files

The following configuration files are copied to the folder `/opt/Altova/`

`MobileTogetherServer1.3/etc` so as not to overwrite already existing configuration files. Make

the necessary changes as required. The parts highlighted in blue are environment-specific and will need to be adjusted to match your environment:

Shell script

```
#- jdbc - environment -
export PATH=/usr/local/jdk1.7.0_17/bin:/usr/lib64/qt-3.3/bin:/usr/local/bin:/
bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/qa/bin
export JAVA_HOME=/usr/local/jdk1.7.0_17
export CLASSPATH=/usr/local/jdbc/oracle/ojdbc6.jar:/usr/local/jdbc/oracle/
xdb.jar:/usr/local/jdbc/oracle/xmlparserv2.jar:/usr/local/jdbc/postgre/
postgresql-9.0-801.jdbc4.jar:/usr/local/jdbc/mssql/sqljdbc4.jar:/usr/local/
jdbc/iseres/lib/jt400.jar:/usr/local/jdbc/mysql/mysql-connector-java-5.1.16-
bin.jar:/usr/local/jdbc/sqlite/sqlitejdbc-v056.jar:/usr/local/jdbc/
Informix_JDBC_Driver/lib/ifxjdbc.jar:/usr/local/jdbc/sybase/jconn7/
jconn4.jar:/usr/local/jdbc/db2/db2jcc.jar:/usr/local/jdbc/db2/
db2jcc_license_cu.jar:./:
```

Plist file

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>Label</key>
    <string>com.altova.MobileTogetherServer</string>
    <key>ProgramArguments</key>
    <array>
      <string>/usr/local/Altova/MobileTogetherServer1.3/bin/
MobileTogetherServer</string>
      <string>debug</string>
    </array>
    <key>KeepAlive</key>
    <true/>
    <key>UserName</key>
    <string>_altovamobiletogetherserver</string>
    <key>EnvironmentVariables</key>
    <dict>
      <key>CLASSPATH</key>
      <string>/usr/local/jdbc/oracle/ojdbc6.jar:/usr/local/jdbc/oracle/
xdb.jar:/usr/local/jdbc/oracle/xmlparserv2.jar:/usr/local/jdbc/postgre/
postgresql-9.0-801.jdbc4.jar:/usr/local/jdbc/mssql/sqljdbc4.jar:/usr/local/
jdbc/iseres/lib/jt400.jar:/usr/local/jdbc/mysql/mysql-connector-java-5.1.16-
bin.jar:/usr/local/jdbc/sqlite/sqlitejdbc-v056.jar:/usr/local/jdbc/
Informix_JDBC_Driver/lib/ifxjdbc.jar:/usr/local/jdbc/sybase/jconn7/
jconn4.jar:/usr/local/jdbc/db2/db2jcc.jar:/usr/local/jdbc/db2/
db2jcc_license_cu.jar:./</string>
    </dict>
  </dict>
</plist>
```

3.3 Setup on Mac OS X

This section describes the [installation](#) and [licensing](#) of MobileTogether Server on Mac OS X systems.

[Installation on Mac OS X](#)

- [System requirements](#)
- [Uninstall old versions of Altova server products](#)
- [Download the Mac OS X package](#)
- [Install MobileTogether Server](#)
- [Altova LicenseServer](#)
- [LicenseServer versions](#)
- [Trial license](#)

[Licensing on Mac OS X](#)

- [Start LicenseServer](#)
- [Start MobileTogether Server](#)
- [Register MobileTogether Server](#)
- [Assign a license](#)

[Notes about Environment](#)

Installation on Mac OS X

MobileTogether Server is available for installation on Linux systems. Its installation and setup procedure is described below.

- ▼ System requirements

- ▼ *Mac OS X*
 - Mac OS X 10.7 or newer

- ▼ FlowForce Server integration

If you are installing MobileTogether Server together with FlowForce Server, it is recommended to install FlowForce Server first. Otherwise, after having installed both MobileTogether Server and FlowForce Server, run the following command:

```
cp /usr/local/Altova/MobileTogetherServer1.3/etc/*.tool /usr/local/Altova/FlowForceServer2015/tools
```

This command copies the **.tool** file from **/etc** directory of MobileTogether Server to the FlowForce Server **/tools** directory. The **.tool** file is required by FlowForce Server; it contains the path to the MobileTogether Server executable. You do not need to run this command if you install FlowForce Server before installing MobileTogether Server.

- ▼ Uninstall old versions of Altova server products

Before uninstalling MobileTogether Server, stop the service with the following command:

```
sudo launchctl unload /Library/LaunchDaemons/  
com.altova.MobileTogetherServer1.3.plist
```

To check whether the service has been stopped, open the Activity Monitor terminal and make sure that MobileTogether Server is not in the list. In the Applications terminal, right-click the MobileTogether Server icon and select **Move to Trash**. The application will be moved to Trash. You will, however, still need to remove the application from the `usr` folder. Do this with the command:

```
sudo rm -rf /usr/local/Altova/MobileTogetherServer1.3/
```

If you need to uninstall an old version of Altova LicenseServer, you must first stop it running as a service. Do this with the following command:

```
sudo launchctl unload /Library/LaunchDaemons/com.altova.LicenseServer.plist
```

To check whether the service has been stopped, open the Activity Monitor terminal and make sure that LicenseServer is not in the list. Then proceed to uninstall in the same way as described above for MobileTogether Server.

- ▼ Download the Mac OS X package

After downloading the MacOS X package from the [Altova website](#), copy the package to any directory on the Mac OS X system. Since you will need to have an [Altova LicenseServer](#) installed in order to run MobileTogether Server, you may want to download LicenseServer from the [Altova website](#) at the same time as you download MobileTogether Server, rather than download it at a later time. The Mac OS X installer file has a `.pkg` file extension.

▼ Install MobileTogether Server

In a terminal window, switch to the directory where you have copied the installer file, and double-click it. Go through the successive steps of the installer wizard. These are self-explanatory and include one step in which you have to agree to the license agreement before being able to proceed.

The MobileTogether Server package will be installed in the folder:

```
/usr/local/Altova/MobileTogetherServer1.3
```

Clicking the MobileTogether Server icon in the Application terminal pops up the onscreen help (this documentation).

▼ Altova LicenseServer

In order for any Altova Server product—including MobileTogether Server—to run, that server product must be licensed via an [Altova LicenseServer](#) on your network.

On Mac OS X systems, [Altova LicenseServer](#) will need to be installed separately. Download [Altova LicenseServer](#) from the [Altova website](#) and double-click the installer package to start the installation. Follow the onscreen instructions. You will need to accept the license agreement for installation to proceed.

The LicenseServer package will be installed in the folder:

```
/usr/local/Altova/LicenseServer
```

For information about how to register MobileTogether Server with [Altova LicenseServer](#) and license it, see the section, [Licensing on Mac OS X](#).

▼ LicenseServer versions

- Altova server products must be licensed either with the version of LicenseServer that is appropriate to the installed MobileTogether Server version, or with a later version of LicenseServer.
- The LicenseServer version that is appropriate for a particular version of MobileTogether Server is displayed during the installation of MobileTogether Server. You can install this version of LicenseServer along with MobileTogether Server, or you can install LicenseServer separately.
- Before installing a newer version of LicenseServer, any older one must be de-installed. The LicenseServer installer will do this automatically if it detects an older version.
- LicenseServer versions are backwards compatible. They will work with older versions of MobileTogether Server.
- If you install a new version of MobileTogether Server and if your installed LicenseServer version is older than the appropriate LicenseServer, install the latest version available on the Altova website.
- At the time of LicenseServer de-installation, all registration and licensing information held in the older version of LicenseServer will be saved to a database on your server machine. This data will be imported automatically into the newer version when the newer version is installed.
- The version number of the currently installed LicenseServer is given at the bottom of the [LicenseServer configuration page](#) (all tabs).

Current version: 1.13

- ▼ Trial license
During the installation process, you will be given the option of requesting a 30-day trial license for MobileTogether Server. After submitting the request, a trial license will be sent to the email address you registered.

Licensing on Mac OS X

MobileTogether Server must be licensed with an Altova LicenseServer in order to run it. Licensing is a two-step process:

1. **Register MobileTogether Server** with LicenseServer. Registration is done from MobileTogether Server.
2. **Assign a license** to MobileTogether Server. License-assigning is done from LicenseServer.

The steps you need to carry out are given below.

▼ Start LicenseServer

To correctly register and license MobileTogether Server with LicenseServer, LicenseServer must be running as a daemon. Start LicenseServer as a daemon with the following command:

```
sudo launchctl load /Library/LaunchDaemons/com.altova.LicenseServer.plist
```

If at any time you need to stop LicenseServer, replace `load` with `unload` in the above command:

```
sudo launchctl unload /Library/LaunchDaemons/com.altova.LicenseServer.plist
```

▼ Start MobileTogether Server

Start MobileTogether Server as a daemon with the following command:

```
sudo launchctl load /Library/LaunchDaemons/  
com.altova.MobileTogetherServer1.3.plist
```

If at any time you need to stop MobileTogether Server, use:

```
sudo launchctl unload /Library/LaunchDaemons/  
com.altova.MobileTogetherServer1.3.plist
```

When started for the first time, MobileTogether Server will open a Web UI (Setup) page.

If your web browser is on the same machine as MobileTogether Server, the URL of the Setup page is:

```
file:///var/Altova/MobileTogetherServer/MobileTogetherweb.html
```

If your web browser is on a different machine than MobileTogether Server, extract the URL of the Setup page from the log file:

```
grep running /var/Altova/MobileTogetherServer/data/mtweb.log
```

▼ Register MobileTogether Server

Register MobileTogether Server via:

- its CLI, using the `licenseserver` command:

```
sudo /usr/local/Altova/MobileTogetherServer1.3/bin/MobileTogetherServer  
licenseserver [options] ServerName-Or-IP-Address
```

For example, if `localhost` is the name of the server on which LicenseServer is installed:

```
sudo /usr/local/Altova/MobileTogetherServer1.3/bin/MobileTogetherServer
licenseserver localhost
```

In the command above, `localhost` is the name of the server on which LicenseServer is installed. Notice also that the location of the MobileTogether Server executable is:

```
/usr/local/Altova/MobileTogetherServer1.3/bin/
```

- [the Settings tab of MobileTogether Server's Web UI](#). Essentially: (i) Start MobileTogether Server via ServiceController (see *previous point*); (ii) Enter your password to access the Setup page; (iii) Select the LicenseServer name or address, and click **Register with LicenseServer**.

After successful registration, go to the [Server Management tab of LicenseServer's configuration page](#) to assign a license to MobileTogether Server.

▼ Assign a license

After successfully registering MobileTogether Server, it will be listed in the [Server Management tab](#) of the configuration page of LicenseServer. Go [there](#) and [assign a license](#) to MobileTogether Server.

Note on cores and licenses

The licensing of Altova server products, *except MobileTogether Server****, is based on the number of processor cores available on the product machine. For example, a dual-core processor has two cores, a quad-core processor four cores, a hexa-core processor six cores, and so on. The number of cores licensed for a product on a particular server machine must be greater than or equal to the number of cores available on that server, whether it's a physical or virtual machine.

For example, if a server has eight cores (an octa-core processor), you must purchase at least an 8-core license. You can also combine licenses to achieve the core count. So, two 4-core licenses can also be used for an octa-core server instead of an 8-core license.

If you are using a computer server with a large number of CPU cores but only have a low volume to process, you may also create a virtual machine that is allocated a smaller number of cores, and purchase a license for that number. Such a deployment, of course, will have less processing speed than if all available cores on the server were utilized.

Note: Each license can be used for only one client machine at a time, even if it has unused licensing capacity. For example, if a 10-core license is used for a client machine that has 6 CPU cores, then the remaining 4 cores of the license cannot be used simultaneously for another client machine.

*** MobileTogether Server licenses are assigned on the basis of the number of users, that is, the number of client devices that connect to MobileTogether Server.

Notes about Environment

Folders

Given below is a list of important folders in your MobileTogether Server setup.

▣ Installation root

`/usr/local/Altova/MobileTogetherServer1.3/`

▣ Database, License, and Solution Files

`/var/Altova/MobileTogetherServer`

▣ Environment settings

`/Library/LaunchDaemons/com.altova.MobileTogetherServer.plist`

The environment settings file must be defined according to your specific environment. The example path above serves only as a general guide.

Note: These environment variables are only set for the MobileTogether Server process and do not have an impact on other users.

File-based databases

File-based databases (such as SQLite databases) must reside in the folder defined in the Settings tab of MobileTogether Server as the [Server Side's Solutions Working Directory](#). By default, this folder is:

`/var/Altova/MobileTogetherServer/SolutionFiles`

JDBC-Connections

Note the following points:

- The Java Runtime Environment or SDK must be installed.
- The JDBC-Connects for the target database must be installed.
- The following environment variables must be set correctly for your environment:
 - **CLASSPATH:** to find the jar-files
 - **PATH:** to find the JRE, but might not be necessary depending on the installation
 - **JAVA_HOME:** if necessary, depending on the installation

Note

On Mac OS X servers, the only database connections supported are JDBC.

Listing of important files

The following configuration files are installed in the appropriate folder. The parts highlighted in blue are environment-specific and will need to be adjusted to match your environment:

Shell script

```

#- jdbc - environment -
export PATH=/usr/local/jdk1.7.0_17/bin:/usr/lib64/qt-3.3/bin:/usr/local/bin:/
bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/qa/bin
export JAVA_HOME=/usr/local/jdk1.7.0_17
export CLASSPATH=/usr/local/jdbc/oracle/ojdbc6.jar:/usr/local/jdbc/oracle/
xdb.jar:/usr/local/jdbc/oracle/xmlparserv2.jar:/usr/local/jdbc/postgre/
postgresql-9.0-801.jdbc4.jar:/usr/local/jdbc/mssql/sqljdbc4.jar:/usr/local/
jdbc/iseres/lib/jt400.jar:/usr/local/jdbc/mysql/mysql-connector-java-5.1.16-
bin.jar:/usr/local/jdbc/sqlite/sqlitejdbc-v056.jar:/usr/local/jdbc/
Informix_JDBC_Driver/lib/ifxjdbc.jar:/usr/local/jdbc/sybase/jconn7/
jconn4.jar:/usr/local/jdbc/db2/db2jcc.jar:/usr/local/jdbc/db2/
db2jcc_license_cu.jar:./:

```

Plist file

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>Label</key>
    <string>com.altova.MobileTogetherServer</string>
    <key>ProgramArguments</key>
    <array>
      <string>/usr/local/Altova/MobileTogetherServer1.3/bin/
MobileTogetherServer</string>
      <string>debug</string>
    </array>
    <key>KeepAlive</key>
    <true/>
    <key>UserName</key>
    <string>_altovamobiletogetherserver</string>
    <key>EnvironmentVariables</key>
    <dict>
      <key>CLASSPATH</key>
      <string>/usr/local/jdbc/oracle/ojdbc6.jar:/usr/local/jdbc/oracle/
xdb.jar:/usr/local/jdbc/oracle/xmlparserv2.jar:/usr/local/jdbc/postgre/
postgresql-9.0-801.jdbc4.jar:/usr/local/jdbc/mssql/sqljdbc4.jar:/usr/local/
jdbc/iseres/lib/jt400.jar:/usr/local/jdbc/mysql/mysql-connector-java-5.1.16-
bin.jar:/usr/local/jdbc/sqlite/sqlitejdbc-v056.jar:/usr/local/jdbc/
Informix_JDBC_Driver/lib/ifxjdbc.jar:/usr/local/jdbc/sybase/jconn7/
jconn4.jar:/usr/local/jdbc/db2/db2jcc.jar:/usr/local/jdbc/db2/
db2jcc_license_cu.jar:./</string>
    </dict>
  </dict>
</plist>

```

3.4 Setting Up SSL Encryption

If you require that communications between your MobileTogether Server and MobileTogether Client devices are encrypted using the SSL protocol, you will need to:

- Generate an SSL private key and create an SSL public key certificate file
- Set up MobileTogether Server for SSL communication.

The steps to do this are listed below.

MobileTogether uses the open-source [OpenSSL toolkit](#) to manage SSL encryption. The steps listed below, therefore, need to be carried out on a computer on which [OpenSSL](#) is available. [OpenSSL](#) typically comes pre-installed on most Linux distributions and on Mac OS X machines. It can also be [installed on Windows computers](#).

1. Generate a private key

SSL requires that a **private key** is installed on MobileTogether Server. This private key will be used to encrypt all data sent to MobileTogether Client apps. To create the private key, use the following OpenSSL command:

```
openssl genrsa -out private.key 2048
```

This creates a file called `private.key`, which contains your private key. Note where you save the file. You will need the private key to (i) generate the Certificate Signing Request (CSR), and (ii) to be installed on MobileTogether Server (*see Step 8 below*).

2. Certificate Signing Requests (CSRs)

A Certificate Signing Request (CSR) is sent to a certificate authority (CA), such as [VeriSign](#) or [Thawte](#), to request a public key certificate. The CSR is based on your private key and contains information about your organization. Create a CSR with the following OpenSSL command (which provides the private-key file, `private.key`, that was created in Step 1, as one of its parameters):

```
openssl req -new -nodes -key private.key -out my.csr
```

During generation of the CSR you will need to give information about your organization, such as that listed below. This information will be used by the certificate authority to verify your company's identity.

- *Country*
- *Locality* (the city where your business is located)
- *Organization* (your company name). Do not use special characters; these will invalidate your certificate
- *Common Name* (the DNS name of your server). This must exactly match your server's official name, that is, the DNS name client apps will use to connect to the server
- *A challenge password*. Keep this entry blank!

3. Buy an SSL certificate

Purchase an SSL certificate from a recognized certificate authority (CA), such as

[VeriSign](#) or [Thawte](#). For the rest of these instructions, we follow the VeriSign procedure. The procedure with other CAs is similar.

- Go to the [VeriSign website](#).
- Click **Buy SSL Certificates**.
- Different types of SSL certificates are available. For MobileTogether Server, Secure Site or Secure Site Pro certificates are sufficient. EV (extended verification) is not necessary, since there is no "green address bar" for users to see.
- Proceed through the sign-up process, and fill in the information required to place your order.
- When prompted for the CSR (*created in Step 2*), copy and paste the content of the `my.csr` file into the order form.
- Pay for the certificate with your credit card.

Allow time for obtaining a certificate

Obtaining public key certificates from an SSL certificate authority (CA) typically takes **two to three business days**. Please take this into account when setting up your MobileTogether Server.

4. Receive public key from CA
Your certificate authority will complete the enrollment process over the next two to three business days. During this time you might get emails or phone calls to check whether you are authorized to request an SSL certificate for your DNS domain. Please work with the authority to complete the process.

After the authorization and enrollment process has been completed, you will get an email containing the **public key** of your SSL certificate. The public key will be in plain text form or attached as a `.cer` file.

5. Save public key to file
For use with MobileTogether Server, the public key must be saved in a `.cer` file. If the public key was supplied as text, copy-paste all the lines from

```
--BEGIN CERTIFICATE--  
...  
--END CERTIFICATE--
```

into a text file that we will call `mycertificate.cer`.

6. Save CA's intermediate certificates to file
To complete your SSL certificate, you will need two additional certificates: the **primary** and **secondary intermediate certificates**. Your certificate authority (CA) will list content of intermediate certificates on its website.
 - Verisign's intermediate certificates: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657&actp=LIST&viewlocale=en_US
 - Verisign's intermediate certificates for its Secure Site product: <https://>

knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR1735

Copy-paste both intermediate certificates (primary and secondary) into separate text files and save them on your computer.

7. Combine certificates in one public key certificate file

You now have three certificate files:

- Public key (*mycertificate.cer*)
- Secondary intermediate certificate
- Primary intermediate certificate

Each contains text blocks bracketed by lines that look like this:

```
--BEGIN CERTIFICATE--  
...  
--END CERTIFICATE--
```

Now copy-paste all three certificates into one file so that they are in sequence. The order of the sequence is important: (i) public key, (ii) secondary intermediate certificate, (iii) primary intermediate certificate. Ensure that there are no lines between certificates.

```
--BEGIN CERTIFICATE--  
public key from mycertificate.cer (see Step 5)  
--END CERTIFICATE--  
--BEGIN CERTIFICATE--  
secondary intermediate certificate (see Step 6)  
--END CERTIFICATE--  
--BEGIN CERTIFICATE--  
primary intermediate certificate (see Step 6)  
--END CERTIFICATE--
```

Save the resulting combined certificate text to a file named **publickey.cer**. This is the *public key certificate file* of your SSL certificate. It includes your public key certificate as well as the complete chain of trust in the form of the intermediate certificates that were used by the CA to sign your certificate. The public key certificate file will be installed on MobileTogether Server together with the private key (see Step 8).

8. Install SSL certificate on MobileTogether Server

The SSL certificate is a set of certificates that are saved in the following files:

- *private.key*: Contains the private key certificate
- *publickey.cer*: Contains the public key certificate and the CA's intermediate certificates (primary and secondary)

To install the SSL certificates on MobileTogether Server, do the following:

- Log in to the MobileTogether Server UI (by default on port 8085 of your server).
- Go to the Settings tab.
- Under SSL Certificates (see *screenshot below*), upload the two certificate files.

SSL certificates:

Select the private key and the certificate needed for secure (SSL) communication.
A valid private key and certificate must be supplied in order to use secure (HTTPS) ports.
The private key/certificate must be in PEM format.

Private Key:

No file selected.

Certificate:

No file selected.

- For the private key, select `private.key` (created in Step 1)
 - For the certificate, select `publickey.cer` (created in Step 7)
 - Click **Save** at the bottom of the General Settings section to save your changes.
9. Set the server's HTTPS port
- After installing the SSL certificate, you can specify a server port for SSL client communication. Do this as follows:
- Log in to the MobileTogether Server UI (by default on port 8085 of your server).
 - Go to the Settings tab.
 - Under Mobile Client Ports (see screenshot below), enable and specify the HTTPS port.

Mobile client ports:

Select unsecure (HTTP) and secure (HTTPS) ports the Mobile clients will use.
These ports cannot be used for administrative purposes!

HTTP Port: 8083

HTTPS Port: 8084

Make sure that any firewall is set up to allow access to MobileTogether Server through the HTTPS port.

10. Test SSL communication
- You can now use any SSL testing tool to check whether secure communication with your server via HTTPS is working properly. For example, this can be done with a browser, using the following SSL test site: <https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp>

This will tell you: (i) whether the public key certificate file was properly constructed with the intermediate trust chain in Step 7, and (ii) whether your server can be reached properly through the firewall.

11. Enable MobileTogether Clients to use SSL

In MobileTogether Client apps that communicate with an SSL-enabled MobileTogether Server, enable SSL communication by checking the *SSL Encryption* checkbox. See the MobileTogether Client documentation for information about how to find this check box.

Chapter 4

Server Procedures

4 Server Procedures

This section describes important server procedures. It assumes that MobileTogether Server has [already been licensed](#). Note, however, that in order for MobileTogether Server to be accessed, both LicenseServer and MobileTogether Server must be started and running as services.

- [Start Altova LicenseServer](#)
- [Start MobileTogether Server](#)
- [Set Up SSL Encryption](#)
- [Set Administrator and Mobile Client Ports](#)
- [Users and Roles](#)
- [Available Privileges](#)
- [Information for Clients](#)

4.1 Start Altova LicenseServer

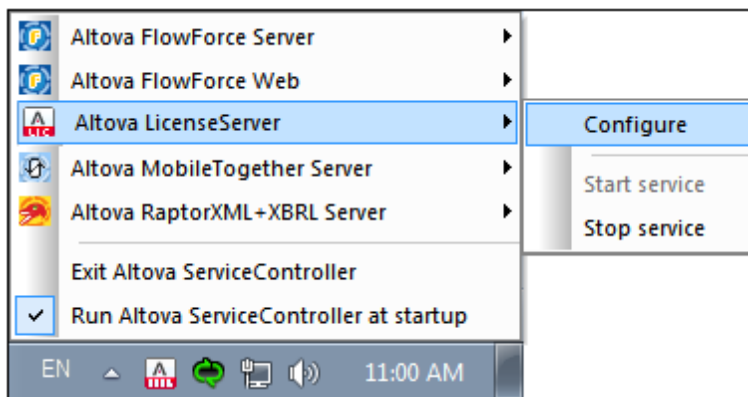
In order to run an installation of an Altova server product (i) FlowForce Server; (ii) RaptorXML(+XBRL) Server; (iii) MobileTogether Server; (iv) MapForce Server; (v) StyleVision Server, that installation must be licensed with an Altova LicenseServer on your network. LicenseServer must be running continuously as a service in order for all connected MobileTogether Server installations to run. Stopping LicenseServer will also stop all connected MobileTogether Server installations. If this happens, you will need to first restart LicenseServer, and then restart the stopped MobileTogether Server installation that you want to work with.

Start and stop LicenseServer as follows:

▼ On Windows

You can start LicenseServer via the Altova ServiceController, which is available in the system tray.

First, click **Start | All Programs | Altova LicenseServer | Altova ServiceController** to start Altova ServiceController and display its icon in the system tray (see screenshot below). If you select the *Run Altova ServiceController at Startup* option, Altova ServiceController will start up on system start and its icon will be available in the system tray from then onwards.



To start LicenseServer, click the Altova ServiceController icon in the system tray, hover over **Altova LicenseServer** in the menu that pops up (see screenshot above), and then select **Start Service** from the LicenseServer submenu. If LicenseServer is already running, the *Start Service* option will be disabled.

To stop LicenseServer, select **Stop Service** from the LicenseServer submenu (see screenshot above).

▼ On Linux

To start LicenseServer as a service on Linux systems, run the following command in a terminal window.

```
[Debian]:          sudo /etc/init.d/licenseserver start
```

```
[Ubuntu]:      sudo initctl start licenseserver
[CentOS]:     sudo initctl start licenseserver
[RedHat]:     sudo initctl start licenseserver
```

(If you need to stop LicenseServer, replace `start` with `stop` in the above commands.)

▼ **On Mac OS X**

To start LicenseServer as a service on Mac OS X systems, run the following command in a terminal window:

```
sudo launchctl load /Library/LaunchDaemons/com.altova.LicenseServer.plist
```

If at any time you need to stop LicenseServer, use:

```
sudo launchctl unload /Library/LaunchDaemons/com.altova.LicenseServer.plist
```

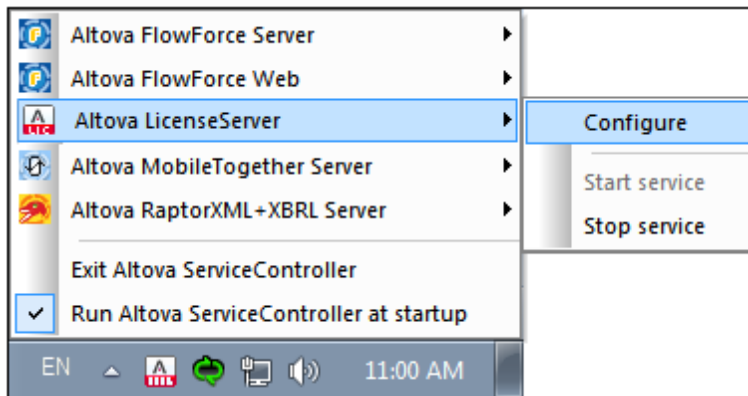
4.2 Start MobileTogether Server

In order to run MobileTogether Server, MobileTogether Server must be started as a service. Additionally, in order to use the Web UI of MobileTogether Server, it too must be started as a service. How to do this explained below.

▼ On Windows

You can start MobileTogether Server via the Altova ServiceController, which is available in the system tray.

First, click **Start | All Programs | Altova LicenseServer | Altova ServiceController** to start Altova ServiceController and display its icon in the system tray (see screenshot below). If you select the *Run Altova ServiceController at Startup* option, Altova ServiceController will start up on system start and its icon will be available in the system tray from then onwards.



To start MobileTogether Server, click the Altova ServiceController icon in the system tray, hover over **MobileTogether Server** in the menu that appears (see screenshot above), and then select **Start Service** from the MobileTogether Server submenu. If MobileTogether Server is already running, the *Start Service* option will be disabled.

To stop MobileTogether Server, select **Stop Service** from the MobileTogether Server submenu (see screenshot above).

▼ On Linux

To start MobileTogether Server as a service on Linux systems, run the following command in a terminal window.

```
[Debian]:          sudo /etc/init.d/mobiletogetherserver start
[Ubuntu]:          sudo initctl start mobiletogetherserver
[CentOS]:          sudo initctl start mobiletogetherserver
[RedHat]:          sudo initctl start mobiletogetherserver
```

(If you need to stop MobileTogether Server, replace `start` with `stop` in the above commands.)

▼ On Mac OS X

To start MobileTogether Server as a service on Mac OS X systems, run the following command in a terminal window:

```
sudo launchctl load /Library/LaunchDaemons/  
com.altova.MobileTogetherServer.plist
```

If at any time you need to stop MobileTogether Server, use:

```
sudo launchctl unload /Library/LaunchDaemons/  
com.altova.MobileTogetherServer.plist
```

4.3 Set Up SSL Encryption

If you require that communications between your MobileTogether Server and MobileTogether Client devices are encrypted using the SSL protocol, you will need to:

- Generate an SSL private key and create an SSL public key certificate file
- Set up MobileTogether Server for SSL communication.

The steps to do this are listed below.

MobileTogether uses the open-source [OpenSSL toolkit](#) to manage SSL encryption. The steps listed below, therefore, need to be carried out on a computer on which [OpenSSL](#) is available. [OpenSSL](#) typically comes pre-installed on most Linux distributions and on Mac OS X machines. It can also be [installed on Windows computers](#).

1. Generate a private key

SSL requires that a **private key** is installed on MobileTogether Server. This private key will be used to encrypt all data sent to MobileTogether Client apps. To create the private key, use the following OpenSSL command:

```
openssl genrsa -out private.key 2048
```

This creates a file called `private.key`, which contains your private key. Note where you save the file. You will need the private key to (i) generate the Certificate Signing Request (CSR), and (ii) to be installed on MobileTogether Server (*see Step 8 below*).

2. Certificate Signing Requests (CSRs)

A Certificate Signing Request (CSR) is sent to a certificate authority (CA), such as [VeriSign](#) or [Thawte](#), to request a public key certificate. The CSR is based on your private key and contains information about your organization. Create a CSR with the following OpenSSL command (which provides the private-key file, `private.key`, that was created in Step 1, as one of its parameters):

```
openssl req -new -nodes -key private.key -out my.csr
```

During generation of the CSR you will need to give information about your organization, such as that listed below. This information will be used by the certificate authority to verify your company's identity.

- *Country*
- *Locality* (the city where your business is located)
- *Organization* (your company name). Do not use special characters; these will invalidate your certificate
- *Common Name* (the DNS name of your server). This must exactly match your server's official name, that is, the DNS name client apps will use to connect to the server
- *A challenge password*. Keep this entry blank!

3. Buy an SSL certificate

Purchase an SSL certificate from a recognized certificate authority (CA), such as

[VeriSign](#) or [Thawte](#). For the rest of these instructions, we follow the VeriSign procedure. The procedure with other CAs is similar.

- Go to the [VeriSign website](#).
- Click **Buy SSL Certificates**.
- Different types of SSL certificates are available. For MobileTogether Server, Secure Site or Secure Site Pro certificates are sufficient. EV (extended verification) is not necessary, since there is no "green address bar" for users to see.
- Proceed through the sign-up process, and fill in the information required to place your order.
- When prompted for the CSR (*created in Step 2*), copy and paste the content of the `my.csr` file into the order form.
- Pay for the certificate with your credit card.

Allow time for obtaining a certificate

Obtaining public key certificates from an SSL certificate authority (CA) typically takes **two to three business days**. Please take this into account when setting up your MobileTogether Server.

4. Receive public key from CA
Your certificate authority will complete the enrollment process over the next two to three business days. During this time you might get emails or phone calls to check whether you are authorized to request an SSL certificate for your DNS domain. Please work with the authority to complete the process.

After the authorization and enrollment process has been completed, you will get an email containing the **public key** of your SSL certificate. The public key will be in plain text form or attached as a `.cer` file.

5. Save public key to file
For use with MobileTogether Server, the public key must be saved in a `.cer` file. If the public key was supplied as text, copy-paste all the lines from

```
--BEGIN CERTIFICATE--
...
--END CERTIFICATE--
```

into a text file that we will call `mycertificate.cer`.

6. Save CA's intermediate certificates to file
To complete your SSL certificate, you will need two additional certificates: the **primary** and **secondary intermediate certificates**. Your certificate authority (CA) will list content of intermediate certificates on its website.
 - Verisign's intermediate certificates: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657&actp=LIST&viewlocale=en_US
 - Verisign's intermediate certificates for its Secure Site product: <https://>

knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR1735

Copy-paste both intermediate certificates (primary and secondary) into separate text files and save them on your computer.

7. Combine certificates in one public key certificate file

You now have three certificate files:

- Public key (*mycertificate.cer*)
- Secondary intermediate certificate
- Primary intermediate certificate

Each contains text blocks bracketed by lines that look like this:

```
--BEGIN CERTIFICATE--  
...  
--END CERTIFICATE--
```

Now copy-paste all three certificates into one file so that they are in sequence. The order of the sequence is important: (i) public key, (ii) secondary intermediate certificate, (iii) primary intermediate certificate. Ensure that there are no lines between certificates.

```
--BEGIN CERTIFICATE--  
public key from mycertificate.cer (see Step 5)  
--END CERTIFICATE--  
--BEGIN CERTIFICATE--  
secondary intermediate certificate (see Step 6)  
--END CERTIFICATE--  
--BEGIN CERTIFICATE--  
primary intermediate certificate (see Step 6)  
--END CERTIFICATE--
```

Save the resulting combined certificate text to a file named **publickey.cer**. This is the *public key certificate file* of your SSL certificate. It includes your public key certificate as well as the complete chain of trust in the form of the intermediate certificates that were used by the CA to sign your certificate. The public key certificate file will be installed on MobileTogether Server together with the private key (see Step 8).

8. Install SSL certificate on MobileTogether Server

The SSL certificate is a set of certificates that are saved in the following files:

- *private.key*: Contains the private key certificate
- *publickey.cer*: Contains the public key certificate and the CA's intermediate certificates (primary and secondary)

To install the SSL certificates on MobileTogether Server, do the following:

- Log in to the MobileTogether Server UI (by default on port 8085 of your server).
- Go to the Settings tab.
- Under SSL Certificates (see *screenshot below*), upload the two certificate files.

SSL certificates:

Select the private key and the certificate needed for secure (SSL) communication.
A valid private key and certificate must be supplied in order to use secure (HTTPS) ports.
The private key/certificate must be in PEM format.

Private Key:

Certificate:

- For the private key, select `private.key` (created in Step 1)
 - For the certificate, select `publickey.cer` (created in Step 7)
 - Click **Save** at the bottom of the General Settings section to save your changes.
9. Set the server's HTTPS port
- After installing the SSL certificate, you can specify a server port for SSL client communication. Do this as follows:
- Log in to the MobileTogether Server UI (by default on port 8085 of your server).
 - Go to the Settings tab.
 - Under Mobile Client Ports (see screenshot below), enable and specify the HTTPS port.

Mobile client ports:

Select unsecure (HTTP) and secure (HTTPS) ports the Mobile clients will use.
These ports cannot be used for administrative purposes!

HTTP Port:

HTTPS Port:

Make sure that any firewall is set up to allow access to MobileTogether Server through the HTTPS port.

10. Test SSL communication
- You can now use any SSL testing tool to check whether secure communication with your server via HTTPS is working properly. For example, this can be done with a browser, using the following SSL test site: <https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp>

This will tell you: (i) whether the public key certificate file was properly constructed with the intermediate trust chain in Step 7, and (ii) whether your server can be reached properly through the firewall.

11. Enable MobileTogether Clients to use SSL

In MobileTogether Client apps that communicate with an SSL-enabled MobileTogether Server, enable SSL communication by checking the *SSL Encryption* checkbox. See the MobileTogether Client documentation for information about how to find this check box.

4.4 Set Administrator and Mobile Client Ports

The administrator ports are used to connect to the Web UI of MobileTogether Server, while the mobile client ports are those the mobile client device uses to connect to the services of MobileTogether Server.

Set the administrator ports

The administrator ports provide access for the following purposes:

- To connect to the server's Web UI and perform administrative functions, such as setting up [Users and Roles](#).
- To deploy MobileTogether designs (as MobileTogether solutions) to the server. MobileTogether Designer has a setting that specifies the address and port of the MobileTogether Server to which to deploy designs.

Administrator ports:
Select unsecure (HTTP) and secure (HTTPS) ports to be used by the administrator. These ports can be used for server configuration, user, role, and user license administration, workflow deployment and workflow simulation.
 HTTP Port:
 HTTPS Port:

The HTTP port is the unsecure port; HTTPS is the secure port. To use HTTPS, you need to set up [SSL Encryption](#).

Set the mobile client ports

The ports that mobile devices will use to connect to the server. The HTTP port is the unsecure port; HTTPS is the secure port. To use HTTPS, you need to set up [SSL Encryption](#).

Mobile client ports:
Select unsecure (HTTP) and secure (HTTPS) ports the Mobile clients will use. These ports cannot be used for administrative purposes!
 HTTP Port:
 HTTPS Port:

4.5 Users and Roles

A user account is defined by a log-in name and password, and has a set of access rights associated with it. Users access MobileTogether Server for administrative purposes or as client end users.

Access rights are determined by the privileges a user is granted. A user receives privileges in the following ways: (i) privileges inherited from roles the user is a member of, (ii) privileges assigned directly to the user. A role is defined by a set of privileges. A role is either assigned privileges directly and/or inherits the privileges of another role that it is a member of. Privileges themselves are access rights to the various administrative functions and services of MobileTogether Server. Examples of privileges are: the right to manage server settings, to set a user's own password, to run simulations on the server.

Through the use of roles, user privileges can be defined in a hierarchical way. For example, the role of `SimpleAdmin` role could allow the privilege, *Manage server settings*. If `AdvancedAdmin` is a member of `SimpleAdmin`, it inherits the management of server settings, and could additionally be assigned the privilege, *Maintain users, roles and privileges*. The hierarchical chain can be further extended. For a list of privileges, see [Available Privileges](#).

▼ About Users

A user is defined by a name-and-password combination. Users access MobileTogether Server in two ways:

- *Web UI access*: The Web UI is the administrative interface of MobileTogether Server. Logging in to the Web UI requires a name-and-password combination; it is therefore done as a user.
- *Service interface*: The HTTP service interface exposes MobileTogether Server services, typically to the MobileTogether Client app on a mobile device. A user accesses the service interface, using a name-and-password combination. The services exposed relate typically to access to MobileTogether solutions and their related data.

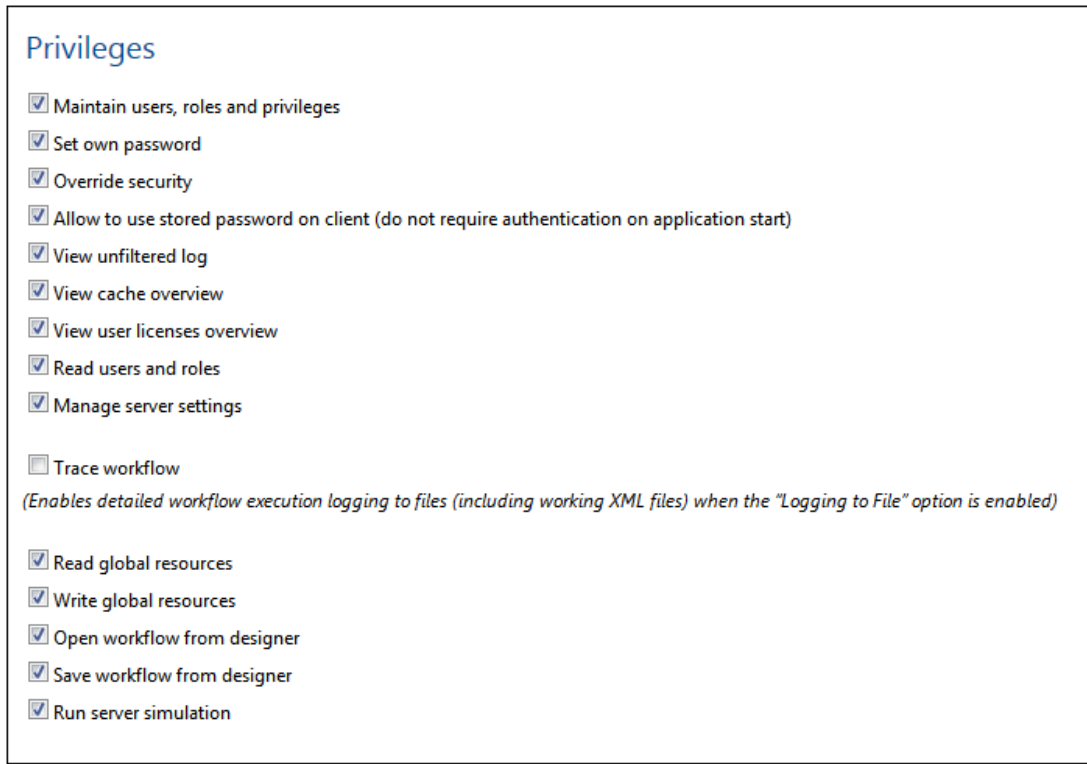
Two special users are predefined:

root	root is the initial administrator user. It is initially the most powerful user, having all privileges and having the ability to add other users and to set roles. Its initial name-password combination is: <code>root-root</code> . The password can be changed at any time.
anonymous	anonymous is an account for anonymous users that access services exposed via the HTTP service interface. It cannot be used for logging in top the Web UI, and it has no initial password.

▼ About Privileges

A privilege is an activity that a user is allowed to carry out. There is a fixed number of MobileTogether Server privileges, and a user can be assigned zero to all of the available privileges. It is, however, good practice to assign privileges via roles (*see next section*), rather than to assign privileges directly to the user. The assigning of privileges and roles to a user is done by a user that has been assigned this privilege. Initially, it is `root` user that has this privilege.

The screenshot below shows all the available privileges.



The tab [Users and Roles | Reports | Privileges Report](#) provides a list of all privileges, with each privilege being listed together with all the users/roles that have that privilege.

▼ About Roles

A role defines a set of privileges. It can be assigned to another role or to a user. A role's privileges automatically become the privileges of any other role or any user that the role is assigned to. A user can be assigned any number of roles. As a result, a user will have all the privileges defined in the multiple assigned roles.

The following roles are predefined:

- **authenticated** is automatically assigned to every user **except** **anonymous**. So user with a name-and-password is assigned the **authenticated** role.
- **a11** is automatically assigned to every user **including** **anonymous**.
- **workflow-designer** is assigned to users that design workflows in MobileTogether Designer. This role allows a user to open and save workflows, as well as to run a simulation on the server.
- **workflow-user** is assigned to users running the workflow on a mobile device. This role allows the user to access the service interface without needing to log in to the server and start the solution on the client.

4.6 Available Privileges

Privileges themselves are access rights to the various administrative functions and services of MobileTogether Server. When a user logs in to MobileTogether Server (either via its Web UI or services interface), the user's access rights are determined by the user's privileges. Privileges are assigned to the user either directly or via roles, in the [Users and Roles](#) tab.

Privileges

- Maintain users, roles and privileges
- Set own password
- Override security
- Allow to use stored password on client (do not require authentication on application start)
- View unfiltered log
- View cache overview
- View user licenses overview
- Read users and roles
- Manage server settings

- Trace workflow
(Enables detailed workflow execution logging to files (including working XML files) when the "Logging to File" option is enabled)

- Read global resources
- Write global resources
- Open workflow from designer
- Save workflow from designer
- Run server simulation

The available privileges are described below.

- ▣ Maintain users, roles and privileges
Any user having this privilege can create, delete and edit users and roles, their privilege assignments and passwords. This is an administrative privilege and should only be assigned to MobileTogether administrators. By default, only the user "root" possesses this privilege.
- ▣ Set own password
Any user having this privilege can change his own password. Users who do not have this privilege need to have their password set by a MobileTogether administrator. By default the "authenticated" role, and hence every user account except "anonymous", possesses this privilege.
- ▣ Override security
Any user having this privilege can change permissions in the container hierarchy without needing "write" security permission. This allows MobileTogether administrators to regain access to resources accidentally rendered inaccessible. This is an administrative privilege and should only be assigned to MobileTogether administrators. By default, only "root" possesses this privilege.

- ▣ Allow use of stored password on client
Allows the user to use the password stored on the client. User does not need authentication.
- ▣ View unfiltered log
By default users can only see log entries related to Configurations they have "read" access to. By granting this privilege a user can read all log entries, including those not associated with a specific configuration. By default, only "root" possesses this privilege.
- ▣ View cache overview
Allows the user to view the cache overview on the server.
- ▣ View user licenses overview
Allows the user to see the licenses overview on the server.
- ▣ Read users and roles
By default users will only see their own user account and any roles they are member of. By granting this privilege a user can read all defined users and roles. By default, only "root" possesses this privilege.
- ▣ Manage server settings
Allows the user to edit [server settings](#).
- ▣ Trace workflow
Allows detailed workflow execution logging to files, if the "logging to file directory" option is enabled in the Logging group of the Settings dialog box.
- ▣ Read global resources
Allows the user with this privilege to read the global resource alias/configuration from the server.
- ▣ Write global resources
Allows the user with this privilege to write/save the global resource alias/configuration to the server.
- ▣ Open workflow from designer
Allows a user to open a deployed MobileTogether design file from the server. The host login details are supplied by selecting the menu option File | Open from MobileTogether server.
- ▣ Save workflow from designer
Allows a user to save/deploy a MobileTogether design file to the server. The host login details are supplied by selecting the menu option File | Save to MobileTogether server.
- ▣ Run server simulation
Allows the user having this privilege to run a simulation from the browser (and preview the result). Note the Back browser button returns you to the container view.

4.7 Information for Clients

The MobileTogether Client app on mobile devices will need to connect to MobileTogether Server, and the following server information will be required by the MobileTogether Client app.

<i>IP Address</i>	The IP address of MobileTogether Server
<i>Port</i>	The HTTP or HTTPS port, which is specified in the Mobile Client Ports setting
<i>SSL</i>	Whether communication should be SSL encrypted or not
<i>User name</i>	As what user to log in. This will determine access rights. See Users and Roles
<i>Password</i>	The password of the user account

Note: Data that is saved on the web client is saved in the local storage (aka web storage) of your browser. HTML 5.0 local storage is supported in the following browsers:

IE 8.0 +	Firefox 3.5+	Safari 4.0+	Chrome 4.0+	Opera 10.5+	iPhone 2.0+	Android 2.0+
-------------	-----------------	----------------	----------------	----------------	----------------	-----------------

Chapter 5

Web UI Reference

5 Web UI Reference

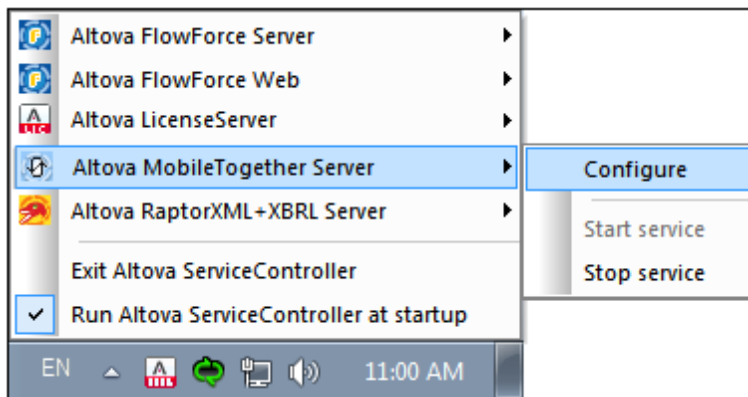
MobileTogether Server has a **Web User Interface** (Web UI) with which you can easily configure MobileTogether Server. The Web UI can be opened in any Internet browser on any of the [supported operating systems](#).

Accessing the Web UI of MobileTogether Server

The MobileTogether Server Web UI is accessed as follows:

▼ On Windows

To access the Web UI, click the **ServiceController** icon in the system tray (see *screenshot below*), hover over **Altova MobileTogether Server** in the menu that pops up, and then select **Configure** from the MobileTogether Server submenu. If MobileTogether Server is not already running, use the *Start Service* option to start MobileTogether Server.



To sign in, enter the username and password. The default `username/password` is `root/root`.

▼ On Linux

To access the Web UI, enter its URL in the address bar of a browser and press **Enter**. By default, the URL of the Web UI page (for administrative access) is:

<http://<serverIPAddressOrName>:8085/>

To sign in, enter the username and password. The default `username/password` is `root/root`.

▼ On Mac OS X

To access the Web UI, enter its URL in the address bar of a browser and press **Enter**. By default, the URL of the Web UI page (for administrative access) is:

<http://<serverIPAddressOrName>:8085/>

To sign in, enter the username and password. The default `username/password` is `root/root`.

Web UI tabs

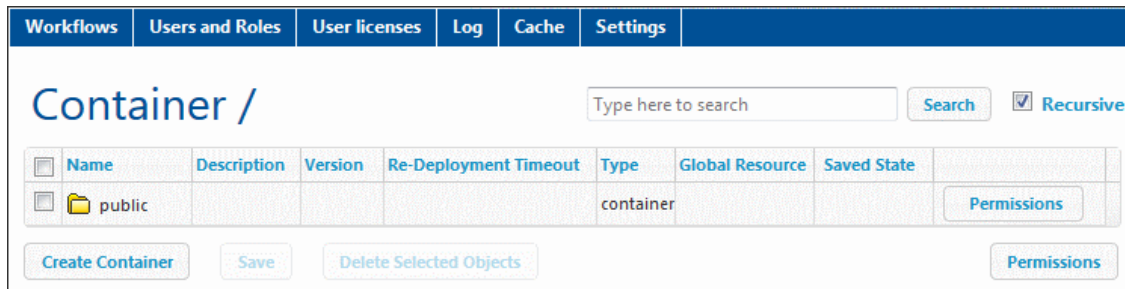
The Web UI is the administrator interface of MobileTogether Server. The various administrative functions are available in the following Web UI tabs:

- [Workflows](#): An interface for managing the server's container structure and container permissions.
- [Users and Roles](#): To set up user accounts and roles, and the privileges associated with users and roles. The access rights of users are defined in this tab.
- [User licenses](#): Shows the mobile devices that are currently licensed, and their license details.
- [Log](#): Displays the logged server actions according to the selected filters.
- [Cache](#): This tab shows the details of caches that are currently available on the server. Caches can also be activated/deactivated and deleted.
- [Settings](#): MobileTogether Server settings, such as access ports, log settings, and server session timeouts, are defined in this tab.

5.1 Workflows

The **Workflows** tab (*screenshot below*) provides an interface for managing the container structure of the `root` folder of MobileTogether Server and the access rights (permissions) for each container. Containers are folders that contain sub-containers and/or solutions (aka design files or `.mtd` files). MTD files cannot be added to a container via the server's Web UI, but are deployed to the server from MobileTogether Designer. At deployment, the exact path to a container must be specified; this is facilitated by being able to browse, in MobileTogether Designer, to the required container.

The *Workflows* tab initially displays the `root` container, which is denoted by the `"/` character.



▼ Functionality

The buttons of the tab provide the following functionality:

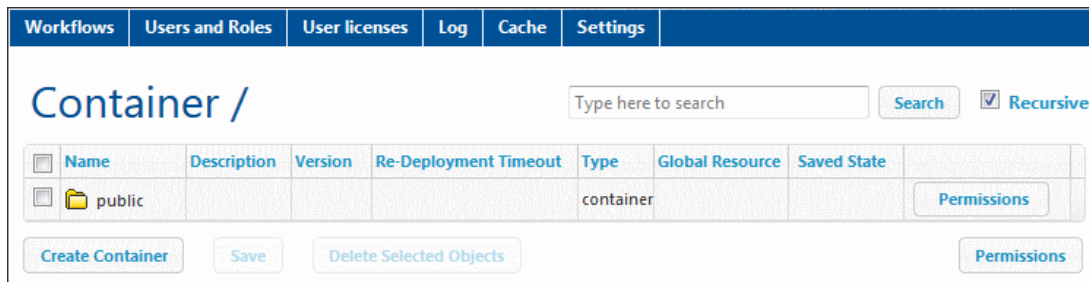
<i>Create Container</i>	Creates a container in the current folder. Click a container to open it
<i>Save</i>	Saves changes such as a modification of descriptions
<i>Delete Selected</i>	Deletes the selected container or file
<i>Permissions</i>	Sets which users/roles can access individual containers, and their level of access
<i>Search</i>	Searches for the term submitted. Check <i>Recursive</i> to search in descendant containers

Other available actions:

- To navigate up the container hierarchy, click the required ancestor folder in the path at the top of the *Workflows* tab
- To navigate down the container hierarchy, click a container to open it
- Click a solution file's URL to run the solution

▼ The container `/public/`

Clicking the `public` container opens the container and displays its contents. `public` is a predefined container containing sample design files (solutions) that are delivered with the program. Click a solution's URL to run it.



▼ The display of a container's contents




A container contains sub-containers and/or solutions (aka design files or .mtd files). The contents of each container are displayed as a tabular list. The columns of the table display the properties of solutions:

- *Name*: Name of the solution file as saved in MobileTogether Designer
- *Description*: Short description of the solution, which can be entered by clicking in the field.
- *Version*: Version of MobileTogether Designer in which the solution was created
- *Re-deployment Timeout*: Period of time an existing solution remains in the server database after a new version of the same file has been deployed there. This allows end users that are using the older solution time (default 5 hours) to log out, restart the MobileTogether Client app, and then use the newer solution. The timeout is set in MobileTogether Designer in the Styles & Properties tab, in **Project | Re-Deployment Timeout**
- *Type*: Either `container` or `workflow`
- *Global Resource*: The global resource that has been defined for that solution and deployed to the server. If no global resource is specified, `Default` is displayed
- *Saved State*: A **Clear Saved Data** button appears in this column if data has been changed while running the solution. Click the button if you wish to undo the changes
- *Location*: The server URL where the solution file is deployed. Click to run the solution

▼ Permissions

Permissions are access rights, and they can be set for each container individually. Permissions determine which users or roles have access to that container, and what kind of access each user/role has (read, write, use). These access rights can be set for the container, its workflows (or solutions), and read/write security.

Permissions for [/ public / contacts](#)

User or Role name	Permissions	
 anonymous	Container: Read, Write inherited from  /public Workflow: Read, Write, Use inherited from  /public Security: Read inherited from  /public	Change
 authenticated	Container: Read inherited from  / Workflow: Read, Write, Use Security: Read inherited from  /	Change
 root	Container: Read, Write inherited from  / Workflow: Read, Write, Use inherited from  authenticated Security: Read, Write inherited from  /	Change

[Add Permissions](#)

Rules for inheritance of permissions

- For containers, permissions are inherited from parent containers.
- For users, permissions are inherited from all roles the user is a member of, as well as from permissions directly assigned to the user.
- Inheritance rules for users take precedence over container hierarchy rules.
- If a permission is redefined for any role the user is a member of, container hierarchy inheritance for this particular permission is overridden.

Permissions are checked for every user interaction. A user can only successfully access and/or edit when all required permissions are granted. Permissions are set for the following groups:

Container

- *Read*: The user can list the contents and find an object in the container.
- *Read-Write*: Additional to read, can create new (and delete existing) objects, depending on other permissions that may apply.

Workflow

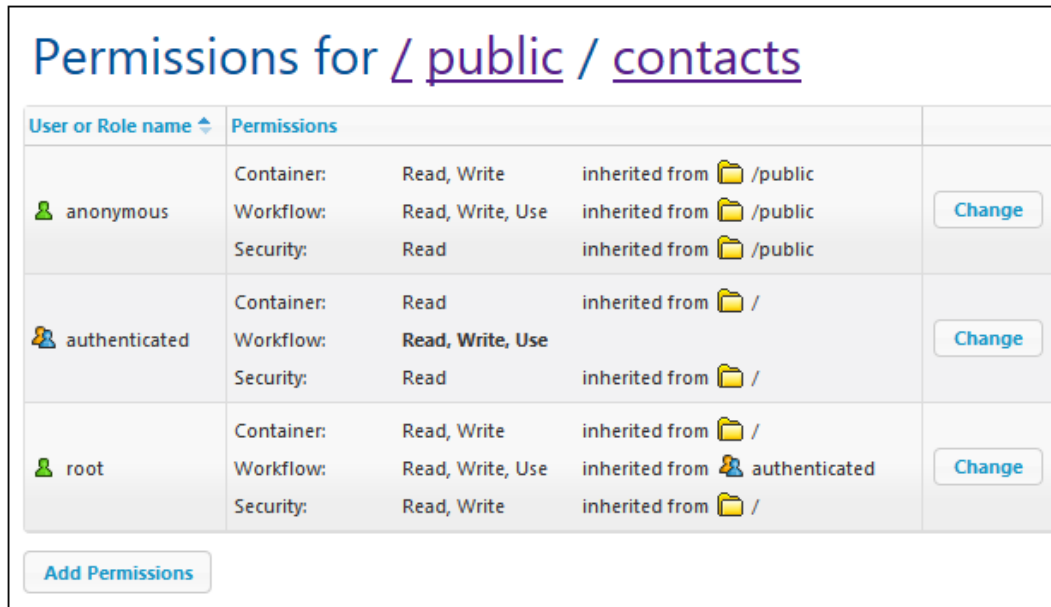
- *Read*: The user can run solutions.
- *Read-Write*: The user can additionally write to solution data. To modify file data, write access must also be granted for the container.

Security

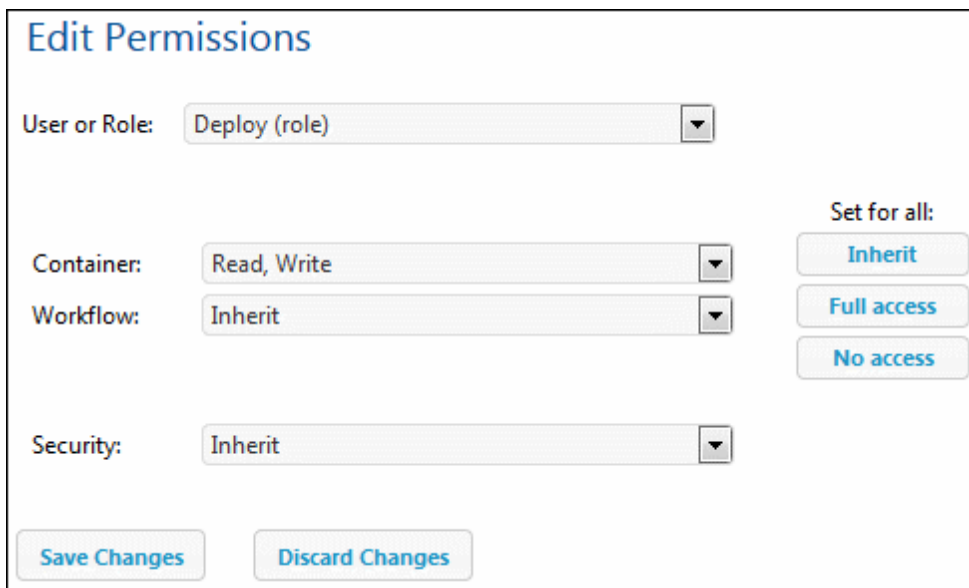
- *Read*: The user is permitted to read the permission list of any child object of the container.
- *Read-Write*: The user can additionally change the permissions list of any child object of the container.
- By default a user is permitted to read only permissions assigned to it or a role it is a member of. If the *Read Users and Roles* privilege is granted (see [Users and Roles](#)), users can read all permission entries.

Editing the permissions of a container

1. Click the **Permissions** button of the container. This takes you to the container's *Permissions* page (screenshot below).



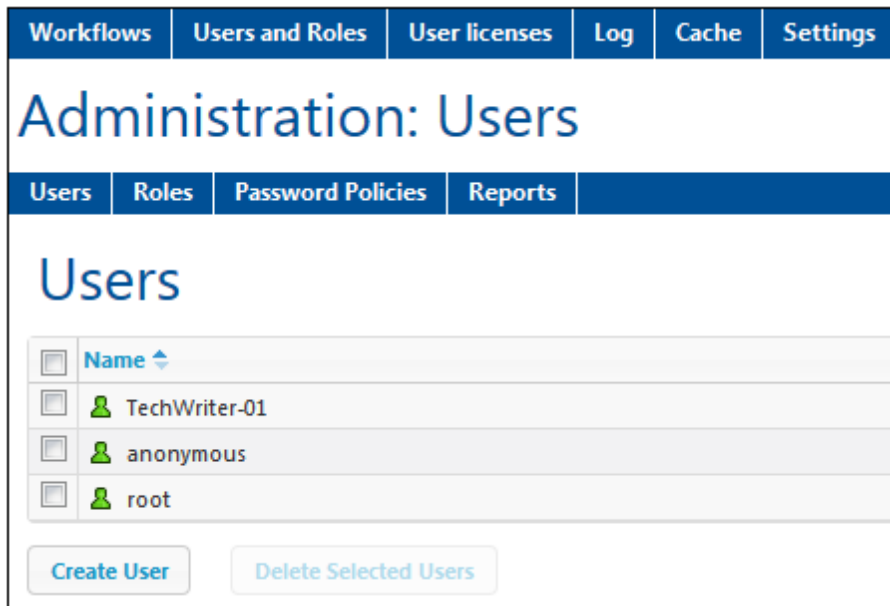
2. To edit the access rights of an already permitted user/role, click its **Change** button. To add permissions for a new user/role, click **Add Permissions**. Both these buttons open the *Edit Permissions* pane.



3. Select a user/role. If you are editing existing permissions, permissions will be inherited from this user/role. If you are adding permissions, this user/role will be added to the permitted users/roles list of this container.
4. Change the permissions as required. The *Inherit* option causes permissions to be inherited from the parent container.

5.2 Users and Roles

The **Users and Roles** tab (*screenshot below*) has four sub-tabs. These sub-tabs work together to enable user accounts to be administered. User accounts can be set up and configured for privileges, and summaries of accounts and privileges can be viewed in the *Reports* sub-tab. See the sub-sections for detailed descriptions.



[New Link](#)

▼ About Users

A user is defined by a name-and-password combination. Users access MobileTogether Server in two ways:

- *Web UI access*: The Web UI is the administrative interface of MobileTogether Server. Logging in to the Web UI requires a name-and-password combination; it is therefore done as a user.
- *Service interface*: The HTTP service interface exposes MobileTogether Server services, typically to the MobileTogether Client app on a mobile device. A user accesses the service interface, using a name-and-password combination. The services exposed relate typically to access to MobileTogether solutions and their related data.

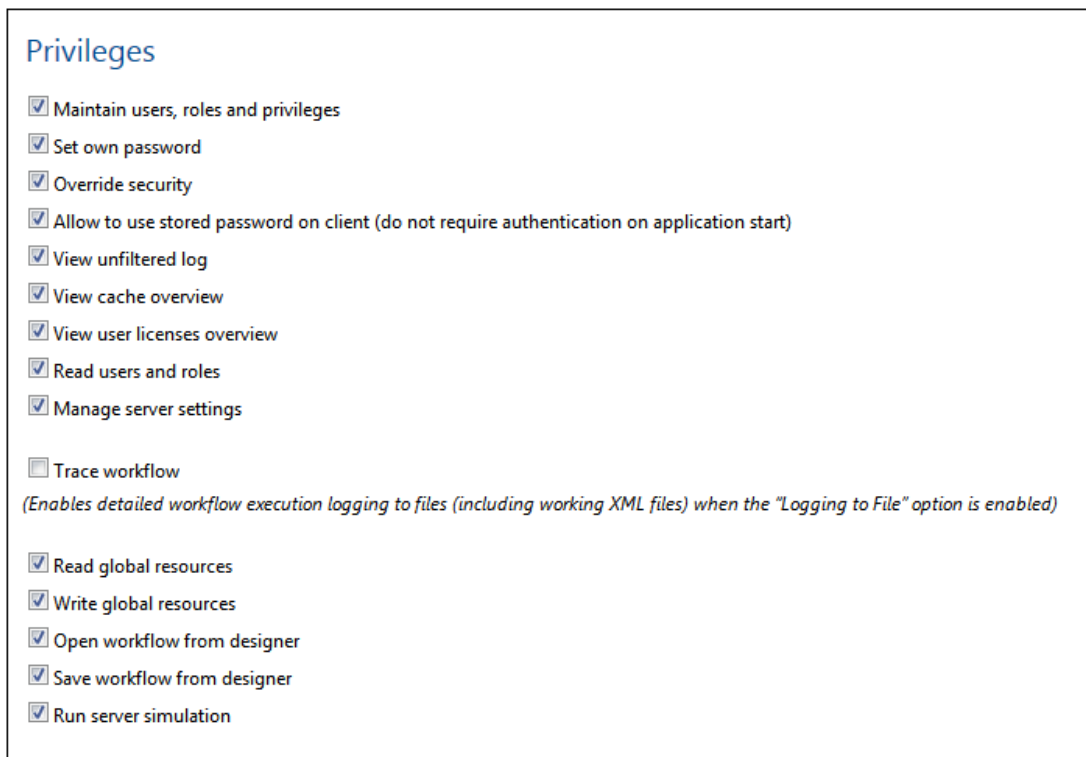
Two special users are predefined:

root	root is the initial administrator user. It is initially the most powerful user, having all privileges and having the ability to add other users and to set roles. Its initial name-password combination is: <code>root-root</code> . The password can be changed at any time.
anonymous	anonymous is an account for anonymous users that access services exposed via the HTTP service interface. It cannot be used for logging in top the Web UI, and it has no initial password.

▼ About Privileges

A privilege is an activity that a user is allowed to carry out. There is a fixed number of MobileTogether Server privileges, and a user can be assigned zero to all of the available privileges. It is, however, good practice to assign privileges via roles (*see next section*), rather than to assign privileges directly to the user. The assigning of privileges and roles to a user is done by a user that has been assigned this privilege. Initially, it is `root` user that has this privilege.

The screenshot below shows all the available privileges.



The tab [Users and Roles | Reports | Privileges Report](#) provides a list of all privileges, with each privilege being listed together with all the users/roles that have that privilege.

▼ About Roles

A role defines a set of privileges. It can be assigned to another role or to a user. A role's privileges automatically become the privileges of any other role or any user that the role is assigned to. A user can be assigned any number of roles. As a result, a user will have all the privileges defined in the multiple assigned roles.

The following roles are predefined:

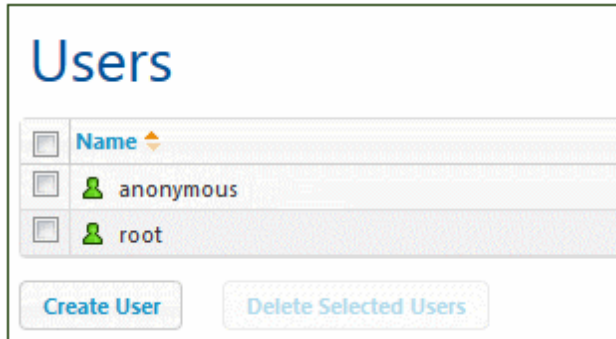
- `authenticated` is automatically assigned to every user **except** `anonymous`. So user with a name-and-password is assigned the `authenticated` role.
- `all` is automatically assigned to every user **including** `anonymous`.
- `workflow-designer` is assigned to users that design workflows in MobileTogether

Designer. This role allows a user to open and save workflows, as well as to run a simulation on the server.

- **workflow-user** is assigned to users running the workflow on a mobile device. This role allows the user to access the service interface without needing to log in to the server and start the solution on the client.

Users

The *Users and Roles | Users* tab (screenshot below) displays all users, and enables you to create new users, access a user's properties (by clicking a user name), and delete users.



▼ About Users

A user is defined by a name-and-password combination. Users access MobileTogether Server in two ways:

- *Web UI access:* The Web UI is the administrative interface of MobileTogether Server. Logging in to the Web UI requires a name-and-password combination; it is therefore done as a user.
- *Service interface:* The HTTP service interface exposes MobileTogether Server services, typically to the MobileTogether Client app on a mobile device. A user accesses the service interface, using a name-and-password combination. The services exposed relate typically to access to MobileTogether solutions and their related data.

Two special users are predefined:

root	root is the initial administrator user. It is initially the most powerful user, having all privileges and having the ability to add other users and to set roles. Its initial name-password combination is: root-root . The password can be changed at any time.
anonymous	anonymous is an account for anonymous users that access services exposed via the HTTP service interface. It cannot be used for logging in top the Web UI, and it has no initial password.

▼ About Privileges

A privilege is an activity that a user is allowed to carry out. There is a fixed number of MobileTogether Server privileges, and a user can be assigned zero to all of the available privileges. It is, however, good practice to assign privileges via roles (*see next section*), rather than to assign privileges directly to the user. The assigning of privileges and roles to a user is done by a user that has been assigned this privilege. Initially, it is **root** user that has this privilege.

The screenshot below shows all the available privileges.

Privileges

- Maintain users, roles and privileges
- Set own password
- Override security
- Allow to use stored password on client (do not require authentication on application start)
- View unfiltered log
- View cache overview
- View user licenses overview
- Read users and roles
- Manage server settings

- Trace workflow
(Enables detailed workflow execution logging to files (including working XML files) when the "Logging to File" option is enabled)

- Read global resources
- Write global resources
- Open workflow from designer
- Save workflow from designer
- Run server simulation

The tab [Users and Roles | Reports | Privileges Report](#) provides a list of all privileges, with each privilege being listed together with all the users/roles that have that privilege.

▼ About Roles

A role defines a set of privileges. It can be assigned to another role or to a user. A role's privileges automatically become the privileges of any other role or any user that the role is assigned to. A user can be assigned any number of roles. As a result, a user will have all the privileges defined in the multiple assigned roles.

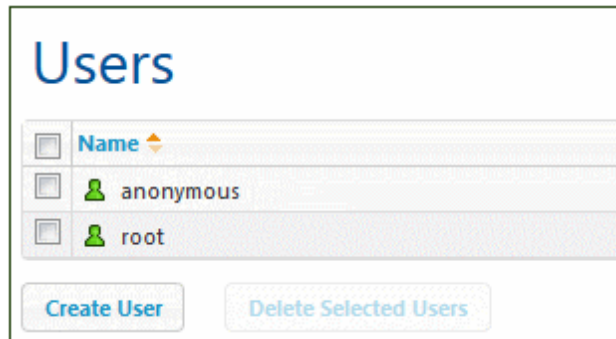
The following roles are predefined:

- **authenticated** is automatically assigned to every user **except** **anonymous**. So user with a name-and-password is assigned the **authenticated** role.
- **all** is automatically assigned to every user **including** **anonymous**.
- **workflow-designer** is assigned to users that design workflows in MobileTogether Designer. This role allows a user to open and save workflows, as well as to run a simulation on the server.
- **workflow-user** is assigned to users running the workflow on a mobile device. This role allows the user to access the service interface without needing to log in to the server and start the solution on the client.

▼ Creating a user

A new user can be created by `root` user or any user that has the *Maintain users, roles, and privileges* privilege. Create a new user as follows:

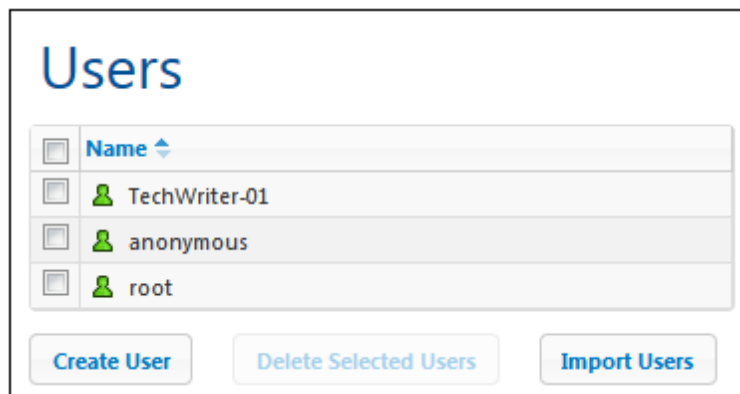
1. In the *Users and Roles / Users* tab, click **Create User** (see screenshot below). This displays the Create User page.



2. On the Create User page, enter a user name and password.
3. To assign privileges to the user, you can either select the privileges directly (by checking their check boxes), and/or assign roles to the user (see next section). A user will have privileges that are directly assigned plus those inherited from all assigned roles. We recommend using roles to assign privileges to a user (see next section).
4. Click **Save** to finish. The user now appears in the list of users (see screenshot above). You can edit a user's properties by clicking the user name in the list of users.

▼ Importing a user

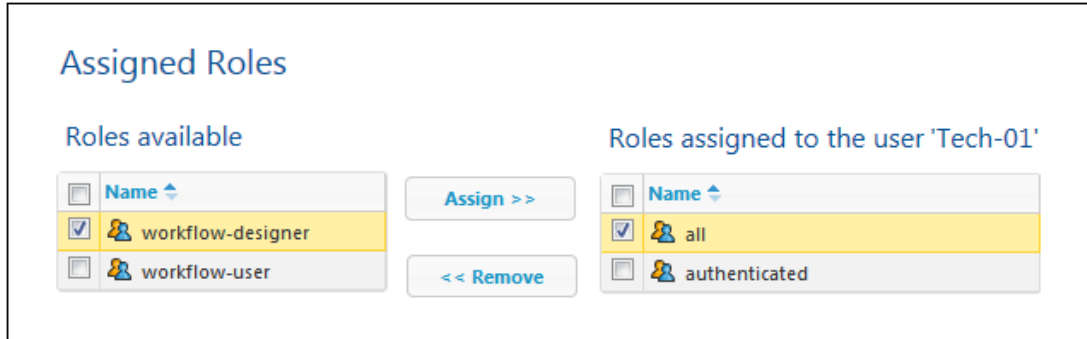
If [Active Directory login](#) has been enabled for a domain without automatically importing all users, you can import individual users of an enabled domain. Click **Import Users** (see screenshot below). In the Import Users dialog that is displayed, search for the user you want to import, select the user, and click **Import Selected**.



After the user is imported, you can assign roles to the user as for any other user. The new user can now log in to MobileTogether Server with the user's domain-specific user name and password.

▼ Assigning roles to a user

Roles can be assigned to a user on the user's Properties page. To access the user's Properties page, click the user name in the *Users and Roles / Users* tab. At the bottom of the user's Properties page is the Assigned Roles pane (screenshot below).

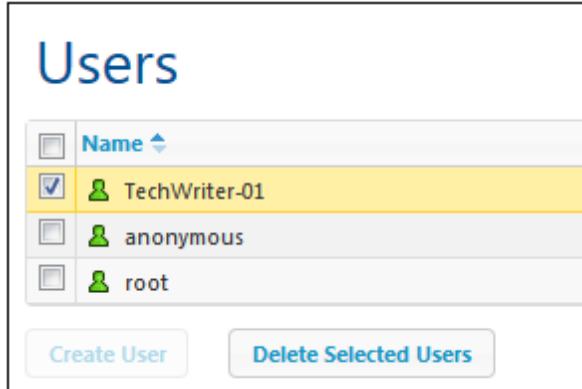


All available roles are listed on the left. All roles assigned to the user are listed on the right. Select the available role (in the list on the left) that you want to assign, and click **Assign**. To remove an assigned role, select it in the list on the right, and click **Remove**.

To see a listing of all the privileges of a user, go to [Users and Roles | Reports | Privileges by User](#).

▼ Deleting a user

A user can be deleted by `root` user or any user that has the *Maintain users, roles, and privileges* privilege. Delete a user as follows: In the *Users and Roles | Users* tab, select the user/s you want to delete (see screenshot below), click **Delete Selected Users**.

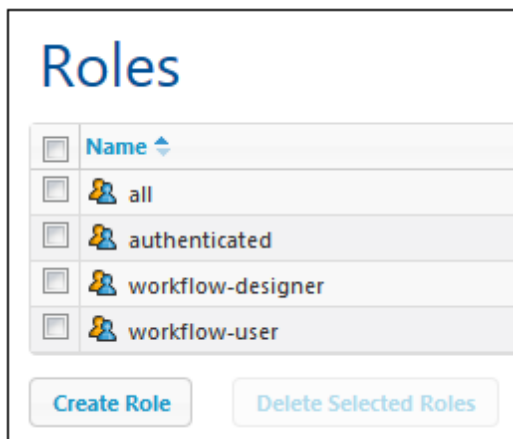


Roles

A role defines a set of privileges. It can be assigned to another role or to a user. A role's privileges automatically become the privileges of any other role or any user that the role is assigned to. A user can be assigned any number of roles. As a result, a user will have all the privileges defined in the multiple assigned roles.

The following roles are predefined:

- **authenticated** is automatically assigned to every user **except** **anonymous**. So user with a name-and-password is assigned the **authenticated** role.
- **all** is automatically assigned to every user **including** **anonymous**.
- **workflow-designer** is assigned to users that design workflows in MobileTogether Designer. This role allows a user to open and save workflows, as well as to run a simulation on the server.
- **workflow-user** is assigned to users running the workflow on a mobile device. This role allows the user to access the service interface without needing to log in to the server and start the solution on the client.

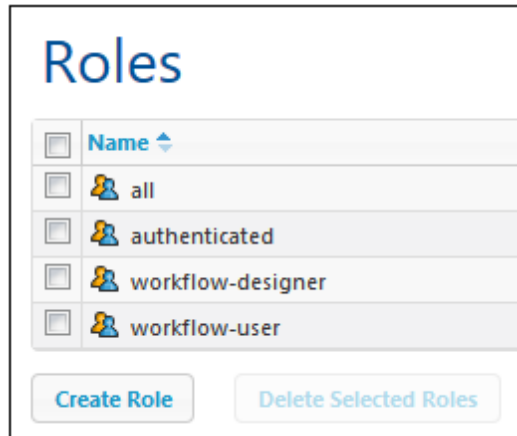


Via the *Users and Roles / Roles* tab, you can create new roles, edit the properties of roles, and assign roles to users and/or other roles. Click the name of a role to access its Properties page, where you can select/deselect privileges and assign the role to a user and/or other roles.

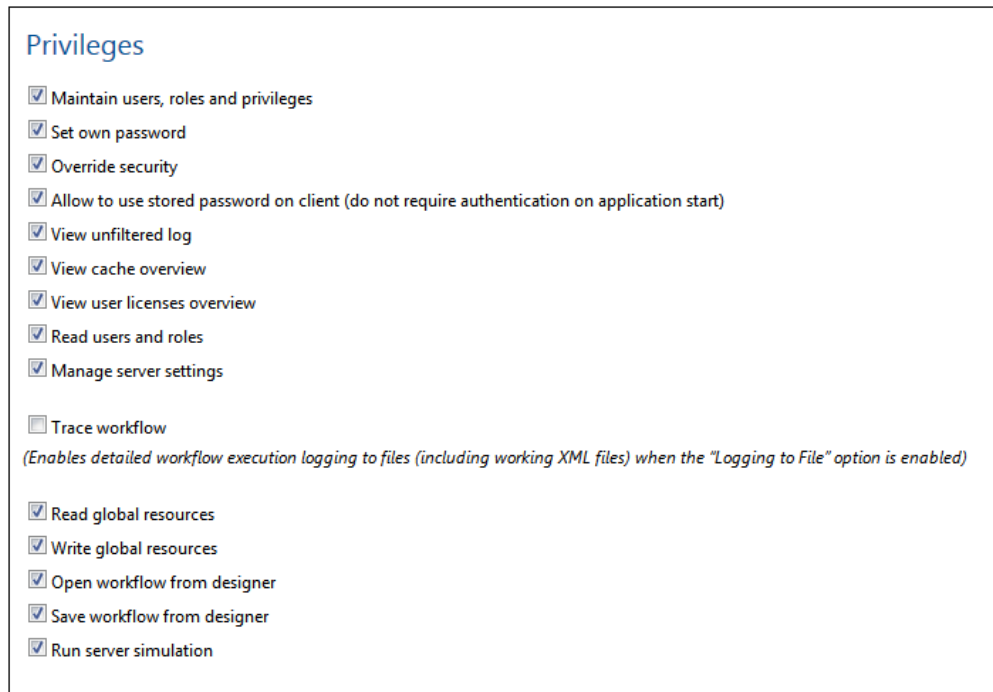
▼ Creating a role and defining its privileges

A new role can be created by `root` user or any user that has the *Maintain users, roles, and privileges* privilege. Create a new role as follows:

1. In the *Users and Roles / Roles* tab, click **Create Role** (see screenshot below). This displays the Create Role page.



2. On the Create Role page, give the role a name.
3. To define privileges for the role, select the privileges by checking their check boxes.



4. Click **Save** to finish.

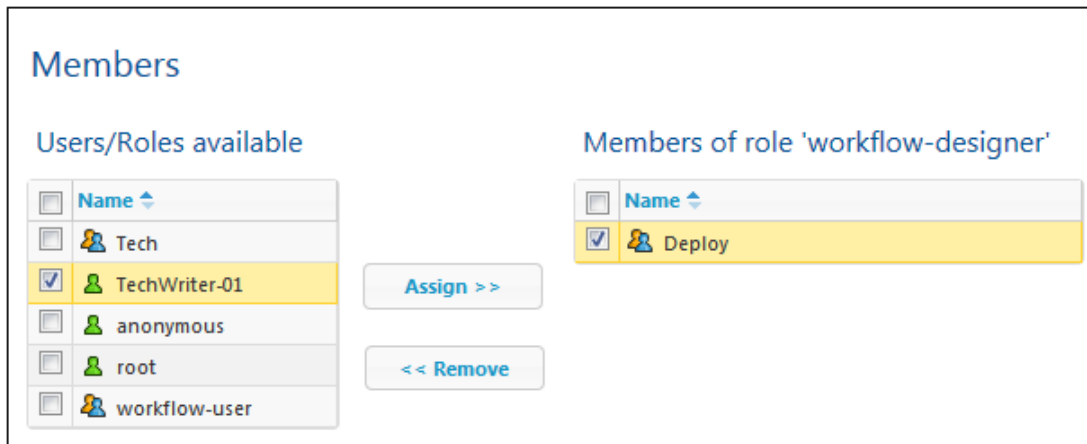
After you have saved the role, you can assign members to it in the Members pane at the bottom of the page (see *next section*). A member can be a user or another role. You can subsequently edit a role's properties by clicking the role's name in the list of roles in the *Users and Roles | Roles* tab.

To see a listing of all the privileges of a role, go to the tab, [Users and Roles | Reports | Privileges by User](#).

- ▼ Assigning members (users or other roles) to a role

Roles can have members, which can be either users or other roles. Members inherit the privileges of its parent role.

To assign a member to a role, go to the Members pane at the bottom of the role's Properties page (*screenshot below*).

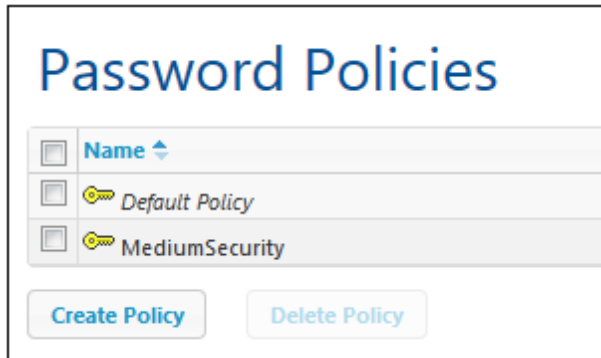


All available users/roles are listed on the left. All users/roles that are members of the role are listed on the right. Select the user/role (from the list on the left) that you want to assign as a member, and click **Assign**. To remove an assigned user/role, select it in the list on the right, and click **Remove**. The screenshot above, for example, shows the Members pane of the `workflow-designer` role. It has a single member, the role, `Deploy`, which will inherit all the privileges of the `workflow-designer` role.

Note that you can give a user or a role multiple sets of privileges. If a user/role is added as a member of multiple roles, it will inherit the privileges of all its parent roles. To see a listing of all the privileges of a user or role, go to the tab, [Users and Roles | Reports | Privileges by User](#).

Password Policies

A password policy defines the strength of passwords that use that policy. You can define your own password policies and apply different policies to different users. The *Users and Roles | Password Policies* tab (*screenshot below*) displays all defined password policies, enables you to create new policies, assign policies to users, and delete policies.

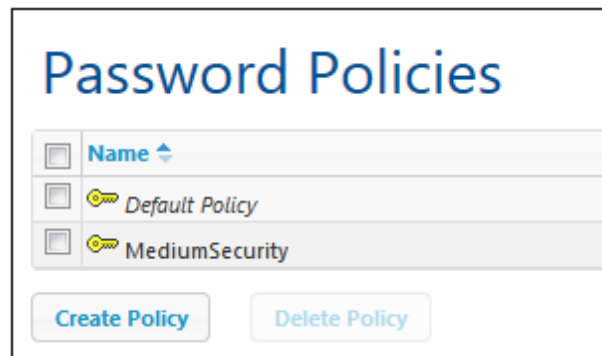


Note: By default every new user is assigned the **default password policy**, which does not define any constraint and cannot be changed. If you want users to have stronger passwords than defined by the default policy, create a strong policy and assign this policy to individual users.

▼ Creating a password policy

A new password policy can be created by `root` user or any user that has the *Maintain users, roles, and privileges* privilege. Create a new password policy as follows:

1. In the *Users and Roles | Password Policies* tab, click **Create Policy** (*see screenshot below*). This displays the Create Password Policy page.



2. On the Create Password Policy page, give the policy a name.
3. To define the constraints of the password, click the plus icon next to a constraint (*Total length; Letters; Digits*), and enter a value for the constraint (*see screenshot below*).

The screenshot shows the configuration page for a password policy named 'MediumSecurity'. The policy name is entered in a text field. Below, there are three rows for password requirements: 'Total length: must contain at least 8 characters', 'Letters: must contain at least 4 letters', and 'Digits:'. Each row has a numeric input field and a trash icon. A 'Save' button is at the bottom left.

4. Click **Save** to finish.

After you have saved the policy, you can assign users to it in the Members pane at the bottom of the page (see *next section*). You can subsequently edit a policy's properties by clicking its name in the list of policies in the *Users and Roles | Policies* tab.

▼ Assigning members (users) to a password policy

A password policy can be applied to a user by adding the user as a member of the policy in the Members pane at the bottom of the policy's Properties page (see *screenshot below*).

The screenshot shows the 'Members' pane for the 'MediumSecurity' policy. It is divided into two sections: 'Users available' and 'Members of policy 'MediumSecurity''. The 'Users available' section contains a table with columns 'Name' and 'Current Policy'. The 'Members of policy' section contains a list of members.

Name	Current Policy
<input checked="" type="checkbox"/> Default for new users	➡ null
<input type="checkbox"/> root	➡ null

Members of policy 'MediumSecurity':

Name
<input checked="" type="checkbox"/> TechWriter-01

All available users are listed on the left. All users that are members of the policy are listed on the right. Select the user that you want to assign as a member from the list on the left, and click **Assign**. To remove an assigned user, select it in the list on the right, and click **Remove**. The screenshot above, for example, shows the Members pane of the `MediumSecurity` policy. It has a single member, the user `TechWriter-01`.

Reports

The *Users and Roles | Reports* tab provides links to reports about privileges. These reports are useful summaries of what users/roles use what privileges.

▼ Privileges Report

The Privileges Report (*screenshot below*) lists each privilege together with all the users and roles that use that privilege. The inheritance is also displayed.

Privileges Report		
Privilege	Principal	Granted to and/or inherited from Principals
Allow to use stored password on client	root	granted to root
	workflow-user	granted to workflow-user
Maintain users, roles and privileges	TechWriter-01	granted to TechWriter-01
	root	granted to root
Manage server settings	TechWriter-01	granted to TechWriter-01
	root	granted to root
Open workflow from designer	Deploy	inherited from workflow-designer
	TechWriter-01	inherited from workflow-designer
	root	granted to root
	workflow-designer	granted to workflow-designer

▼ Privileges-by-User Report

The Privileges-by-User Report (*screenshot below*) lists each user/role with a summary of its privileges. The inheritance is also displayed.

Privileges by User Report		
Principal	Privilege	Granted to and/or inherited from Principals
Deploy	Open workflow from designer	inherited from workflow-designer
	Read global resources	inherited from workflow-designer
	Run server simulation	inherited from workflow-designer
	Save workflow from designer	inherited from workflow-designer
	Write global resources	inherited from workflow-designer
TechWriter-01	Maintain users, roles and privileges	granted to TechWriter-01
	Manage server settings	granted to TechWriter-01
	Open workflow from designer	inherited from workflow-designer
	Read global resources	inherited from workflow-designer

5.3 User Licenses

The **User Licenses** tab (*screenshot below*) displays license information about the devices currently connected to and licensed with MobileTogether Server, and enables licenses to be activated and deactivated.

ID	User Name	Device	Request Time	Active	Activation Time
5	root	{ Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0)	2014-04-14 13:41:00	<input checked="" type="checkbox"/>	2014-04-14 13:41:00
2	root	Samsung GT-I9000 (Android 2.3.3)	2014-04-10 12:11:14	<input checked="" type="checkbox"/>	2014-04-10 12:11:14

- A MobileTogether Server license allows a certain number of devices to communicate with the MobileTogether Server at any given time. This number is given in the *Licenses used* field. For example, in the screenshot above, the server is licensed to communicate with 8 devices. Two devices are connected, and both are licensed (indicated by their *Active* check boxes being selected). The *Licenses used* field therefore shows 2 out of 8 licenses used.
- Once a client device connects to the server, it will be assigned a license automatically if the *Licensing mode* option is set to *Auto* (see *screenshot above*). If this option is set to *Manual*, a newly connected mobile device is shown in the list of connected devices. It will be licensed only when an administrator checks the device's *Active* check box and clicks **Save**.
- Once the user license limit is reached, no more devices can be licensed. In order to license additional devices, an existing license must first be deactivated. An administrator can activate and deactivate devices at any time so that new devices can be licensed without exceeding the user license limit.

User license fields

Given below is a description of the fields of the user license tab.

- *Licensing mode*: *Auto* automatically activates a license for a newly connected device, provided one is free. *Manual* requires that the administrator manually activate a license for a device, and then save the setting for the activation to take effect.
- *ID*: The internal number assigned to the licensed device.
- *User Name*: The user name with which the client device made the connection and logged in. The user name determines the privileges that are extended to the client device.
- *Device*: The mobile device or browser that requested the license.
- *Active*: The *Active* check box is used to activate/deactivate a license. Click **Save** to finalize the change.
- *Request Time*, *Activation Time*: The times when a license is requested and activated,

respectively.

5.4 Log

The **Log** tab shows the logged actions according to the selected filters, located at the top of the tab (see *screenshot below*).

The screenshot shows the 'Log View' interface. At the top, there are filters for 'Show last 7 days' (selected), 'Show from 2014-04-07 to 2014-04-14', and 'Minimum severity: Info'. There are 'Delete All' and 'Delete' buttons. Below the filters is a search bar and a table of log entries. The table has columns for Date, User, Device, Design, Severity, and Message. The log entries include system events like 'License loaded from the LicenseServer.', 'Starting web server', and 'Stopping; canceling running tasks', as well as error messages about missing image files.

Date	User	Device	Design	Severity	Message
2014-04-14 11:	system			Info	License loaded from the LicenseServer.
2014-04-14 11:	system			Info	Starting web server
2014-04-14 11:	system			Info	Stopping; canceling running tasks
2014-04-13 02:	system			Error	Database: database is locked
2014-04-11 19:	system			Info	License loaded from the LicenseServer.
2014-04-11 19:	system			Info	Starting web server
2014-04-11 19:	system			Info	Stopping; canceling running tasks
2014-04-11 17:	root	2	/public/WidgetsSalesData	Error	Executed on server: Error loading image: 'Widgets Logo' (Deployable file 'http://www.altova.com/images/WidgetsHeader.png' does not exist.)
2014-04-11 17:	root	2	/public/WidgetsSalesData	Error	Executed on server: Error loading image: 'Image1' (Deployable file 'http://www.altova.com/images/WidgetsHeader.png' does not exist.)

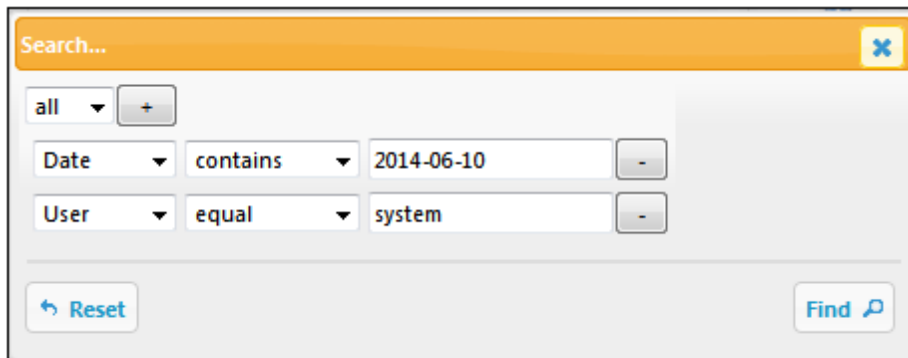
The view can be filtered by:

- **Date:** Ranges or specific dates can be set.
- **Minimum severity:** Errors is the highest severity (only errors are shown); Warnings is next (errors and warnings are shown); Info is the lowest severity, and shows errors, warnings, and info.
- **Search criteria:** Click the **Search** button at the top or bottom left of the log table to open the Search dialog (*described below*). To remove the filter defined by the search criteria, click the **Reload Grid** icon next to the **Search** button.

Logs can be deleted by clicking the **Delete All** button at the top of the tab, or by defining a date range and clicking **Delete**.

Searching for log messages

To access the Search dialog (*screenshot below*), click the **Search** button at the top or bottom left of the log table (see *screenshot above*).



The screenshot shows a search filter interface. At the top is an orange header bar with the text "Search..." and a close button (X). Below the header, there is a selector for "all" with a plus button. Two search rules are defined: "Date contains 2014-06-10" and "User equal system". Each rule has a minus button to delete it. At the bottom, there are "Reset" and "Find" buttons.

For each search rule, select a field (such as *Date* or *User*), an operator (such as *contains* or *equals*), and the value to search for. Add a new search rule by clicking the **Add Rule** button. Delete a search rule by clicking its **Delete Rule** button. The **all** selector at the top specifies that the search condition is fulfilled only when all the search rules are individually fulfilled. The **any** selector specifies that the search condition is fulfilled if any one search rule is fulfilled. Click **Find** to start the search. Click **Reset** to remove the search filter.

5.5 Cache

The **Cache** tab displays the details of caches that are currently available on the server. A cache is a data file that is generated from a data source of a design at a given time. In the Web UI of MobileTogether Server, you can see details about the caches on the server, activate/deactivate caches, and delete caches.

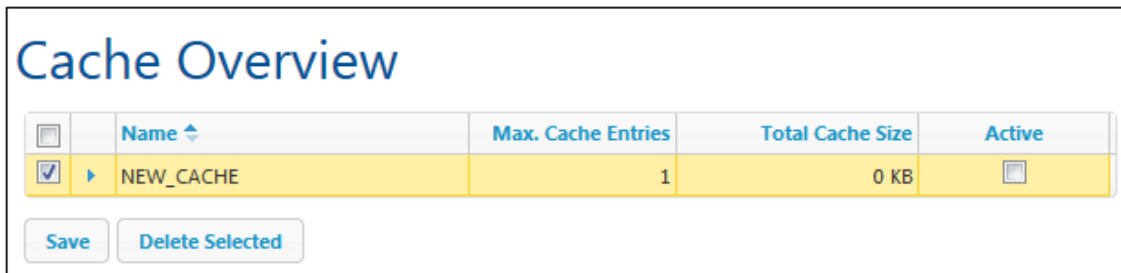
Creating caches

A new cache is defined in MobileTogether Designer for a data source. Right-click a data source in the Page Sources window, select **Cache Settings**, and specify the properties of the cache. There are two main reasons to create caches: (i) If a page data source generates reports slowly (for example, a large database); (ii) If a data source is not modified often. In such cases, execution of a solution would be faster if data is taken from data caches on the server. In order to keep caches up-to-date, the frequency of cache updates can be specified when the cache is created. Once a cache has been defined in MobileTogether Designer, it can be used by the data sources of different designs, providing the underlying data structure is compatible.

If a data source is defined as having a cache, the cached data will be used when the solution is run. Caches can be used as soon as the solution has been deployed to the server.

Details displayed and available actions

In the Cache tab you can see all caches available on the server, activate or deactivate individual caches, save any change to the active/inactive status of a cache, and delete selected caches.



<input type="checkbox"/>	Name ↕	Max. Cache Entries	Total Cache Size	Active
<input checked="" type="checkbox"/>	NEW_CACHE	1	0 KB	<input type="checkbox"/>

Save Delete Selected

- *Name:* Names are given at the time a cache is defined in MobileTogether Designer and cannot be changed in MobileTogether Server. The same cache can be used in multiple designs if the referenced data structure is compatible. Assigning caches to different designs is done in MobileTogether Designer. See the <http://manual.altova.com/MobileTogether/mobiletogetherdesigner/index.html> for more information.
- *Max. Cache Entries:* A cache can be created by using a set of parameters. Each set of parameters generates one cache entry, and if different sets of parameters are specified, multiple cache entries will be created. When defining a cache, the maximum number of cache entries can be specified so that an upper limit is placed on the amount of server space that is used for the caches of a particular data source. specify parameters. This number specifies how many cache entries will be stored before the first cache entry is purged and the latest cache entry is appended.

- *Total Cache Size*: This is the total size (for all cache entries) allocated to the cache on the hard disk (or other medium). Cache size is automatically allocated.
- *Active*: This check box lets you activate or deactivate a cache on the server. When a cache is deactivated, its metadata (properties) still exists on the server but the cache is emptied and it is not available. Click **Save** to confirm the setting.
- To delete a cache from the server, select it and click **Delete Selected**. If the cache has been defined to be updated periodically, a new cache will be generated at the next update time.

5.6 Settings

The **Settings** tab is divided into a *General Settings* pane and a *LicenseServer* pane. The *General Settings* pane contains sub-panes for various MobileTogether Server settings. These sub-panes and the LicenseServer pane are described separately below. After changing any setting in the *General Settings* pane, click **Save** for the setting to take effect.

▼ Host settings

Specifies whether the server will use a specific IP address or all interfaces and IP addresses. If a single IP address is to be used, enter it in the *Only the following IP address* field.

Host settings:
Select the network adapters the server will use.
 All interfaces and assigned IP addresses
 Only the following IP address:

▼ Mobile client ports

The ports that mobile devices will use to connect to the server. The HTTP port is the unsecure port; HTTPS is the secure port. To use HTTPS, you need to set up [SSL Encryption](#).

Mobile client ports:
Select unsecure (HTTP) and secure (HTTPS) ports the Mobile clients will use.
These ports cannot be used for administrative purposes!
 HTTP Port:
 HTTPS Port:

▼ Administrator ports

The administrator ports provide access for the following purposes:

- To connect to the server's Web UI and perform administrative functions, such as setting up [Users and Roles](#).
- To deploy MobileTogether designs (as MobileTogether solutions) to the server. MobileTogether Designer has a setting that specifies the address and port of the MobileTogether Server to which to deploy designs.

Administrator ports:

Select unsecure (HTTP) and secure (HTTPS) ports to be used by the administrator. These ports can be used for server configuration, user, role, and user license administration, workflow deployment and workflow simulation.

HTTP Port:

HTTPS Port:

The HTTP port is the unsecure port; HTTPS is the secure port. To use HTTPS, you need to set up [SSL Encryption](#).

▼ **SSL certificates**

Specifies the private key certificate and public key certificate to use for SSL communication. Click **Browse**, and select the files containing the certificates (*Private Key* for private key, and *Certificate* for public key). See [Setting Up SSL Encryption](#) for more information.

SSL certificates:

Select the private key and the certificate needed for secure (SSL) communication. A valid private key and certificate must be supplied in order to use secure (HTTPS) ports. The private key/certificate must be in PEM format.

Private Key:

No file selected.

Certificate:

No file selected.

▼ **Logging**

Logs contain reports of workflow activity, and they are displayed in the Log tab of the Web UI. The settings in this pane define logging parameters.

Logging

Logging level detail:
 ▼
 Select logging detail you want to use during a workflow execution. Logs are, by default, stored in the database and are accessible via [Log](#) page.

Log Limit: day(s)

Logging to file
 Enable workflow execution logging to file for users granted the *Trace workflow* privilege. Log files contain detailed workflow execution information, including working XMLs.

Logging to file directory:

 Specify the server side directory where log files will be placed.

- *Logging level detail:* The detail can vary from logging only errors, through logging errors and warnings, and (most detailed) logging errors, warnings, and information.
- *Log limit:* Specifies for how long logs are kept.
- *Log files:* Users that have been granted *Trace workflow* privileges can have logs saved to file if the *Logging to file* option is selected. The directory where logs are saved is specified in the *Logging to file directory* option.

▼ **Workflow simulation on server**

Activating the check box allows workflow simulations to be performed on the server for users granted the *Run server simulation* privilege.

Workflow simulation on server:

Enable workflow simulation on the server for users granted the *Run server simulation* privilege.

Simulation on server

▼ **Workflow execution**

Activating the check box allows workflow execution to be performed from web browsers.

Workflow execution:

Enable workflow execution from web browsers.

Workflow execution from web browsers

▼ Sessions

Sets the timeout period in minutes before a new logon has to be performed.

Sessions:
The expiration timeout (in minutes) for the stored session data.
Session timeout: min(s)

▼ Server side solution's working directory

When solutions are run on the server, this setting specifies the following:

- The base URI of all relative paths in the design. In a design, the paths of all files that are not deployed to the server will be resolved relative to the directory specified in this setting. For example, if a file in the design is addressed with a relative path of `MTSData\Test.xml`, then, if the file is not deployed, it must be located at: `<Working-Directory-Setting-Of-Server>MTSData\Test.xml`. (If the file is deployed to the server, the design uses internal mechanisms to access the files.)
- If, in the design, the file's location is given by an absolute path, then this path must point to a location inside a directory that is a sub-directory of the Working Directory specified in this setting. For example, if the file is addressed with the absolute path: `C:\MTSData\Test.xml`, then the file will be accessed only if the Working Directory is `C:\` or `C:\MTSData`.

Server side solution's working directory:
Directory:

Specify the server side directory where solution's files can be saved. It is also used as the base for resolving solution's relative paths.

The Working Directory setting, in effect, restricts any read/write access to local files during execution of solutions. Only files inside the Working Directory or any of its sub-directories can be accessed by MobileTogether Server for the execution of solutions.

▼ Cache settings

Specifies: (i) the directory where cache files are saved, (ii) the timeout for each cache operation, and (iii) the duration in days for how long cache log items are displayed. See the [Cache tab](#) for more information.

Cache settings:

Cache directory:

 Specify the server side directory where cached files will be placed.

Cache operation timeout: sec(s)
 Timeout (in seconds) for each cache operation. '0' means infinite.

Cache Log Limit: day(s)

▼ **Active Directory login**

Enables users to log in to the server with their domain-specific user names and passwords. Each domain-specific user can be imported as a user in the [Users](#) tab, and then be assigned roles or privileges in the usual way. In the Options dialog of MobileTogether Designer, the type of user login for connecting to the server can be specified: either as a direct server-defined user or as a domain user.

After enabling Active Directory login, enter the domain or domains you wish to allow. Then go to the [Users and Roles | Users](#) tab to import specific users as MobileTogether Server users. These users can now use their domain-specific login information to log in to MobileTogether Server.

Active Directory login:

Enable
 Enable Active Directory login.

Allow any existing domain user to login
 If unchecked, use "Import Domain Users" button on "User licenses" page to allow specific domain users to login.
 Note: Even if any domain user may login, you can use workflow permissions to control access to specific workflows.

Domain suffixes:
 The list of comma-separated domain names used for login to the server.

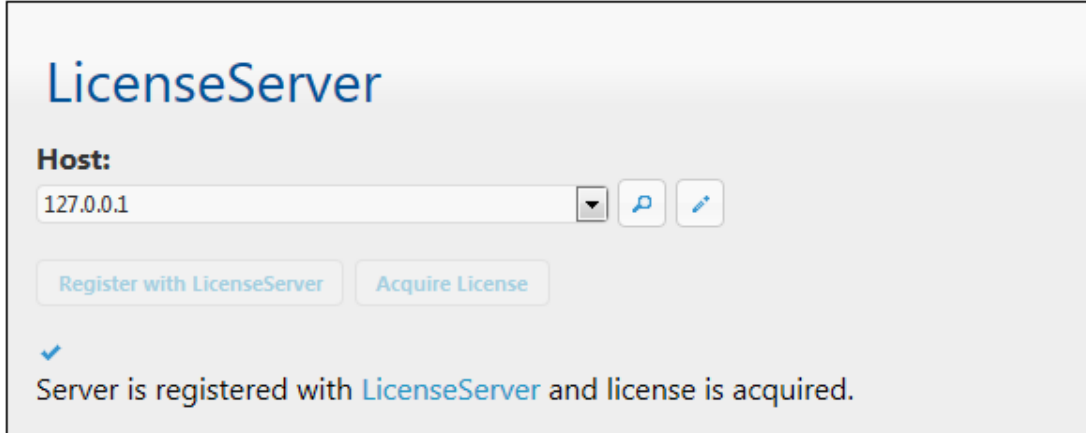
Set as default
 Forces Active Directory login providers to be at the beginning of the providers list.

- *Allow any existing domain user to log in:* All users in the domain can log in to MobileTogether Server. If unchecked, domain users will need to be imported individually as MobileTogether Server users. This import is done via the **Import Users** button of the [Users](#) tab.

- *Domain suffixes:* Enter the domains to include, separating domains from one another with a comma.

▼ LicenseServer

MobileTogether Server must be registered with an Altova LicenseServer on your network. The LicenseServer settings specify the LicenseServer machine to connect to, and enables you to register MobileTogether Server with LicenseServer. See the section, [Setting Up MobileTogether Server](#) for information about licensing.



LicenseServer

Host:

127.0.0.1

Register with LicenseServer Acquire License

✓
Server is registered with LicenseServer and license is acquired.

- To search for LicenseServers on your network, click the **Search** button. The detected LicenseServers are listed in the dropdown list of the combo box. From this list, select the LicenseServer that you wish to connect to.
- To enter a server address, click the **Address** button, and enter the server address.

When the LicenseServer is found, **Register with LicenseServer** becomes enabled. Click the button to register MobileTogether Server with LicenseServer. Click **Acquire License** to go to LicenseServer and assign a license to MobileTogether Server.

Chapter 6

Altova LicenseServer

6 Altova LicenseServer

Altova LicenseServer (hereafter also called **LicenseServer** for short) provides a central location for the management of licenses for Altova products. Altova applications running in a network can have licenses assigned to them from the LicenseServer, thus giving administrators the flexibility to manage and monitor licenses.

Current version: 1.13

Licensing process with Altova LicenseServer

To assign an Altova server product a license via Altova LicenseServer, you need to do the following:

1. [Start LicenseServer](#)
2. Open the [LicenseServer Configuration page](#), which is the Web UI of LicenseServer, on [Windows](#), [Linux](#), or [Mac OS X](#).
3. [Upload the license/s](#) you have received from Altova to LicenseServer. Do this in the [License Pool](#) tab of the Configuration page.
4. Register Altova server products ([FlowForce Server](#), [MapForce Server](#), [StyleVision Server](#), [RaptorXML\(+XBRL\) Server](#)) with LicenseServer.
5. [Assign licenses](#) to Altova server In the [Server Management](#) tab of the Configuration page.

Licenses can thereafter be conveniently monitored and managed centrally with LicenseServer. See the [Configuration Page Reference](#) for available functionality.

Note: The [LicenseServer Configuration page](#) does not support SSL.

▼ LicenseServer versions and their compatibility with Altova server products

New versions of Altova server products can only be licensed with the version of LicenseServer that is the latest at the time of the server product's release. However, older versions of Altova server products will work with newer versions of LicenseServer.

So, if you are installing a new version of an Altova server product and if your current LicenseServer version is not the latest, de-install this older version and install the latest version available on the Altova website. All registration and licensing information held in your older version of LicenseServer will be saved at the time of de-installation to a database on your server machine, and will be imported automatically into the newer version. When you install a newer version of LicenseServer, the older version will be de-installed before the newer version is installed.

The version number of the currently installed LicenseServer is given at the bottom of the [LicenseServer configuration page](#) (all tabs).

Current version: 1.13

About this documentation

This documentation is organized into the following parts:

- Introductory information about: [network requirements](#); installation on [Windows](#), [Linux](#), and [Mac OS X](#); and [Altova ServiceController](#).
- [How to Assign Licenses](#), which describes in a step-by-step way how to assign licenses with Altova LicenseServer.
- [Configuration Page Reference](#): A description of the administrator's interface with LicenseServer.

Last updated: 11-10-2014

6.1 Network Information

Altova LicenseServer must be installed on a server machine that is accessible by all clients running Altova products that require a license. Any firewall on both the client and server must allow the network traffic to and from the LicenseServer that is necessary for the LicenseServer to operate correctly.

On the LicenseServer machine, **port 35355** is used to distribute licenses, and therefore it must be open for network traffic with client machines.

The following are the default networking parameters and requirements of LicenseServer:

- *For LicenseServer license distribution:*
Either one or both of
IPv4 TCP connection on port 35355
IPv6 TCP connection on port 35355

For administrative tasks, the LicenseServer is accessed by a web interface that uses port 8088. The port used can be [configured to suit your requirements](#).

Connection to the Master Licensing Server at altova.com

The Altova LicenseServer needs to be able to communicate with the Master Licensing Server at altova.com to validate and authenticate license-related data and to ensure continuous compliance with the Altova license agreements. This communication occurs over HTTPS using port 443. If the Altova LicenseServer, after making the initial verification with the altova.com Master Licensing Server, is unable to again connect with altova.com for a duration of more than 5 days (= 120 hours), then the Altova LicenseServer will no longer permit the usage of any Altova software products connected to the Altova LicenseServer.

Any such loss of connection with the altova.com master servers will be logged in the [Messages tab](#) of the [Configuration page of the Altova LicenseServer](#). In addition, the administrator can configure the Altova LicenseServer to automatically send an alert email when the connection to altova.com is lost. Alert Mail settings are available in the [Settings tab](#) of the [Configuration page](#).

6.2 Installation (Windows)

Altova LicenseServer can be installed on Windows systems in one of two ways:

- As an independent installation.
- As part of an Altova server product installation. (Altova server products are: Altova FlowForce Server, Altova MapForce Server, Altova StyleVision Server, Altova RaptorXML(+XBRL), and Altova MobileTogether Server.)

If LicenseServer is not installed on your system at the time an Altova server product is installed, the option to install LicenseServer is selected by default during installation setup. If LicenseServer is already installed, the option to install it is deselected by default. You can change the default option if you like.

For information about how to proceed with assigning licenses, see the section [How to Assign Licenses](#).

▼ LicenseServer versions and their compatibility with Altova server products

New versions of Altova server products can only be licensed with the version of LicenseServer that is the latest at the time of the server product's release. However, older versions of Altova server products will work with newer versions of LicenseServer.

So, if you are installing a new version of an Altova server product and if your current LicenseServer version is not the latest, de-install this older version and install the latest version available on the Altova website. All registration and licensing information held in your older version of LicenseServer will be saved at the time of de-installation to a database on your server machine, and will be imported automatically into the newer version. When you install a newer version of LicenseServer, the older version will be de-installed before the newer version is installed.

The version number of the currently installed LicenseServer is given at the bottom of the [LicenseServer configuration page](#) (all tabs).

Current version: 1.13

The version number of the LicenseServer that is appropriate for any particular version of a server product is displayed during the installation of that version of the server product. You can choose to install this version of LicenseServer along with the server product, or you can install the newer version of LicenseServer separately. In both cases, the installer will automatically de-install the previous version and install the new version.

6.3 Installation (Linux)

Altova LicenseServer can be installed on Linux systems (Debian, Ubuntu, CentOS, RedHat).

Uninstalling old versions of LicenseServer

On the Linux command line interface (CLI), you can check whether LicenseServer is installed with the following command:

```
[Debian, Ubuntu]:  dpkg --get-selections | grep altova
[CentOS, RedHat]:  rpm -qa | grep server
```

If LicenseServer is not installed, go ahead with the installation as documented in the next steps. If LicenseServer is installed and you wish to install a newer version of it, uninstall the old version with the command:

```
[Debian, Ubuntu]:  sudo dpkg --remove licenseserver
[CentOS, RedHat]:  sudo rpm -e licenseserver
```

Installing Altova LicenseServer

On Linux systems, LicenseServer must be installed independently of other Altova server products. It is not included as part of the installation packages of Altova server products. Download Altova LicenseServer from the [Altova website](#) and copy the package to any directory on the Linux system.

Distribution	Installer extension
Debian	.deb
Ubuntu	.deb
CentOS	.rpm
RedHat	.rpm

In a terminal window, switch to the directory where you have copied the Linux package. For example, if you copied it to a user directory called `MyAltova` (that is located, say, in the `/home/User` directory), then switch to this directory as follows:

```
cd /home/User/MyAltova
```

Install LicenseServer with the following command:

```
[Debian]:  sudo dpkg --install licenseserver-1.13-debian.deb
[Ubuntu]:  sudo dpkg --install licenseserver-1.13-ubuntu.deb
[CentOS]:  sudo rpm -ivh licenseserver-1.13-1.x86_64.rpm
```



```
[RedHat]: sudo rpm -ivh licenseserver-1.13-1.x86_64.rpm
```

The LicenseServer package will be installed in:

```
/opt/Altova/LicenseServer
```

For information about how to proceed with assigning licenses, see the section [How to Assign Licenses](#).

▼ **LicenseServer versions and their compatibility with Altova server products**

New versions of Altova server products can only be licensed with the version of LicenseServer that is the latest at the time of the server product's release. However, older versions of Altova server products will work with newer versions of LicenseServer.

So, if you are installing a new version of an Altova server product and if your current LicenseServer version is not the latest, de-install this older version and install the latest version available on the Altova website. All registration and licensing information held in your older version of LicenseServer will be saved at the time of de-installation to a database on your server machine, and will be imported automatically into the newer version. When you install a newer version of LicenseServer, the older version will be de-installed before the newer version is installed.

The version number of the currently installed LicenseServer is given at the bottom of the [LicenseServer configuration page](#) (all tabs).

Current version: 1.13

6.4 Installation (Mac OS X)

Altova LicenseServer can be installed on Mac OS X systems (version 10.7 or higher). Since you might need to uninstall a previous version, uninstalling is described first.

Uninstalling old versions of LicenseServer

Before uninstalling LicenseServer, stop the service with the following command:

```
sudo launchctl unload /Library/LaunchDaemons/com.altova.LicenseServer.plist
```

To check whether the service has been stopped, open the Activity Monitor terminal and make sure that LicenseServer is not in the list.

In the Applications terminal, right-click the LicenseServer icon and select **Move to Trash**. The application will be moved to Trash. You will, however, still need to remove the application from the `usr` folder. Do this with the command:

```
sudo rm -rf /usr/local/Altova/LicenseServer
```

Installing Altova LicenseServer

Download Altova LicenseServer from the [Altova website](#) (the installer file has a `.pkg` file extension), and double-click the installer package to start the installation. Follow the on-screen instructions. You will need to accept the license agreement for installation to proceed.

The LicenseServer package will be installed in the folder:

```
/usr/local/Altova/LicenseServer
```

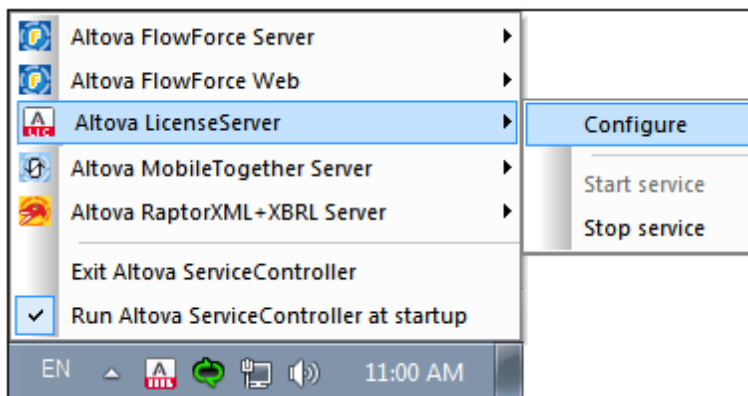
6.5 Altova ServiceController

Altova ServiceController (ServiceController for short) is an application for conveniently starting, stopping and configuring Altova services **on Windows systems**.

ServiceController is installed with Altova LicenseServer and with *Altova server products that are installed as services* (FlowForce Server, RaptorXML(+XBRL) Server, and Mobile Together Server). It can be started by clicking **Start | Altova LicenseServer | Altova ServiceController**. (This command is also available in the **Start** menu folders of *Altova server products that are installed as services* (FlowForce Server, RaptorXML(+XBRL) Server, and Mobile Together Server).) After ServiceController has been started, it can be accessed via the system tray (*screenshot below*).



To specify that ServiceController starts automatically on logging in to the system, click the **ServiceController** icon in the system tray to display the **ServiceController** menu (*screenshot below*), and then toggle on the command **Run Altova ServiceController at Startup**. (This command is toggled on by default.) To exit ServiceController, click the **ServiceController** icon in the system tray and, in the menu that appears (*see screenshot below*), click **Exit Altova ServiceController**.



Starting and stopping Altova services

Each installed Altova service component will have an entry in the ServiceController menu (*see screenshot above*). An Altova service can be started or stopped via a command in its ServiceController sub-menu. Additionally, important administration tasks of individual services can be accessed via the ServiceController menu. In the screenshot above, for example, Altova LicenseServer service has a sub-menu in which you can choose to access LicenseServer's Configuration page via the **Configure** command.

6.6 How to Assign Licenses

To assign an Altova server product a license using Altova LicenseServer, do the following:

1. [Start LicenseServer](#)
2. Open the [LicenseServer Configuration page](#), which is the administrator's interface with LicenseServer, on [Windows](#), [Linux](#), or [Mac OS X](#).
3. [Upload the license/s](#) you have received from Altova to the license pool of your Altova LicenseServer. Do this in the [License Pool](#) tab of the LicenseServer Configuration page.
4. Register the Altova server product ([FlowForce Server](#), [MapForce Server](#), [StyleVision Server](#), [RaptorXML\(+XBRL\) Server](#)) with LicenseServer. Depending on the product's type, the method of registering it with LicenseServer will be different: either via the product's Web UI or its command line. See the documentation of your Altova server product for additional information.
5. In the [Server Management](#) tab of the [LicenseServer Configuration page](#), [assign a license](#) to the Altova server product according to the number of cores on the product machine.

Note on cores and licenses

The licensing of Altova server products, *except MobileTogether Server****, is based on the number of processor cores available on the product machine. For example, a dual-core processor has two cores, a quad-core processor four cores, a hexa-core processor six cores, and so on. The number of cores licensed for a product on a particular server machine must be greater than or equal to the number of cores available on that server, whether it's a physical or virtual machine.

For example, if a server has eight cores (an octa-core processor), you must purchase at least an 8-core license. You can also combine licenses to achieve the core count. So, two 4-core licenses can also be used for an octa-core server instead of an 8-core license.

If you are using a computer server with a large number of CPU cores but only have a low volume to process, you may also create a virtual machine that is allocated a smaller number of cores, and purchase a license for that number. Such a deployment, of course, will have less processing speed than if all available cores on the server were utilized.

Note: Each license can be used for only one client machine at a time, even if it has unused licensing capacity. For example, if a 10-core license is used for a client machine that has 6 CPU cores, then the remaining 4 cores of the license cannot be used simultaneously for another client machine.

*** MobileTogether Server licenses are assigned on the basis of the number of users, that is, the number of client devices that connect to MobileTogether Server.

Start LicenseServer

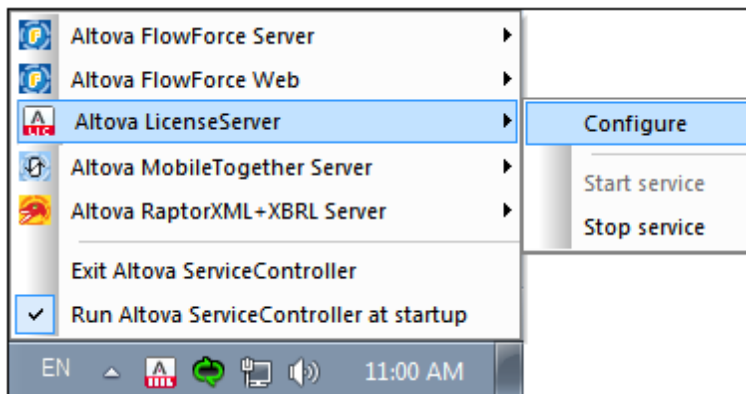
This section:

- How to start LicenseServer on [Windows systems](#)
- How to start LicenseServer on [Linux systems](#)
- How to start LicenseServer on [Mac OS X systems](#)
- Note about [Connection to altova.com](#)

Windows systems

You can start LicenseServer via the Altova ServiceController, which is available in the system tray.

First, click **Start | All Programs | Altova LicenseServer | Altova ServiceController** to start Altova ServiceController and display its icon in the system tray (see *screenshot below*). If you select the *Run Altova ServiceController at Startup* option, Altova ServiceController will start up on system start and its icon will be available in the system tray from then onwards.



To start LicenseServer, click the Altova ServiceController icon in the system tray, hover over **Altova LicenseServer** in the menu that pops up (see *screenshot below*), and then select **Start Service** from the LicenseServer submenu. If LicenseServer is already running, the *Start Service* option will be disabled.

Linux systems

To start LicenseServer as a service on Linux systems, run the following command in a terminal window.

```
[Debian]:          sudo /etc/init.d/licenseserver start
[Ubuntu]:          sudo initctl start licenseserver
[CentOS]:          sudo initctl start licenseserver
[RedHat]:          sudo initctl start licenseserver
```

(If you need to stop LicenseServer, replace **start** with **stop** in the above command.)

Mac OS X systems

To start LicenseServer as a service on Mac OS X systems, run the following command in a terminal window:

```
sudo launchctl load /Library/LaunchDaemons/com.altova.LicenseServer.plist
```

If at any time you need to stop LicenseServer, use:

```
sudo launchctl unload /Library/LaunchDaemons/com.altova.LicenseServer.plist
```

Connection to the Master Licensing Server at altova.com

The Altova LicenseServer needs to be able to communicate with the Master Licensing Server at altova.com to validate and authenticate license-related data and to ensure continuous compliance with the Altova license agreements. This communication occurs over HTTPS using port 443. If the Altova LicenseServer, after making the initial verification with the altova.com Master Licensing Server, is unable to again connect with altova.com for a duration of more than 5 days (= 120 hours), then the Altova LicenseServer will no longer permit the usage of any Altova software products connected to the Altova LicenseServer.

Any such loss of connection with the altova.com master servers will be logged in the [Messages tab](#) of the [Configuration page of the Altova LicenseServer](#). In addition, the administrator can configure the Altova LicenseServer to automatically send an alert email when the connection to altova.com is lost. Alert Mail settings are available in the [Settings tab](#) of the [Configuration page](#).

Open LicenseServer's Config Page (Windows)

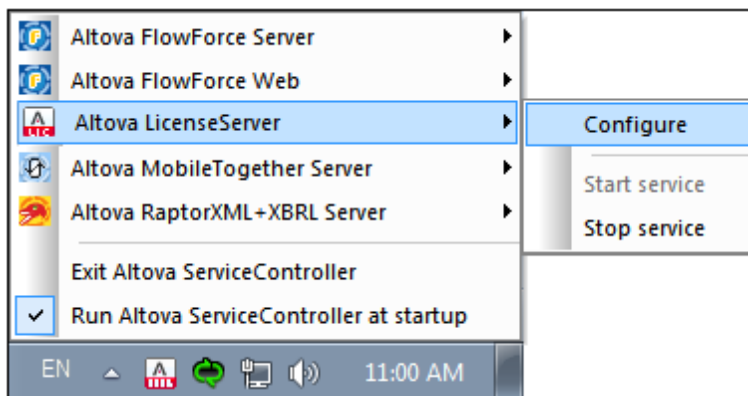
This section:

- [Opening the Configuration page if LicenseServer is on the same machine](#)
- [Opening the Configuration page if LicenseServer is on another machine](#)
- [Logging in with the initial password](#)
- [Setting a fixed port for the Configuration page](#)

Opening the Configuration page if LicenseServer is on the same machine

On Windows systems, if LicenseServer is on the same machine, you can open the [Configuration page](#) of LicenseServer in one of two ways:

- Click **Start | All Programs | Altova LicenseServer | LicenseServer Configuration Page**. The Configuration page opens in a new tab of your Internet browser.
- Click the Altova ServiceController icon in the system tray, mouse over **Altova LicenseServer** in the menu that pops up (see *screenshot below*), and then select **Configure** from the LicenseServer submenu.



The [Configuration page](#) opens in a new browser window, and its login mask is displayed (*screenshot below*).

Opening the Configuration page if LicenseServer is on another machine

To open the LicenseServer [Configuration page](#) from some other Windows machine on the local network (than that on which LicenseServer is installed), enter the URL of the LicenseServer [Configuration page](#) in the address bar of a browser and press **Enter**. By default, the URL of the Configuration page will be:

```
http://<serverIPAddressOrName>:8088/
```

The URL is present in the HTML code of the Configuration page itself, which is named `webUI.html` and is located at:

```
C:/ProgramData/Altova/LicenseServer/WebUI.html
```

If you have [set the URL of the Configuration page](#) to be generated dynamically (in the Settings tab of the Configuration page), then a new URL is generated each time LicenseServer is started. You will need to check the current version of `webUI.html` to find out the current URL of the [Configuration page](#).

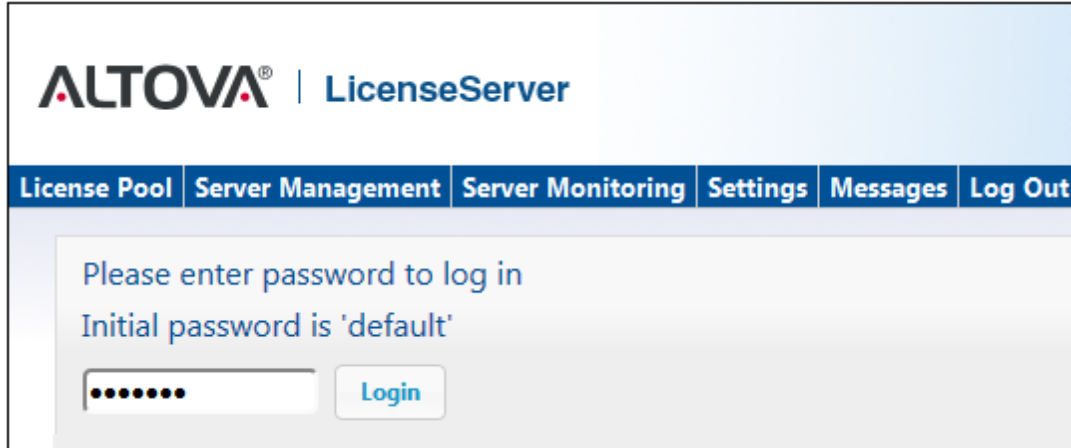
The dynamically generated URL in `webUI.html` will have a form something like:

```
http://127.0.0.1:55541/optionally-an-additional-string
```

, and it is located in the function `checkIfServiceRunning()` in a script near the end of the `<head>` element. While the port number in the URL is dynamically assigned, the IP address part identifies the server on which LicenseServer has been installed. If you wish to access the LicenseServer [Configuration page](#) from another machine, make sure that the IP address part of the URL has the correct IP address or name of the server on which LicenseServer has been installed. For example, the URL could be something like: `http://MyServer:55541`.

Logging in with the initial password

After going through the steps above, the [Configuration page](#) is opened with the login mask displayed (*screenshot below*). You can log in with the initial password of `default`. After you have logged in, you can change your password in the [Settings](#) tab.



Setting a fixed or dynamic port for the Configuration page

The port of the Configuration page (Web UI)—and consequently its address—can be specified in the [Settings page](#). By default the port is 8088. You can set any other port you want for the LicenseServer [Configuration page](#) (see *screenshot below*). Alternatively, you allow the port to be selected dynamically each time LicenseServer starts up. In this case, you will need to find out the URL of the Configuration page from the file `webUI.html` (see [Open LicenseServer Config Page \(Windows\)](#) and [Open LicenseServer Config Page \(Linux\)](#)).

Web UI

Configure the host addresses where the web UI is available to administrators.

- All interfaces and assigned IP addresses
- Local only (localhost)
- Only the following hostname or IP address:
Ensure this hostname or IP address exists or LicenseServer will fail to start!

Configure the port used for the web UI.

- Dynamically chosen by the operating system
- Fixed port
Ensure this port is available or LicenseServer will fail to start!

The advantage of a fixed port is that the page URL is known in advance and therefore can be accessed easily. If the port is assigned dynamically, the port part of the URL will have to be looked up in the file `webUI.html` each time LicenseServer is started.

Open LicenseServer's Config Page (Linux)

This section:

- [Opening the Configuration page for the first time with the returned URL](#)
 - [URL of the LicenseServer Configuration page](#)
 - [Logging in with the initial password](#)
 - [Setting a fixed port for the Configuration page](#)
-

Opening the Configuration page for the first time with the returned URL

On Linux systems, when you register your Altova server product with LicenseServer via the CLI, the URL of the LicenseServer Configuration page is returned. On opening this URL in a browser, you are prompted to read and accept the license agreement. After accepting the license agreement, the Configuration page's login mask is displayed (*screenshot below*).

URL of the LicenseServer Configuration page

To open the LicenseServer [Configuration page](#) at any time, enter its URL in the address bar of a browser and press **Enter**. By default, the URL of the Configuration page will be:

```
http://<serverIPAddressOrName>:8088/
```

The URL is present in the HTML code of the Configuration page itself, which is named `webUI.html` and is located at:

```
/var/opt/Altova/LicenseServer/webUI.html
```

If you have [set the URL of the Configuration page](#) to be generated dynamically (in the Settings tab of the Configuration page), then a new URL is generated each time LicenseServer is started. You will need to check the current version of `webUI.html` to find out the current URL of the [Configuration page](#).

The dynamically generated URL in `webUI.html` will have a form something like:

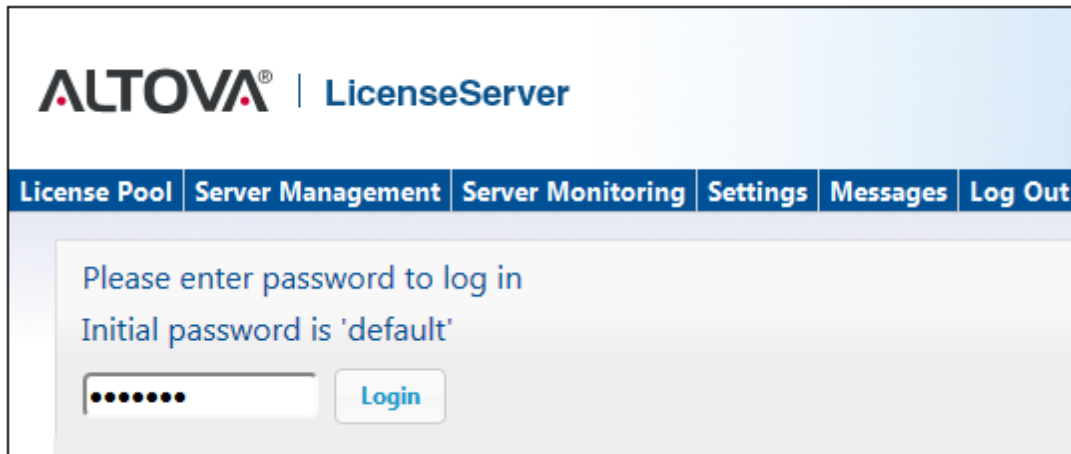
```
http://127.0.0.1:55541
```

and it is located in the function `checkIfServiceRunning()` in a script near the end of the `<head>` element. While the port number in the URL is dynamically assigned, the IP address part identifies the server on which LicenseServer has been installed. If you wish to access the LicenseServer [Configuration page](#) from another machine, make sure that the IP address part of the URL has the correct IP address or name of the server on which LicenseServer has been installed. For example, the URL could be something like: `http://MyServer:55541`.

Logging in with the initial password

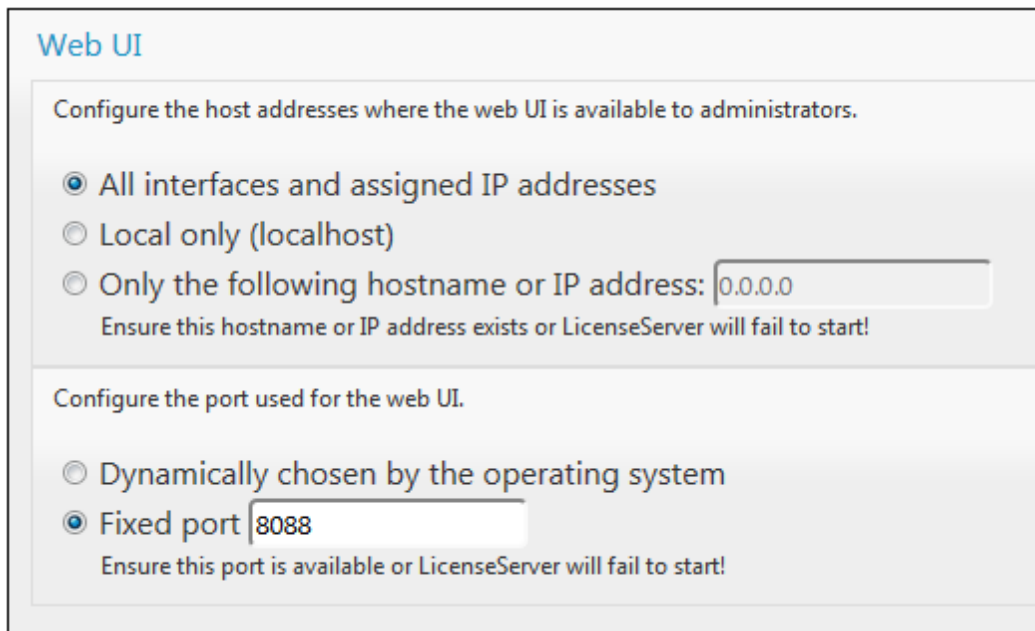
After going through the steps above, the [Configuration page](#) is opened with the login mask displayed (*screenshot below*). You can log in with the initial password of `default`. After you have

logged in, you can change your password in the [Settings](#) tab.



Setting a fixed or dynamic port for the Configuration page

The port of the Configuration page (Web UI)—and consequently its address—can be specified in the [Settings page](#). By default the port is 8088. You can set any other port you want for the LicenseServer [Configuration page](#) (see *screenshot below*). Alternatively, you allow the port to be selected dynamically each time LicenseServer starts up. In this case, you will need to find out the URL of the Configuration page from the file `webUI.html` (see [Open LicenseServer Config Page \(Windows\)](#) and [Open LicenseServer Config Page \(Linux\)](#)).



The advantage of a fixed port is that the page URL is known in advance and therefore can be accessed easily. If the port is assigned dynamically, the port part of the URL will have to be looked up in the file `webUI.html` each time LicenseServer is started.

Open LicenseServer's Config Page (Mac OS X)

This section:

- [Opening the Configuration page for the first time with the returned URL](#)
 - [URL of the LicenseServer Configuration page](#)
 - [Logging in with the initial password](#)
 - [Setting a fixed port for the Configuration page](#)
-

Opening the Configuration page for the first time with the returned URL

On Mac OS X systems, when you register your Altova server product with LicenseServer via the CLI, the URL of the LicenseServer Configuration page is returned. On opening this URL in a browser, you are prompted to read and accept the license agreement. After accepting the license agreement, the Configuration page's login mask is displayed (*screenshot below*).

URL of the LicenseServer Configuration page

To open the LicenseServer [Configuration page](#) at any time, enter its URL in the address bar of a browser and press **Enter**. By default, the URL of the Configuration page will be:

```
http://<serverIPAddressOrName>:8088/
```

The URL is present in the HTML code of the Configuration page itself, which is named `webUI.html` and is located at:

```
/var/Altova/LicenseServer/webUI.html
```

If you have [set the URL of the Configuration page](#) to be generated dynamically (in the Settings tab of the Configuration page), then a new URL is generated each time LicenseServer is started. You will need to check the current version of `webUI.html` to find out the current URL of the [Configuration page](#).

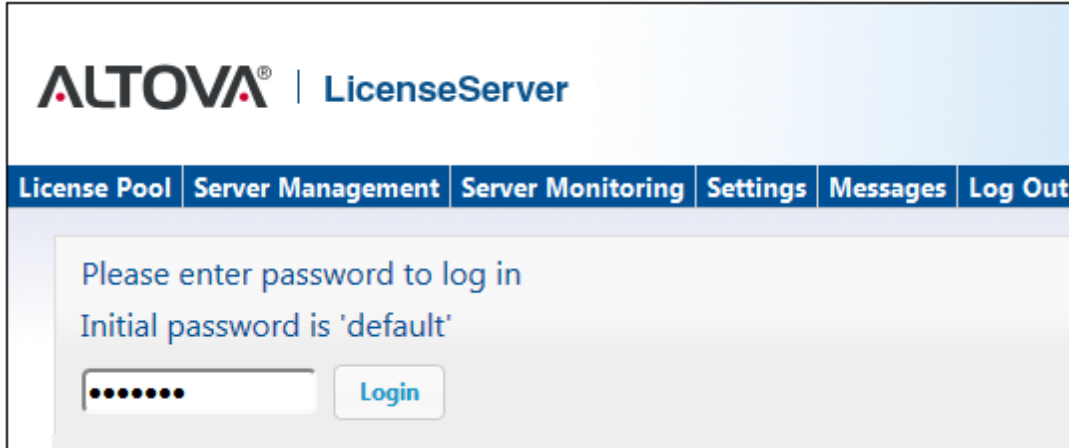
The dynamically generated URL in `webUI.html` will have a form something like:

```
http://127.0.0.1:55541, and it is located in the function checkIfServiceRunning() in a script near the end of the <head> element. While the port number in the URL is dynamically assigned, the IP address part identifies the server on which LicenseServer has been installed. If you wish to access the LicenseServer Configuration page from another machine, make sure that the IP address part of the URL has the correct IP address or name of the server on which LicenseServer has been installed. For example, the URL could be something like: http://MyServer:55541.
```

Note: The [Configuration page](#) can also be accessed directly via the **Finder | Applications | Altova License Server** icon.

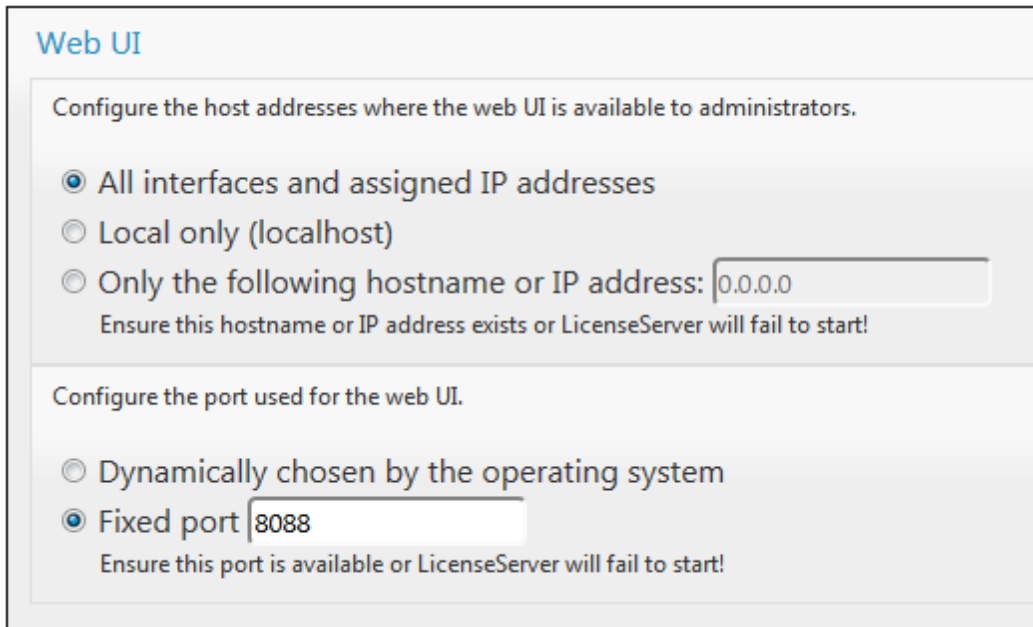
Logging in with the initial password

After going through the steps above, the [Configuration page](#) is opened with the login mask displayed (*screenshot below*). You can log in with the initial password of `default`. After you have logged in, you can change your password in the [Settings](#) tab.



Setting a fixed or dynamic port for the Configuration page

The port of the Configuration page (Web UI)—and consequently its address—can be specified in the [Settings page](#). By default the port is 8088. You can set any other port you want for the LicenseServer [Configuration page](#) (see *screenshot below*). Alternatively, you allow the port to be selected dynamically each time LicenseServer starts up. In this case, you will need to find out the URL of the Configuration page from the file `webUI.html` (see [Open LicenseServer Config Page \(Windows\)](#) and [Open LicenseServer Config Page \(Linux\)](#)).



The advantage of a fixed port is that the page URL is known in advance and therefore can be accessed easily. If the port is assigned dynamically, the port part of the URL will have to be looked up in the file `webUI.html` each time LicenseServer is started.

Upload Licenses to LicenseServer

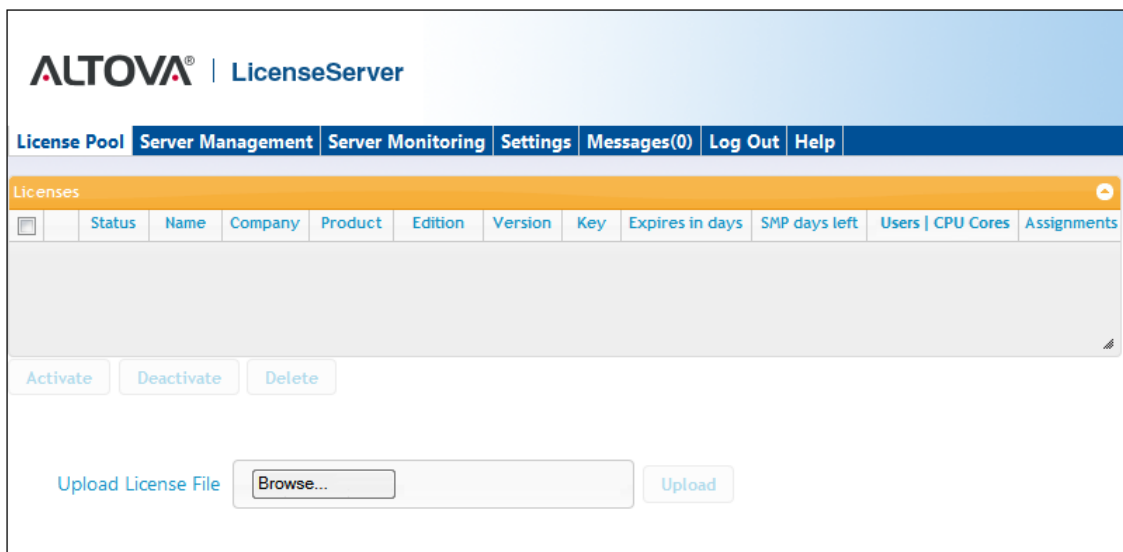
This section:

- [Uploading a license file to the license pool of LicenseServer](#)
- [License status](#)
- [Activating the licenses you wish to use](#)
- [Next steps](#)

Uploading a license file to the license pool of LicenseServer

After you have obtained a license file from Altova, you must upload it to the Altova LicenseServer. (How to do this is described below.) Each license file can contain one or more licenses and depends on your purchase. When you upload a license file, all the licenses in it will be uploaded to LicenseServer and can be assigned to an Altova product that has been registered with that LicenseServer. All the uploaded licenses, from one or more license files and for all Altova products, are collected in a license pool on the LicenseServer. The license pool is displayed in the License Pool tab of the LicenseServer Configuration page (*screenshot below*).

License files are uploaded to the LicenseServer using the Upload function of the License Pool tab (*see screenshot below*).



Click the **Browse** button and select the license file you want. The license file will appear in the Upload License File text field and the **Upload** button will be enabled. Click the **Upload** button to upload the license file. All the licenses in the file are uploaded and displayed in the License Pool tab. The screenshot below shows multiple licenses, uploaded from multiple license files.

Altova LicenseServer

ALTOVA | LicenseServer

License Pool | Server Management | Server Monitoring | Settings | Messages | Log Out | Help

Licenses

<input type="checkbox"/>	Status	Name	Company	Product	Edition	Version	Key	Expires in day	SMP days left	Users CPU
<input type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova FlowForce Server		2013	CAWYXW8-	334	334	1
<input checked="" type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova FlowForce Server		2013	7CMJT18-	334	334	2
<input type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova MapForce Server		2013	MM5UC1U-	334	334	1
<input type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova RaptorXML+XBRL		2013	HC139LF-	334	334	1
<input type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova StyleVision Server		2013	3D78278-	334	334	1
<input type="checkbox"/>	Inactive	Mr. Nobody	Altova GmbH	Altova FlowForce Server		2013	966PPHM-	334	334	3
<input type="checkbox"/>	Inactive	Mr. Nobody	Altova GmbH	Altova StyleVision Server		2013	DA5T2WU-	334	334	4

Activate | Deactivate | Delete

Upload License File Browse... | Upload

License status

License status values are as follows:

- Activating:** When a license is uploaded into the license pool of LicenseServer, the server will transmit license-related data to the `altova.com` master licensing server to validate, authenticate, and activate the license that was supplied. This is necessary to ensure compliance with the Altova license agreements. During this initial activation and authentication transaction—which typically lasts between 30 seconds and a couple of minutes, depending on your Internet connection, speed, and overall network traffic—the status of the license will be indicated as *Activating...*
- Failed Verification:** If a connection with the `altova.com` master licensing server cannot be made, then the status of the license in the pool will be shown as *Failed Verification*. If this happens, check your Internet connection and firewall rules to ensure that LicenseServer is able to communicate with the `altova.com` master licensing server.
- Active:** Once the license has been authenticated and activated, the status in the pool will change to *Active*.
- Inactive:** If a license has been verified, but is present on another LicenseServer on the network, the status in the pool will be shown as *Inactive*. An *Inactive* status also results when a license is manually deactivated in the license pool by the administrator.
- Blocked:** A license is shown in the license pool as *Blocked* if there was a problem authenticating the license and the `altova.com` master licensing server has not granted permission to the LicenseServer to use this license. This could be the result of a license agreement violation, over-usage of a license, or other compliance issues. Should you see a license showing up as *Blocked*, please contact Altova Support with your license

information and any other relevant data.

These statuses are summarized in the table below:

Status	Meaning
<i>Activating...</i>	On upload, license information is sent to <code>altova.com</code> for verification. Refresh the browser to view the updated status. Verification and activation can take a few minutes.
<i>Failed Verification</i>	A connection to <code>altova.com</code> could not be made. After establishing a connection, either restart the service or activate the license (with the Activate button).
<i>Active</i>	Verification was successful, the license is active.
<i>Inactive</i>	Verification was successful, but the license is on another LicenseServer on the network. Licenses can be made inactive with the Deactivate button.
<i>Blocked</i>	Verification was not successful. License is invalid and is blocked. Contact Altova Support .

Note: After a license has been sent to `altova.com` for verification, the browser must be refreshed to see the updated status. Verification and activation can take a few minutes.

Note: If a connection to `altova.com` could not be made, the status will be *Failed Verification*. After establishing a connection, either restart the service or try activating the license with the **Activate** button.

Note: When a license is given a status of *Inactive* or *Blocked*, a message explaining the status is also added to the Messages log.

Only an active license can be assigned to a product installation. An inactive license can be activated or deleted from the license pool. If a license is deleted from the license pool, it can be uploaded again to the pool by uploading the license file containing it. When a license file is updated, only those licenses in it that are not already in the pool will be uploaded to the pool. To activate, deactivate, or delete a license, select it and then click the **Activate**, **Deactivate**, or **Delete** button, respectively.

Activate the license/s you wish to use

Before you can assign a license to an Altova product, it must be active. So do ensure it is active. If it is inactive, select it and click **Activate**.

Next Steps

After you have uploaded the license file to the LicenseServer and checked that the license you

want is active, do the following:

1. Register the Altova server product ([FlowForce Server](#), [MapForce Server](#), [StyleVision Server](#)) with LicenseServer. (If you have already done this prior to uploading the license file, you can now start assigning licenses.)
2. [Assign a license](#) to your Altova product that has been registered with the LicenseServer.

Register Product/s

Before you can [assign a license](#) to an Altova server product, you must register the product installation with LicenseServer. The registration is done from the Altova server product, and the process is different for those server products that have Web UIs and those that are run from the command line only. You will need the server name or IP Address of the machine on which LicenseServer is installed to carry out the registration.

This section describes how to register different Altova server products:

- [Register FlowForce Server](#)
- [Register MapForce Server](#)
- [Register StyleVision Server](#)
- [Register RaptorXML\(+XBRL\) Server](#)
- [Register MobileTogether Server](#)

Register FlowForce Server

This section:

- [Methods of registering FlowForce Server with LicenseServer](#)
 - [Accessing the FlowForce Server Setup page \(Windows\)](#)
 - [Accessing the FlowForce Server Setup page \(Linux\)](#)
 - [Registering FlowForce Server via the Setup page](#)
 - [Registering FlowForce Server via the FlowForce CLI \(Windows\)](#)
 - [Registering FlowForce Server via the FlowForce CLI \(Linux\)](#)
 - [Next steps](#)
-

Methods of registering FlowForce Server

FlowForce Server can be registered with LicenseServer using any of the following methods:

- [Via the FlowForce Server Setup page](#)
 - [Via the FlowForce CLI \(Windows\)](#)
 - [Via the FlowForce CLI \(Linux\)](#)
-

Accessing the FlowForce Server Setup page (Windows)

The FlowForce Server Setup page can be accessed in one of the following ways:

- Via the **Start** menu:
Start | Altova FlowForce Server 2015 | FlowForce Server Setup Page
- Via [Altova ServiceController](#): Click the ServiceController icon in the system tray. In the menu that pops up, select *Altova FlowForce Web | Setup*.

This pops up the FlowForce Server Setup page (*screenshot above*).

Accessing the FlowForce Server Setup page (Linux)

After you have installed FlowForce Server on Linux (see the FlowForce Server user documentation for information about how to do this), start FlowForce Web Server as a service with the following command:

```
sudo /etc/init.d/flowforcewebservice start
```

A message containing the URL of the FlowForce Server Setup appears in the terminal window:

```
FlowForceWeb running on http://127.0.1.1:3459/setup?key=52239315203
```

Enter the URL in the address field of a browser and hit **Enter** to access the FlowForce Server Setup page (*screenshot below*).

Registering FlowForce Server via the Setup page

In the Setup page (*screenshot below*)—how to access it is described above—the LicenseServer field specifies the Altova LicenseServer to be used for registration.

ALTOVA®
FlowForce®
SERVER 2014

Home Help

Setup

LicenseServer

Enter address here or search for LicenseServer  

[Register with LicenseServer](#)

FlowForce Web Server

Bind address: All interfaces (0.0.0.0) ▼ 127.0.0.1 Port: 8082

Default time zone: Europe/Berlin ▼

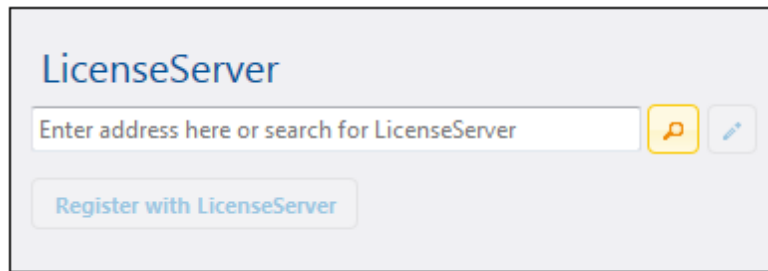
FlowForce Server

Bind address: All interfaces (0.0.0.0) ▼ 127.0.0.1 Port: 4646

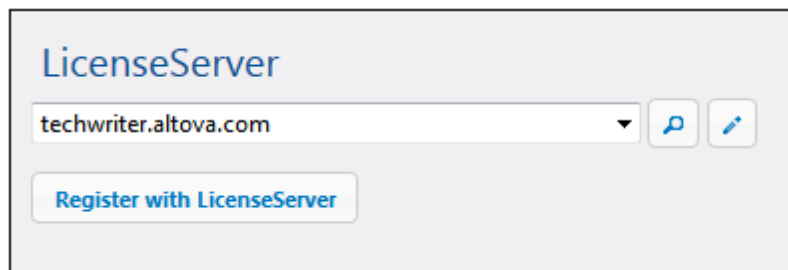
[Apply settings and restart FlowForce services](#)

The LicenseServer can be specified in one of two ways.

- You can search for Altova LicenseServers that are currently available on the network—that is, those that are currently running. Do this by clicking the **Search for Altova LicenseServers** button (*highlighted yellow in the screenshot below*).



The search returns a list of available Altova LicenseServers on the network. One LicenseServer will be selected (*screenshot below*) and the others will be available in the dropdown list of the combo box. Select the LicenseServer on which your FlowForce license is stored.



- Alternatively, you can enter the address of the LicenseServer in the LicenseServer field. If the currently running LicenseServers are available as a dropdown list, you must click the **Manually Enter Address** button to be able to enter an address in the LicenseServer field.

After you have specified the LicenseServer, click **Register with LicenseServer**. The Altova server application will be registered with the specified LicenseServer, and that LicenseServer's [Configuration page](#) will open in a browser with its Server Management tab active (*screenshot below*).

Note: You may need to allow pop-ups in order for the LicenseServer Configuration page to be displayed.

The screenshot shows the Altova LicenseServer interface with the following details:

- Navigation:** License Pool | Server Management | Server Monitoring | Settings | Messages(0) | Log Out | Help
- Server List:**
 - Altova FlowForce Server 2014:** This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Key Code: [empty]. CPU Cores: [empty]. Max licensed CPU cores: 0.
 - Altova StyleVision Server 2014:** This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Key Code: [empty]. CPU Cores: [empty]. Max licensed CPU cores: 0.
 - Altova MapForce Server 2014:** This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Key Code: [empty]. CPU Cores: [empty]. Max licensed CPU cores: 0.
- Actions:**
 - Request evaluation licenses
 - Unregister server and all products

In the screenshot below, three Altova products have been registered with the Altova LicenseServer at DOC.altova.com. How to assign licenses is described in the next section, [Assign Licenses to Registered Products](#).

Registering FlowForce Server via the FlowForce CLI (Windows)

On Windows machines, FlowForce Server can also be registered with an Altova LicenseServer on your network via the command line (CLI) by using the `licenseserver` command:

```
FlowForceServer licenseserver Server-Or-IP-Address
```

For example, if LicenseServer is running on `http://localhost:8088`, then register FlowForce Server with:

```
FlowForceServer licenseserver localhost
```

If FlowForce Server was installed with other Altova server products as sub-packages, registering

FlowForce Server will automatically also register the Altova server products. After successfully registering FlowForce Server, you can go to LicenseServer and assign a license to FlowForce Server. How to do this is described in the section [Assign Licenses to Registered Products](#).

Registering FlowForce Server via the FlowForce CLI (Linux)

On Linux machines, FlowForce Server can be registered with LicenseServer by using the `licenseserver` command of the FlowForce Server CLI. Note that FlowForce Server must be started with root rights.

```
sudo /opt/Altova/FlowForceServer2015/bin/flowforceserver licenseserver localhost
```

In the command above, `localhost` is the name of the server on which LicenseServer is installed. Notice also that the location of the FlowForce Server executable is:

```
/opt/Altova/MapForceServer2015/bin
```

After successfully registering FlowForce Server, you can go to LicenseServer and assign a license to FlowForce Server. How to do this is described in the section [Assign Licenses to Registered Products](#).

Next Steps

After you have registered your Altova product with LicenseServer, do the following:

1. If you have not already uploaded your license file/s to the LicenseServer (see previous section, [Upload the license/s](#)), upload the license file now and check that the license you want is active. If you have already done this, carry on to the next step, [Assign Licenses](#).
2. [Assign a license](#) to your Altova product that has been registered with the LicenseServer.

Register MapForce Server

This section:

- [Registering MapForce Server from FlowForce Server \(Windows\)](#)
 - [Registering a standalone MapForce Server \(Windows\)](#)
 - [Registering MapForce Server \(Linux\)](#)
 - [Next steps](#)
-

MapForce Server can be installed as part of the FlowForce Server package or as a standalone server product. In either case, it must be registered with Altova LicenseServer. Only after it has been registered with LicenseServer can a [license be assigned](#) to it from LicenseServer. On Windows systems, if MapForce Server was installed as part of the FlowForce Server package, it will automatically be registered when FlowForce is registered. On Linux systems, only if MapForce Server is installed after FlowForce Server will it be registered automatically when FlowForce Server is registered subsequently.

Registering MapForce Server from FlowForce Server (Windows)

MapForce Server is packaged with FlowForce Server, so when FlowForce Server is registered with an Altova LicenseServer on your network, MapForce Server will automatically also be registered with LicenseServer. How to register FlowForce Server is described in the FlowForce Server documentation and in the section, [Register FlowForce Server with LicenseServer](#).

After the registration, you can go to LicenseServer and assign a MapForce Server license to MapForce Server. How to do this is described in the section, [Assign Licenses to Registered Products](#).

Registering a standalone MapForce Server (Windows)

If you have installed MapForce Server as a standalone package, you must register it with an Altova LicenseServer on your network and then license it from the Altova LicenseServer. You can register MapForce Server via its command line interface (CLI) by using the `licenseserver` command:

```
MapForceServer licenseserver Server-Or-IP-Address
```

For example, if LicenseServer is running on `http://localhost:8088`, then register MapForce Server with:

```
MapForceServer licenseserver localhost
```

After successfully registering MapForce Server, you can go to LicenseServer and assign a license to MapForce Server. How to do this is described in the section, [Assign Licenses to Registered Products](#).

Registering MapForce Server (Linux)

On Linux machines, MapForce Server can be registered with LicenseServer by using the `licenseserver` command of the MapForce Server CLI. Note that MapForce Server must be started with root rights.

```
sudo /opt/Altova/MapForceServer2015/bin/mapforceserver licenseserver localhost
```

In the command above, `localhost` is the name of the server on which LicenseServer is installed. Notice also that the location of the MapForce Server executable is:

```
/opt/Altova/MapForceServer2015/bin
```

After successfully registering MapForce Server, you can go to LicenseServer and assign a license to MapForce Server. How to do this is described in the section [Assign Licenses to Registered Products](#).

Next Steps

After you have registered your Altova product with LicenseServer, do the following:

1. If you have not already uploaded your license file/s to the LicenseServer (see previous section, [Upload the license/s](#)), upload the license file now and check that the license you want is active. If you have already done this, carry on to the next step, [Assign Licenses](#).
2. [Assign a license](#) to your Altova product that has been registered with the LicenseServer.

Register StyleVision Server

This section:

- [Registering StyleVision Server from FlowForce Server \(Windows\)](#)
 - [Registering a standalone StyleVision Server \(Windows\)](#)
 - [Registering StyleVision Server \(Linux\)](#)
 - [Next steps](#)
-

StyleVision Server can be installed as part of the FlowForce Server package or as a standalone server product. In either case, it must be registered with Altova LicenseServer. Only after it has been registered with LicenseServer can a [license be assigned](#) to it from LicenseServer. On Windows systems, if StyleVision Server was installed as part of the FlowForce Server package, it will automatically be registered when FlowForce is registered. On Linux systems, only if StyleVision Server is installed after FlowForce Server will it be registered automatically when FlowForce Server is registered subsequently.

Registering StyleVision Server from FlowForce (Windows)

StyleVision Server is packaged with FlowForce Server, so when FlowForce Server is registered with an Altova LicenseServer on your network, StyleVision Server will automatically also be registered with LicenseServer. How to register FlowForce Server is described in the FlowForce Server documentation and in the section, [Register FlowForce Server with LicenseServer](#).

After the registration, you can go to LicenseServer and assign a StyleVision Server license to StyleVision Server. How to do this is described in the section [Assign Licenses to Registered Products](#).

Registering a standalone StyleVision Server (Windows)

If you have installed StyleVision Server as a standalone package on Windows, you must register it with an Altova LicenseServer on your network and then license it from the Altova LicenseServer. You can register StyleVision Server via its command line interface (CLI) by using the `licenseserver` command:

```
StyleVisionServer licenseserver Server-Or-IP-Address
```

For example, if LicenseServer is running on `http://localhost:8088`, then register StyleVision Server with:

```
StyleVisionServer licenseserver localhost
```

After successfully registering StyleVision Server, you can go to LicenseServer and assign a license to StyleVision Server. How to do this is described in the section [Assign Licenses to Registered Products](#).

Registering StyleVision Server (Linux)

On Linux machines, StyleVision Server can be registered with LicenseServer by using the `licenseserver` command of the StyleVision Server CLI. Note that StyleVision Server must be started with root rights.

```
sudo /opt/Altova/StyleVisionServer2015/bin/stylevisionserver licenseserver localhost
```

In the command above, `localhost` is the name of the server on which LicenseServer is installed. Notice also that the location of the StyleVision Server executable is:

```
/opt/Altova/StyleVisionServer2015/bin
```

After successfully registering StyleVision Server, you can go to LicenseServer and assign a license to StyleVision Server. How to do this is described in the section [Assign Licenses to Registered Products](#).

Next Steps

After you have registered your Altova product with LicenseServer, do the following:

1. If you have not already uploaded your license file/s to the LicenseServer (see previous section, [Upload the license/s](#)), upload the license file now and check that the license you want is active. If you have already done this, carry on to the next step, [Assign Licenses](#).
2. [Assign a license](#) to your Altova product that has been registered with the LicenseServer.

Register RaptorXML(+XBRL) Server

This section:

- [Registering RaptorXML\(+XBRL\) Server \(Windows\)](#)
 - [Registering RaptorXML\(+XBRL\) Server \(Linux\)](#)
 - [Next steps](#)
-

RaptorXML(+XBRL) Server must be installed on the server machine or network to which LicenseServer is connected and then be started as a service. It must then be registered with LicenseServer. Only after registration can a [license be assigned](#) to it from LicenseServer. This section describes how to register RaptorXML(+XBRL) Server with LicenseServer.

Registering RaptorXML(+XBRL) Server (Windows)

You can register RaptorXML(+XBRL) Server via its command line interface (CLI) by using the `licenseserver` command:

```
RaptorXML Server:  RaptorXML licenseserver Server-Or-IP-Address
RaptorXML+XBRL   RaptorXMLXBRL licenseserver Server-Or-IP-Address
Server:
```

For example, if LicenseServer is running on `http://localhost:8088`, then register RaptorXML(+XBRL) Server with:

```
RaptorXML Server:  RaptorXML licenseserver localhost
RaptorXML+XBRL   RaptorXMLXBRL licenseserver localhost
Server:
```

After successfully registering RaptorXML(+XBRL) Server, you can go to LicenseServer and assign a license to RaptorXML(+XBRL) Server. How to do this is described in the section [Assign Licenses to Registered Products](#).

Registering RaptorXML(+XBRL) Server (Linux)

On Linux machines, RaptorXML(+XBRL) Server can be registered with LicenseServer by using the `licenseserver` command of the RaptorXML(+XBRL) Server CLI. Note that RaptorXML(+XBRL) Server must be started with root rights.

```
sudo /opt/Altova/RaptorXMLServer2015/bin/raptorxmlserver licenseserver
localhost
```

```
sudo /opt/Altova/RaptorXMLXBRLServer2015/bin/raptorxmlxbrlserver licenseserver localhost
```

In the command above, `localhost` is the name of the server on which LicenseServer is installed. Notice also that the location of the RaptorXML(+XBRL) Server executable is:

```
/opt/Altova/RaptorXMLServer2015/bin  
/opt/Altova/RaptorXMLXBRLServer2015/bin
```

After successfully registering RaptorXML(+XBRL) Server, you can go to LicenseServer and assign a license to RaptorXML(+XBRL) Server. How to do this is described in the section [Assign Licenses to Registered Products](#).

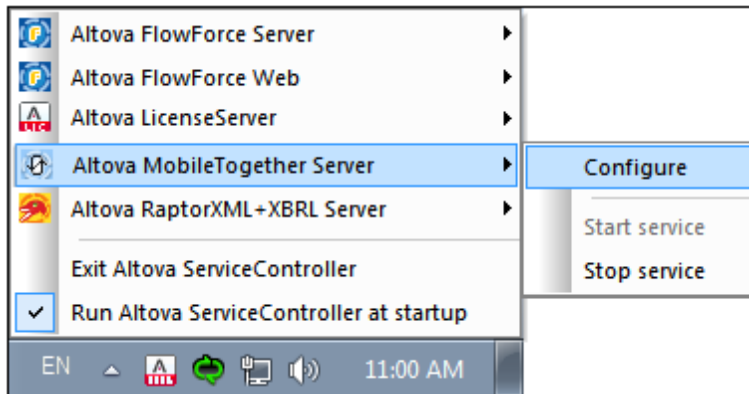
Next Steps

After you have registered your Altova product with LicenseServer, do the following:

1. If you have not already uploaded your license file/s to the LicenseServer (see previous section, [Upload the license/s](#)), upload the license file now and check that the license you want is active. If you have already done this, carry on to the next step, [Assign Licenses](#).
2. [Assign a license](#) to your Altova product that has been registered with the LicenseServer.

Register MobileTogether Server

To start MobileTogether Server, click the **ServiceController** icon in the system tray, hover over **Altova MobileTogether Server** in the menu that pops up (see screenshot below), and then select **Start Service** from the MobileTogether Server submenu. If MobileTogether Server is already running, the *Start Service* option will be disabled.



Register MobileTogether Server via:

- The Settings tab of the MobileTogether Server Web UI: (i) Start MobileTogether Server via ServiceController (see *previous point*); (ii) Enter your password to access the Setup page; (iii) Select the LicenseServer name or address, and click **Register with LicenseServer**.
- its CLI, using the `licenseserver` command:
`MobileTogetherServer licenseserver [options] ServerName-Or-IP-Address`
For example, if `localhost` is the name of the server on which LicenseServer is installed:
`MobileTogetherServer licenseserver localhost`

After successful registration, go to the [Server Management tab of LicenseServer's configuration page](#) to assign a license to MobileTogether Server.

Assign Licenses to Registered Products

This section:

- [Before assigning a license](#)
 - [The Server Management tab](#)
 - [Icons in the Server Management tab](#)
 - [Note on cores and licenses](#)
 - [Assigning a license](#)
 - [Unregistering products from LicenseServer](#)
-

Before assigning a license

Before you assign a license to an Altova product, make sure that:

- The relevant license has been uploaded to the [license pool of LicenseServer](#) and that the license is active.
 - Your Altova product has been registered with LicenseServer.
-

The Server Management tab

Licenses are assigned in the Server Management tab of the LicenseServer Configuration page (*screenshot below*). The screenshot shows that three Altova products have been registered with LicenseServer. (Since MapForce Server and StyleVision Server are bundled with FlowForce Server, registering FlowForce Server with LicenseServer automatically also registers MapForce Server and StyleVision Server. No additional registration of the latter two products are required if FlowForce Server is registered.)

The screenshot shows the Altova LicenseServer interface. At the top, there is a navigation bar with tabs: License Pool, Server Management (selected), Server Monitoring, Settings, Messages(0), Log Out, and Help. Below the navigation bar, the client machine 'DOC.altova.com' is listed. Three servers are registered under this machine:

- Altova FlowForce Server 2014**: This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Max licensed CPU cores: 0.
- Altova StyleVision Server 2014**: This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Max licensed CPU cores: 0.
- Altova MapForce Server 2014**: This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Max licensed CPU cores: 0.

At the bottom of the server list, there are two buttons: 'Request evaluation licenses' and 'Unregister server and all products'.

Note the following points about the Server Management tab:

- Each product is listed under the name of its client machine. In the screenshot above, one client machine, named `Doc.altova.com`, is listed. This client machine (`Doc.altova.com`) has three Altova products registered with the LicenseServer. If an Altova product on a different client machine is registered with this LicenseServer, then that client machine, with its registered products, will also be listed in the Server Management tab.
- Each registered Altova product on a client machine has its own *Key Code* entry, which takes the key code of a license. A registered product's key code is assigned by clicking its **Edit Assigned Licenses** button (see *icon list below*) and selecting the required license from those available for that product (for example, FlowForce Server) in the license pool. This procedure is explained in more detail below.
- Each product also has a line stating how many CPU cores need to be licensed to run that product on that client. If the number of licensed cores is less than the number required, then the information is marked in red (see *screenshot above*). (The number of CPU cores that need to be licensed is the number of CPU cores on that client and is obtained from the client machine by LicenseServer.)
- If **multiple versions** of a single product (for example, StyleVision Server 2013 and StyleVision Server 2014) have been installed on one machine and if each of these installations has been registered with a single LicenseServer, then the multiple registrations are consolidated in a single registration in the Server Management tab and

displayed as a single registration. When a license is assigned to this single registration, all the installations indicated by that registration will be licensed. However, multiple instances of only one installation can be run simultaneously on the client machine. For example, multiple instances of StyleVision Server 2013 or multiple instances of StyleVision Server 2014 can be run simultaneously, but not one instance of StyleVision Server 2013 and one instance of StyleVision Server 2014. Note that newly installed versions must be registered for them to run.

- New versions of Altova server products can only be licensed with the latest version of LicenseServer at the time of the product's release. Older Altova server products will work with newer versions of LicenseServer. So, if you are installing a new version of an Altova server product and if your current LicenseServer version is not the latest, de-install the older version of LicenseServer and install the latest version. All registration and licensing information held in your older version of LicenseServer will be saved, at the time of de-installation, to a database on the server, and will be imported automatically into the newer version. (The version number of the LicenseServer that is appropriate for any particular version of a server product is displayed during the installation of that server product. You can choose to install this version along with the server product. The version of the currently installed LicenseServer is given at the bottom of the [LicenseServer configuration page](#).)

Icons in the Server Management tab



Edit Assigned Licenses. Available with each product. Pops up the Manage Licenses dialog, in which new licenses can be assigned to the product and already assigned licenses can be edited.



Show Licenses. Appears with each license. Switches to the License Pool tab and highlights the selected license, so that license details can be read.



Unregister This Product. Available with each product. The selected product (on the selected client machine) will be unregistered from LicenseServer.

Note on cores and licenses

The licensing of Altova server products, *except MobileTogether Server****, is based on the number of processor cores available on the product machine. For example, a dual-core processor has two cores, a quad-core processor four cores, a hexa-core processor six cores, and so on. The number of cores licensed for a product on a particular server machine must be greater than or equal to the number of cores available on that server, whether it's a physical or virtual machine.

For example, if a server has eight cores (an octa-core processor), you must purchase at least an 8-core license. You can also combine licenses to achieve the core count. So, two 4-core licenses can also be used for an octa-core server instead of an 8-core license.

If you are using a computer server with a large number of CPU cores but only have a low volume to process, you may also create a virtual machine that is allocated a smaller number of cores, and purchase a license for that number. Such a deployment, of course, will have less processing

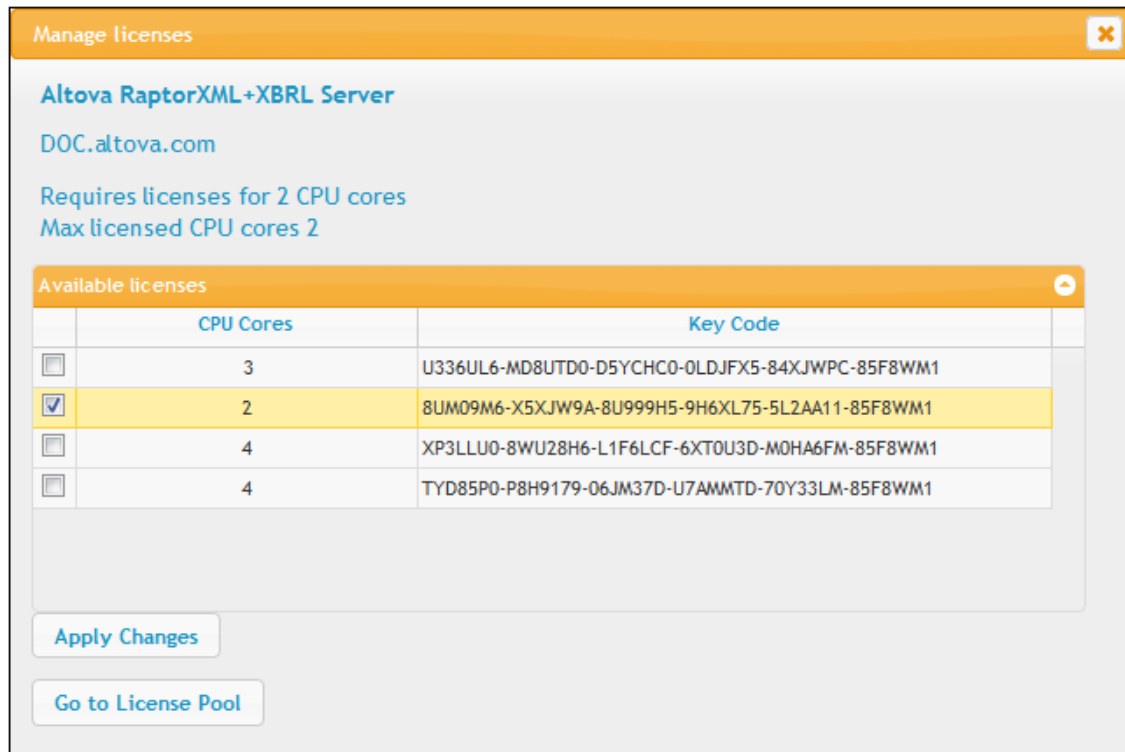
speed than if all available cores on the server were utilized.

Note: Each license can be used for only one client machine at a time, even if it has unused licensing capacity. For example, if a 10-core license is used for a client machine that has 6 CPU cores, then the remaining 4 cores of the license cannot be used simultaneously for another client machine.

*** MobileTogether Server licenses are assigned on the basis of the number of users, that is, the number of client devices that connect to MobileTogether Server.

Assigning a license

To assign a license to a registered product, click the **Edit Assigned Licenses** button of that product. This pops up the Manage Licenses dialog (*screenshot below*).






Note the following points about the licenses displayed in the Manage Licenses dialog:

- The product to be licensed is listed at the top left of the dialog. In the screenshot above the product is Altova FlowForce Server 2013.
- The dialog displays all the currently active licenses for that product in the license pool. In our screenshot, four currently active FlowForce Server licenses are in the license pool. LicenseServer will automatically detect from each license in the pool the product for which it has been issued.
- The licenses in the screenshot above have been licensed, respectively, for 3 CPU cores, 2 CPU cores, 4 CPU cores, and 4 CPU cores.

- You need to know the number of processor cores on the server on which the Altova server product has been installed. If the machine has a dual-core processor, you need a two-core (the CPU Cores count) license. This license could be, for example, the second license in the list shown in the screenshot above. You can also combine licenses. So, if the machine's processor is octa-core (eight-core), you can combine two 4-core licenses; for example, the third and fourth licenses in the list shown in the screenshot above.
- The Manage Licenses dialog will list only currently active licenses for that product. Licenses for other Altova products will not be listed.
- Licenses that have been assigned already—for example, to another installation of the product on the network—will have their check boxes checked. So only unchecked licenses may be selected.
- CPU cores indicates for how many CPU cores a license is valid.
- If you wish to make modifications to the license pool—for example, to upload, activate, deactivate, or delete a license—click the **Go to License Pool** button.

Select the license you wish to assign. The license's check box will be checked. Also, the total number of CPU cores licensed for that product on that client is listed near the top left of the dialog as *Max licensed CPU cores* (see screenshot above). You can select more licenses if you wish to increase the number of licensed CPU cores for that product on that client. The *Max licensed CPU cores* in this case will be the sum of the CPU cores of all the selected licenses.

After selecting the license/s, click **Apply Changes**. The license/s will be assigned to that product and displayed in the Server Management tab (see screenshot below). The screenshot below shows that a 2-CPU-core license for Altova FlowForce Server has been assigned (to the client machine Doc.altova.com).

Altova RaptorXML+XBRL Server 2014 This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. <input type="checkbox"/> Limit to single thread execution	Key Code	CPU Cores		
	8UM09M6-X5XJW9A-8U999H5-9H6XL75-5L2AA11-85F8WM1	2		
	Max licensed CPU cores	2		

Unregistering products

Each Altova product registered with LicenseServer is listed in the Server Management tab under its client machine name and has an **Unregister** icon to its right. Click this icon to unregister the product. If a license was assigned to the product, the assignment will be terminated when the product is unregistered. To unregister all products, click the **Unregister Server and All Products** button at the bottom of the Server Management tab (see first screenshot in this section).

To re-register a product, go to the product's pre-configuration page.

6.7 Configuration Page Reference

The LicenseServer Configuration page is the administrator's interface with LicenseServer (Web UI). It allows the management of LicenseServer and the licensing of Altova products that have been registered with LicenseServer ([FlowForce Server](#), [MapForce Server](#), [StyleVision Server](#), [RaptorXML\(+XBRL\) Server](#)). The LicenseServer Configuration page is viewed in a web browser. How to open the Configuration page is described in the sections, [Open LicenseServer Config Page \(Windows\)](#) and [Open LicenseServer Config Page \(Linux\)](#).

This section is a user reference for the Configuration page and is organized by the tabs of the Configuration page:

- [License Pool](#)
- [Server Management](#)
- [Server Monitoring](#)
- [Settings](#)
- [Messages, Log Out](#)

For a step-by-step guide of how to assign licenses with LicenseServer, see the section [How to Assign Licenses](#).

License Pool

This section:

- [Uploading a license](#)
- [License status](#)
- [Activating, de-activating, and deleting a license](#)
- [Icons in the License Pool tab](#)
- [License information](#)
- [Note on cores and licenses](#)

The **License Pool** tab displays all the licenses that are currently on the LicenseServer (see *screenshot below*). When a license file is uploaded to the LicenseServer with the **Upload** button on this page, all the licenses contained in the license file are placed in the license pool on the server and are displayed on the License Pool page.

The License Pool page displays information about all the licenses currently on the LicenseServer and thus provides a convenient overview of all Altova product licenses. On this page you can also activate, deactivate, and delete selected licenses.

Altova LicenseServer

ALTOVA | LicenseServer

License Pool | Server Management | Server Monitoring | Settings | Messages | Log Out | Help

Licenses

<input type="checkbox"/>	Status	Name	Company	Product	Edition	Version	Key	Expires in day	SMP days left	Users CPU
<input type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova FlowForce Server		2013	CAWYXW8-	334	334	1
<input checked="" type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova FlowForce Server		2013	7CMJT18-	334	334	2
<input type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova MapForce Server		2013	MM5UC1U-	334	334	1
<input type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova RaptorXML+XBRL		2013	HC139LF-	334	334	1
<input type="checkbox"/>	Active	Mr. Nobody	Altova GmbH	Altova StyleVision Server		2013	3D78278-	334	334	1
<input type="checkbox"/>	Inactive	Mr. Nobody	Altova GmbH	Altova FlowForce Server		2013	966PPHM-	334	334	3
<input type="checkbox"/>	Inactive	Mr. Nobody	Altova GmbH	Altova StyleVision Server		2013	DA5T2WU-	334	334	4

Activate | Deactivate | Delete

Upload License File Browse... | Upload

Uploading a license

To upload a license file (which you receive from Altova GmbH for your Altova server product), click the **Browse** button, browse for the license file and select it. On clicking **Upload**, all the licenses

contained in the license file are placed in the license pool and displayed on the License Pool page (*screenshot above*).

License status

License status values are as follows:

- *Activating*: When a license is uploaded into the license pool of LicenseServer, the server will transmit license-related data to the `altova.com` master licensing server to validate, authenticate, and activate the license that was supplied. This is necessary to ensure compliance with the Altova license agreements. During this initial activation and authentication transaction—which typically lasts between 30 seconds and a couple of minutes, depending on your Internet connection, speed, and overall network traffic—the status of the license will be indicated as *Activating...*
- *Failed Verification*: If a connection with the `altova.com` master licensing server cannot be made, then the status of the license in the pool will be shown as *Failed Verification*. If this happens, check your Internet connection and firewall rules to ensure that LicenseServer is able to communicate with the `altova.com` master licensing server.
- *Active*: Once the license has been authenticated and activated, the status in the pool will change to *Active*.
- *Inactive*: If a license has been verified, but is present on another LicenseServer on the network, the status in the pool will be shown as *Inactive*. An *Inactive* status also results when a license is manually deactivated in the license pool by the administrator.
- *Blocked*: A license is shown in the license pool as *Blocked* if there was a problem authenticating the license and the `altova.com` master licensing server has not granted permission to the LicenseServer to use this license. This could be the result of a license agreement violation, over-usage of a license, or other compliance issues. Should you see a license showing up as *Blocked*, please contact Altova Support with your license information and any other relevant data.

These statuses are summarized in the table below:

Status	Meaning
<i>Activating...</i>	On upload, license information is sent to <code>altova.com</code> for verification. Refresh the browser to view the updated status. Verification and activation can take a few minutes.
<i>Failed Verification</i>	A connection to <code>altova.com</code> could not be made. After establishing a connection, either restart the service or activate the license (with the Activate button).
<i>Active</i>	Verification was successful, the license is active.
<i>Inactive</i>	Verification was successful, but the license is on another LicenseServer on the network. Licenses can be made inactive with the Deactivate button.

<i>Blocked</i>	Verification was not successful. License is invalid and is blocked. Contact Altova Support .
----------------	--

Note: After a license has been sent to `altova.com` for verification, the browser must be refreshed to see the updated status. Verification and activation can take a few minutes.

Note: If a connection to `altova.com` could not be made, the status will be *Failed Verification*. After establishing a connection, either restart the service or try activating the license with the **Activate** button.

Note: When a license is given a status of *Inactive* or *Blocked*, a message explaining the status is also added to the Messages log.

Only an active license can be assigned to a product installation. An inactive license can be activated or deleted from the license pool. If a license is deleted from the license pool, it can be uploaded again to the pool by uploading the license file containing it. When a license file is updated, only those licenses in it that are not already in the pool will be uploaded to the pool. To activate, deactivate, or delete a license, select it and then click the **Activate**, **Deactivate**, or **Delete** button, respectively.

Connection to the Master Licensing Server at `altova.com`

The Altova LicenseServer needs to be able to communicate with the Master Licensing Server at `altova.com` to validate and authenticate license-related data and to ensure continuous compliance with the Altova license agreements. This communication occurs over HTTPS using port 443. If the Altova LicenseServer, after making the initial verification with the `altova.com` Master Licensing Server, is unable to again connect with `altova.com` for a duration of more than 5 days (= 120 hours), then the Altova LicenseServer will no longer permit the usage of any Altova software products connected to the Altova LicenseServer.

Any such loss of connection with the `altova.com` master servers will be logged in the [Messages tab](#) of the [Configuration page of the Altova LicenseServer](#). In addition, the administrator can configure the Altova LicenseServer to automatically send an alert email when the connection to `altova.com` is lost. Alert Mail settings are available in the [Settings tab](#) of the [Configuration page](#).

Activating, deactivating, and deleting a license

An active license can be deactivated by selecting the license and clicking **Deactivate**. An inactive license can be activated (**Activate** button) or deleted (**Delete** button). When a license is deleted it is removed from the license pool. A deleted license can be added again to the license pool by uploading the license file containing it. If a license file is re-uploaded, only licenses that are not already in the license pool will be added to the license pool; licenses that are already in the pool will not be re-added.

Icons in the License Pool tab



Edit Assigned Licenses. Appears with each license (in the Assignments column). Pops up the [Manage Licenses dialog](#), in which new licenses can be assigned to the product and already assigned licenses can be edited.



Show License Information. Appears with each license (in the Assignments column). Provides information about the currently active clients.

License information

The following license information is displayed:

- *Status:* Can be one of the following values: *Failed Verification | Activating | Active | Inactive | Blocked*. See [License status](#) above.
- *Name, Company:* The name and company of the licensee. This information was submitted at the time of purchase.
- *Product, Edition, Version:* The version and edition of the licensed products.
- *Key, Expires in days, SMP (days left):* The license key to unlock the product, and the number of days left before the license expires. Each licensed purchase comes with a Support & Maintenance Package, which is valid for a certain number of days. The *SMP* column notes how many SMP days are still left.
- *Users | CPU Cores:* The number of users or CPU cores that the license allows. In the case of Altova's MobileTogether Server product, licenses are assigned on the basis of the number of MobileTogether client devices that connect to MobileTogether Server. In the case of all other Altova server products, licenses are assigned on the basis of CPU cores (*see note below*).
- *Assignments:* Access to editing dialogs and information of individual licenses.

Note on cores and licenses

The licensing of Altova server products, *except MobileTogether Server****, is based on the number of processor cores available on the product machine. For example, a dual-core processor has two cores, a quad-core processor four cores, a hexa-core processor six cores, and so on. The number of cores licensed for a product on a particular server machine must be greater than or equal to the number of cores available on that server, whether it's a physical or virtual machine.

For example, if a server has eight cores (an octa-core processor), you must purchase at least an 8-core license. You can also combine licenses to achieve the core count. So, two 4-core licenses can also be used for an octa-core server instead of an 8-core license.

If you are using a computer server with a large number of CPU cores but only have a low volume to process, you may also create a virtual machine that is allocated a smaller number of cores, and purchase a license for that number. Such a deployment, of course, will have less processing speed than if all available cores on the server were utilized.

Note: Each license can be used for only one client machine at a time, even if it has unused

licensing capacity. For example, if a 10-core license is used for a client machine that has 6 CPU cores, then the remaining 4 cores of the license cannot be used simultaneously for another client machine.

- *** MobileTogether Server licenses are assigned on the basis of the number of users, that is, the number of client devices that connect to MobileTogether Server.

Server Management

This section:

- [Icons in the Server Management tab](#)
- [Assigning licenses](#)
- [One client machine under different names](#)
- [Requesting an evaluation license](#)
- [Unregistering products](#)

In the **Server Management** tab (screenshot below), you can assign licenses to [registered products](#).

The screenshot displays the Altova LicenseServer interface. At the top, the logo 'ALTOVA® | LicenseServer' is visible. Below the logo is a navigation bar with tabs: 'License Pool', 'Server Management' (selected), 'Server Monitoring', 'Settings', 'Messages(0)', 'Log Out', and 'Help'. The main content area shows a client machine named 'DOC.altova.com'. Underneath, three product entries are listed:

- Altova FlowForce Server 2014**: This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Max licensed CPU cores: 0.
- Altova StyleVision Server 2014**: This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Max licensed CPU cores: 0.
- Altova MapForce Server 2014**: This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required. Limit to single thread execution. Max licensed CPU cores: 0.

At the bottom of the product list, there are two buttons: 'Request evaluation licenses' and 'Unregister server and all products'.

Note the following points about the Server Management tab:

- Each product is listed under the name of its client machine. In the screenshot above, one client machine, named `Doc.altova.com`, has three Altova products registered with the LicenseServer. If an Altova product on a different client machine is registered with this

LicenseServer, then that client machine, with its registered products, will also be listed in the Server Management tab.

- Each registered Altova product on a client machine has its own *Key Code* entry, which takes the key code of a license. A registered product's key code is assigned by clicking its **Edit Assigned Licenses** button and selecting the required license from those available for that product (for example, FlowForce Server) in the license pool. This procedure is explained in more detail below.
- Each product ([except MobileTogether Server](#)) also has a line stating how many CPU cores need to be licensed to run that product on that client. If the number of licensed cores is less than the number required, then the information is marked in red (see *screenshot above*). (The number of CPU cores that need to be licensed is the number of CPU cores on that client and is obtained from the client machine by LicenseServer.)

Single thread execution

If a product license for only one core is available in the license pool, a machine with multiple cores can be assigned this one-core license. In such a case, the machine will run that product on a single core. Processing will therefore be slower as multi-threading (which is possible on multiple cores) will not be available. The product will be executed in single thread mode on that machine.

To assign a single-core license to a multiple-core machine, select the *Limit to single thread execution* check box for that product.

Icons in the Server Management tab



Edit Assigned Licenses. Available with each product. Pops up the Manage Licenses dialog, in which new licenses can be assigned to the product and already assigned licenses can be edited.



Show Licenses. Appears with each license. Switches to the License Pool tab and highlights the selected license, so that license details can be read.



Unregister This Product. Available with each product. The selected product (on the selected client machine) will be unregistered from LicenseServer.

Assigning a license

To assign a license to a registered product, click the **Edit Assigned Licenses** button of that product. This pops up the Manage Licenses dialog (*screenshot below*).

Manage licenses
✕

Altova RaptorXML+XBRL Server

DOC.altova.com

Requires licenses for 2 CPU cores
Max licensed CPU cores 2

Available licenses
↻

	CPU Cores	Key Code
<input type="checkbox"/>	3	U336UL6-MD8UTD0-D5YCHC0-0LDJFX5-84XJWPC-85F8WM1
<input checked="" type="checkbox"/>	2	8UM09M6-X5XJW9A-8U999H5-9H6XL75-5L2AA11-85F8WM1
<input type="checkbox"/>	4	XP3LLU0-8WU28H6-L1F6LCF-6XT0U3D-M0HA6FM-85F8WM1
<input type="checkbox"/>	4	TYD85P0-P8H9179-06JM37D-U7AMMTD-70Y33LM-85F8WM1

Apply Changes

Go to License Pool

Select the license you wish to assign. After selecting the license/s, click **Apply Changes**. The license/s will be assigned to that product and displayed in the Server Management tab (see *screenshot below*).

<p>Altova RaptorXML+XBRL Server 2014</p> <p>This server has 2 CPU core(s). Licenses for 2 CPU core(s) are required.</p> <p><input type="checkbox"/> Limit to single thread execution</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f4a460; color: white;"> <th style="width: 70%;">Key Code</th> <th style="width: 10%;">CPU Cores</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td>8UM09M6-X5XJW9A-8U999H5-9H6XL75-5L2AA11-85F8WM1</td> <td style="text-align: center;">2</td> <td style="text-align: center;"></td> </tr> <tr> <td colspan="2">Max licensed CPU cores</td> <td style="text-align: center;">2</td> </tr> </tbody> </table>	Key Code	CPU Cores		8UM09M6-X5XJW9A-8U999H5-9H6XL75-5L2AA11-85F8WM1	2		Max licensed CPU cores		2	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="background-color: #f4a460; color: white; padding: 5px; border-radius: 5px;"></div> <div style="background-color: #f4a460; color: white; padding: 5px; border-radius: 5px;"></div> </div>
Key Code	CPU Cores										
8UM09M6-X5XJW9A-8U999H5-9H6XL75-5L2AA11-85F8WM1	2										
Max licensed CPU cores		2									

One client machine under different names

If a client machine is registered more than once with LicenseServer, it might appear in the Server Management tab under multiple names, that is, with multiple entries. This could happen, for example, if a machine is re-registered with the host name given in a different form.

To ensure that additional licenses are not redundantly assigned to the same machine under its different names, you should unregister redundant client machine entries by clicking the **Unregister server and all products** button of these machines. *(Note: While the client machines are considered for the purposes of this documentation to be clients of LicenseServer, they are in effect servers of their own products.)* Also, if the same license is assigned multiple times to the same machine under its different names, licensing conflicts could arise. So, to avoid these two situations (redundant licensing and multiple assignments of a single license), it is recommended that redundant entries of a single client machine be unregistered.

Given below are forms a machine name might take in the Server Management tab:

- *Host name with domain name (the fully qualified domain name, FQDN), such as: "win80-x64_1.my.domain.com" or "Doc3.my.domain.com".* This happens when the host name of the machine (with or without the domain information) is passed as the argument of the `licenseserver` CLI command that is used to register the server product with LicenseServer. For example: `<AltovaServerProduct> licenseserver Doc3`. This produces an FQDN such as: `Doc3.my.domain.com`.

An FQDN is also produced when `localhost` is supplied on Windows 7 systems as the host name.

- *Host name without domain name. For example: "win80-x64_1" or "Doc3".* This happens on Windows 8 systems when `localhost` is given as the machine name.
- *localhost.* In some cases, `localhost` is also displayed as a machine name.

Note: If, during installation of the Altova server product on Windows machines, the machine is automatically registered with LicenseServer, `localhost` is used by the installer as the machine name.

Requesting an evaluation license

You can obtain a 30-day free evaluation license for each of a client's installed Altova products that have been registered with LicenseServer. Click the **Request Evaluation Licenses** button near the bottom of the Server Management tab. A dialog pops up containing a list of the Altova server products (on that client machine) which have been registered with LicenseServer. Make sure that the products for which you want an evaluation license are checked, then fill in the registration fields, and send the request. You will receive an e-mail from Altova containing the 30-day evaluation license/s. The number of cores for which the license will be valid per product will be exactly the number required by the product at the time the request is sent. Save the license/s to disk and [upload to the license pool](#).

Unregistering products

Each Altova product registered with LicenseServer is listed in the Server Management tab under its client machine name and has an **Unregister** icon to its right. Click this icon to unregister the product. If a license was assigned to the product, the assignment will be terminated when the product is unregistered. To unregister all products, click the **Unregister Server and All Products** button at the bottom of the Server Management tab (*see first screenshot in this section*).

To re-register a product with LicenseServer, go to the product's Setup page or its CLI and register it. See: [Register FlowForce Server](#), [Register MapForce Server](#), [Register StyleVision Server](#), and [Register RaptorXML\(+XBRL\) Server](#).

For more information, see the section, [Assigning Licenses to Registered Products](#).

Server Monitoring

The **Server Monitoring** tab provides an overview of servers currently running licensed Altova products. It contains product information along with information about users and licenses.

Settings

This section:

- [Network settings](#)
 - [Alert Mail settings](#)
 - [Miscellaneous settings](#)
-

The **Settings** tab is described below. You can set the following:

- The password for logging in to LicenseServer. Enter the desired password and click **Change Password**.
 - Test connectivity to Altova by clicking **Test Connection to Altova**. Note that you must save new settings (by clicking the **Save** button at the bottom of the pane) before testing the connection. The **Test Connection to Altova** button is disabled while the test is in progress, and becomes enabled again when the test has been completed.
 - Client statistics
 - Network settings for the web-based configuration page (Web UI), the proxy server used to connect to the Internet (if any), for and for LicenseServer (License Service). These settings are described in [Network settings](#) below.
 - Email server settings and the alert mail recipient to contact in the event of a significant LicenseServer occurrence. These settings are described in [Alert Mail settings](#) below.
 - After you change a setting, click **Save** at the bottom of the pane. A changed setting will not take effect till it is saved.
-

Network settings

Administrators can specify network access points to the LicenseServer configuration page and to LicenseServer.

Web UI

Changing these settings will cause the LicenseServer to restart and any currently running and licensed applications will be shut down!

Configure the host addresses where the web UI is available to administrators.

All interfaces and assigned IP addresses
 Local only (localhost)
 Only the following hostname or IP address:
Ensure this hostname or IP address exists or LicenseServer will fail to start!

Configure the port used for the web UI.

Dynamically chosen by the operating system
 Fixed port
Ensure this port is available or LicenseServer will fail to start!

Proxy Server

Configure the proxy server connection details if a proxy server is needed to communicate with Altova's servers.

Hostname
 Port Number If the port number is left blank the default port 1080 will be used.
 User Name
 Password Leave the user name and password blank if no authentication is required.

License Service

Configure the host addresses where the LicenseServer service is available to clients.

All interfaces and assigned IP addresses
 Local only (localhost)
 Only the following hostnames or IP addresses:
Ensure the hostnames or IP addresses exist or LicenseServer will fail to start!

- *Web UI*: Allowed IP addresses can vary from all interfaces and IP addresses on that machine to a fixed address, and ports can be either dynamically calculated or fixed. This allows a wide range of allowed IP-Address:Port settings. The default port setting is **8088**.
- *Proxy Server (available from v1.3 onwards)*: If a proxy server is being used to connect to the Internet, the details of the proxy server must be entered in the Proxy Server pane (see *screenshot above*). These fields need to be filled in only if a proxy server is being used. Also, proxy servers often do not need authentication (a user-name and password), in which case these two fields can be left blank. To configure LicenseServer for the proxy server, enter the proxy server's host name, and, if required, a port number.
- *License Service*: IP addresses can vary from all interfaces and IP addresses on that machine to a fixed address. If you list hostnames and/or IP addresses, use a comma-separated list without any spaces (for example: `hostname1, IPAddress1, hostname2`). The port number is fixed at **35355**.

By default, these settings allow unrestricted access to LicenseServer and its configuration page from within the networks to which LicenseServer is connected. If you wish to restrict access to

either LicenseServer or its configuration page, enter the appropriate settings and click **Save**.

Run a connectivity test (see *above*) to check that the settings are correct.

Alert Mail settings

Altova LicenseServer needs to be connected to the `altova.com` server. If the connection is broken for more than 24*5 hours (5 days), LicenseServer will not allow licenses. As a result, work sessions with Altova products licensed by LicenseServer could be disrupted.

In order to alert the administrator that a connection is broken, an alert mail can be sent to an email address. The Alert Mail pane (see *screenshot below*) is where you enter settings for sending alert mails to an administrator's email address.

Alert Mail

Configure email settings for communication with administrator.

SMTP Host

SMTP Port

User authentication

User password

From

To

Miscellaneous

Show hint how to receive evaluation licenses for a server product

Send a warning email if contact with a running product is lost.

SMTP Host and *SMTP Port* are the access details of the email server from which the email alert will be sent. *User Authentication* and *User Password* are the user's credentials for accessing the

email server. The *From* field takes the address of the email account from which the email will be sent. The *To* field takes the recipient's email address.

Click **Save** when done. After saving the Alert Mail settings, email alerts will be sent to the address specified whenever a significant event occurs, such as when connection to `altova.com` is lost. Note that such events are also recorded in the [Messages tab](#), and can be looked up there.

Miscellaneous settings

Show hints for receiving and deploying evaluation licenses

Checking this box (see *secreenshot above*) displays, at the top of the configuration page, brief instructions about how to evaluate and deploy evaluation licenses.

Send a warning email if contact with a running product is lost

A warning message is sent from the *From* address to the *To* address if a connection with a product that is licensed and running is lost.

Messages, Log Out

The **Messages** tab displays all messages relevant to licenses in the license pool of the LicenseServer. Each message has a **Delete** button that allows you to delete that particular message.

The **Log Out** tab serves as the Log Out button. Clicking the tab logs you out immediately and then displays the Login mask.

6.8 Password Reset

If you forget your LicenseServer password, you can use the `passwordreset` command from the CLI to reset the password to `default`.

1. Open a command line window.
2. Change to the directory where the LicenseServer application package or executable is installed.
3. Enter the command: `licenseserver passwordreset`
This resets the LicenseServer administrator password to `default`.
4. You can now log in to the Administrator Web UI with the password `default`.

Index

A

Administrator interface, 136

Administrator ports, 52

Alert emails, 147

Altova LicenseServer,

(see LicenseServer), 94

starting, 43

Altova ServiceController, 101

Assigning licenses, 131, 142

C

Caches, 84

Configuration page, 136

opening on Linux, 108

opening on Mac OS X, 111

opening on Windows, 105

URL of, 105

URL of (Linux), 108

URL of (Mac OS X), 111

D

Default password, 105

F

FlowForce Server,

registering with LicenseServer, 119

I

Installation on Linux, 20

Installation on Mac OS X, 29

Installation on Windows, 14

L

License Pool, 114, 137

Licenses,

assigning, 131, 142

uploading, 114, 137

LicenseServer,

Configuration page, 136

installation on Mac OS X, 100

installation on Windows, 97, 98

interface with, 136

registering FlowForce Server with, 119

registering MapForce Server with, 124

registering StyleVision Server with, 126

see Altova LicenseServer, 43

settings, 147

starting, 103

steps for assigning licenses, 102

LicenseServer configuration page,

(see Configuration page), 105, 108, 111

Licensing on Linux, 23

Licensing on Mac OS X, 32

Licensing on Windows, 16

Linux,

installation on, 20

licensing on, 23

Logout, 151

Logs, 82

M

Mac OS X,

installation on, 29

licensing on, 32

MapForce Server,

registering with LicenseServer, 124

Messages, 151

Mobile client ports, 52

Mobile clients,

information for, 58

MobileTogether Server, 3

installing, 12

MobileTogether Server, 3

- licensing, 12
- setting up, 12
- starting, 45
- using, 9

MobileTogether Server overview, 7**N****Network information, 96****Network settings, 147****P****Password,**

- default at startup, 105

Password policies, 77**Privileges, 54**

- descriptive list of, 56

R**Registering FlowForce Server with LicenseServer, 119****Registering MapForce Server with LicenseServer, 124****Registering StyleVision Server with LicenseServer, 126****Reports, 79****Roles, 54, 74****S****Server Management tab, 131, 142****Server Monitoring tab, 146****ServiceController, 101****Settings, 86, 147****Setup,**

- on Linux, 19
- on Mac OS X, 28
- on Windows, 13

SSL encryption, 36, 47**StyleVision Server,**

- registering with LicenseServer, 126

U**Uploading licenses, 114, 137****User licenses, 80****Users, 54, 70****W****Windows,**

- installation on, 14
- licensing on, 16