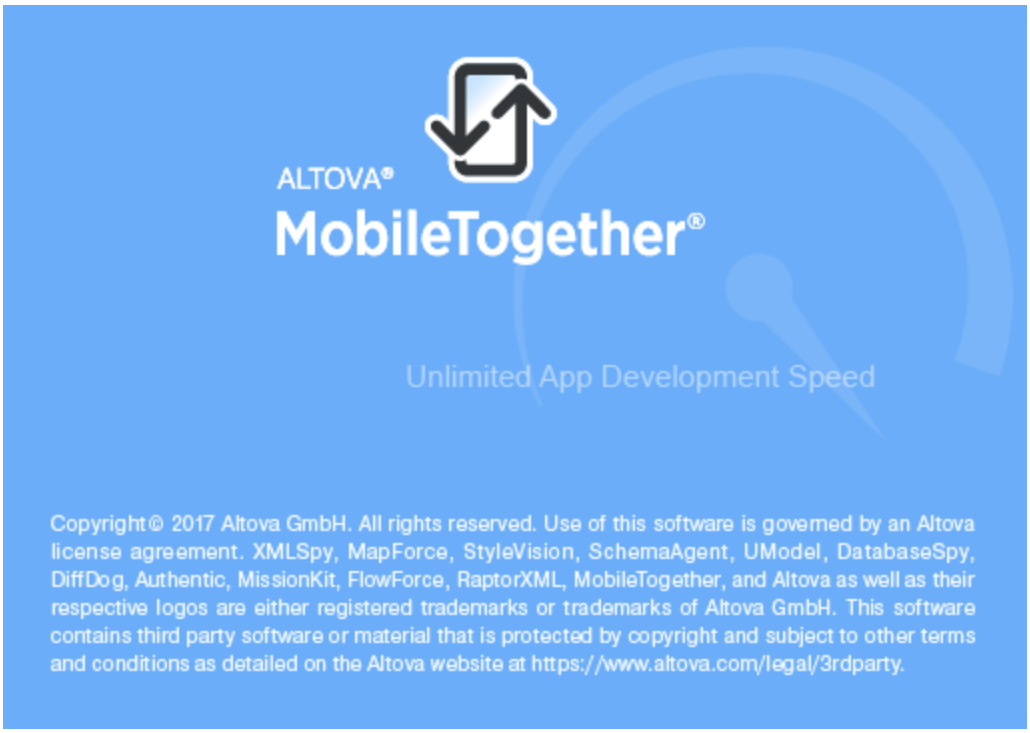
Manual del usuario



Manual del usuario y referencia de Altova MobileTogether Server

Fecha de publicación: 2018

Contenido

Altova MobileTogether Server

Altova MobileTogether Server Advanced Edition

1 Altova MobileTogether Server Advanced Edition

MobileTogether Server Advanced Edition (en adelante, MobileTogether Server) sirve soluciones de MobileTogether a dispositivos cliente y es compatible con Windows, Linux y macOS.

- Las soluciones de MobileTogether se crean en la aplicación de diseño MobileTogether Designer y desde esta aplicación se implementan en MobileTogether Server.
- La aplicación MobileTogether Client que está instalada en los dispositivos cliente acede a las soluciones MobileTogether que están implementadas en el servidor MobileTogether Server.

MobileTogether Server ofrece una sencilla interfaz web donde podrá gestionar los procesos del servidor y consultar registros. Este manual del usuario explica cómo se configura MobileTogether Server y cómo se gestionan sus procesos.

Información sobre este manual

Este manual está dividido en varias secciones:

- Introducción
- Instalación y configuración de MobileTogether Server
- Procedimientos del servidor
- Referencia de la interfaz web

- Uso de la línea de comandos
- Altova LicenseServer

Versión actual: 4.1

Última actualización: 26/02/2018

Altova MobileTogether Server

Introducción

2 Introducción

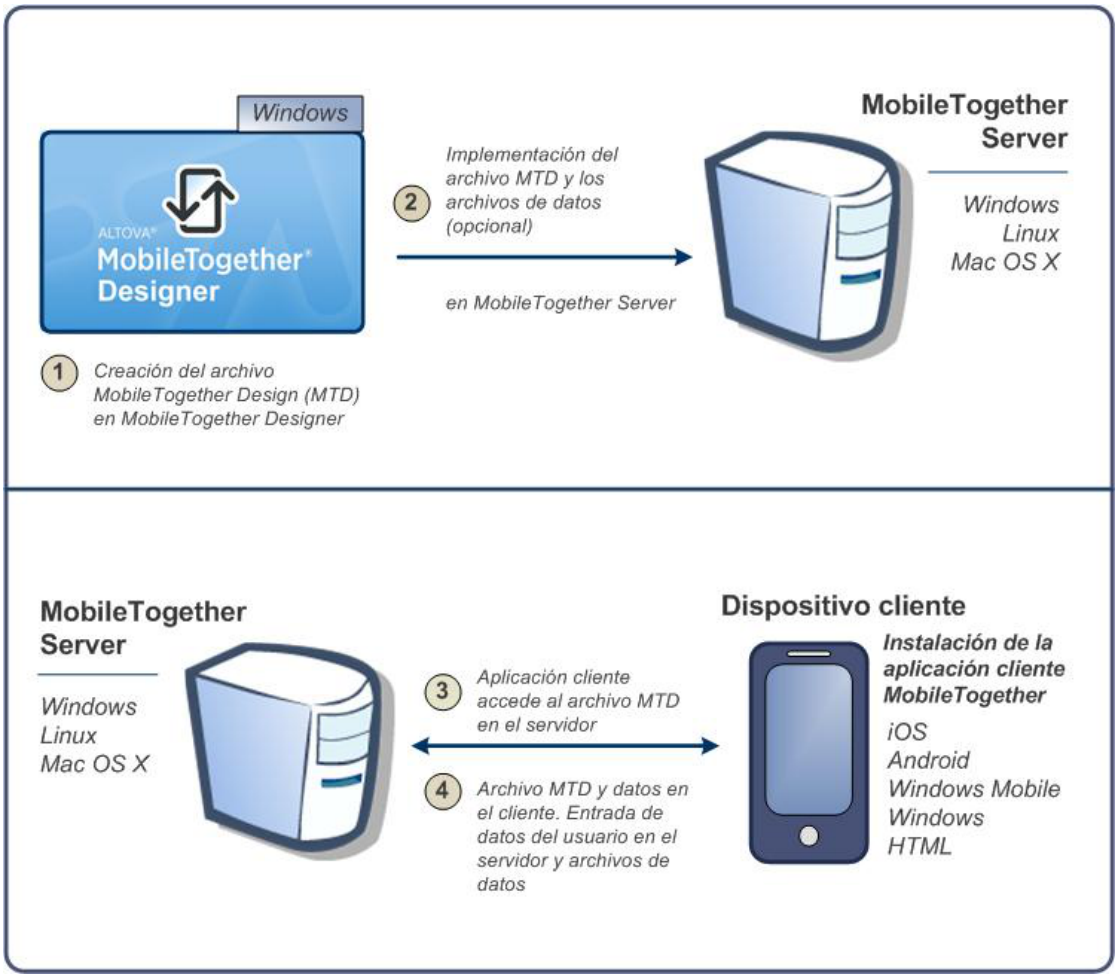
A modo de introducción puede consultar estos dos apartados:

- Información general sobre MobileTogether: aquí describimos el sistema MobileTogether y el papel que desempeña MobileTogether Server dentro del mismo.
- Funcionamiento de MobileTogether Server: instrucciones generales para configurar MobileTogether Server y utilizarlo con aplicaciones de MobileTogether Client.

2.1 Información general sobre MobileTogether

El sistema MobileTogether está compuesto por varios módulos:

- *MobileTogether Designer*: en este programa de diseño se crean las soluciones de MobileTogether. Desde aquí se implementan en el servidor MobileTogether Server (consulte el *Manual del usuario de MobileTogether Designer*).
- *MobileTogether Server*: este software servidor sirve las soluciones de MobileTogether a las aplicaciones MobileTogether Client que están instaladas en los dispositivos móviles (consulte la sección *Procedimientos del servidor* para obtener más información sobre las tareas de administración del servidor).
- Aplicación *MobileTogether Client (para dispositivos móviles)*: esta aplicación móvil se conecta a un servidor MobileTogether Server y accede a las soluciones de MobileTogether que estén implementadas en el mismo (consulte el *Manual del usuario de la aplicación MobileTogether Client*).



Requisitos del sistema

▼ MobileTogether Designer

Windows	Windows 7 SP1 con actualización de la plataforma, Windows 8, Windows 10
Windows Server	Windows Server 2008 R2 SP1 con actualización de la plataforma o superior

▼ MobileTogether Server

Windows	Windows 7 SP1 con actualización de la plataforma, Windows 8, Windows 10
Windows Server	Windows Server 2008 R2 SP1 con actualización de la plataforma o superior
Linux	• CentOS 6 o superior • RedHat 6 o superior • Debian 7 o superior • Ubuntu 12.04 o superior
(Mac) OS X, macOS	OS X10.10, 10.11, macOS 10.12 o superior

▼ MobileTogether Client

iOS	9 y superior para dispositivos móviles Apple
Android	4.0 y superior para dispositivos móviles Android
Windows RT, Metro	Windows 8.1 y 10; Windows RT para equipos y tabletas táctiles de Windows
HTML	Navegadores HTML para los demás dispositivos móviles

2.2 Funcionamiento de MobileTogether Server

Para poder utilizar MobileTogether Server con clientes MobileTogether es necesario:

- Instalar y configurar MobileTogether Server
- Implementar soluciones de MobileTogether desde MobileTogether Designer en MobileTogether Server
- Configurar las aplicaciones MobileTogether Client (en dispositivos móviles) para acceder a soluciones implementadas en MobileTogether Server

---

Los pasos concretos son:

1. Instalar MobileTogether Server

   MobileTogether Server funciona en sistemas Windows, Linux y macOS. Antes de instalar una versión nueva de MobileTogether Server, deberá desinstalar la versión previa. Para más información consulte estos apartados: Instalación en Windows, Instalación en Linux e Instalación en macOS.

2. Asignar licencias a MobileTogether Server

   Para asignar licencias a MobileTogether Server, primero debe conectarse a un servidor LicenseServer ubicado en su red. Inicie MobileTogether Server, registre MobileTogether Server con LicenseServer y asígnele una licencia. Para más información consulte estos apartados: Asignación de licencias en Windows, Asignación de licencias en Linux y Asignación de licencias en macOS.

3. Configurar cifrado SSL

   Si quiere cifrar la comunicación entre el servidor y los clientes puede configurar cifrado SSL para MobileTogether Server. Además deberá configurar las aplicaciones MobileTogether Client para que se puedan comunicar por SSL. Consulte *Manual del usuario de MobileTogether Client* para obtener más información.

4. Definir la configuración básica

   Defina opciones de configuración básica como los puertos del administrador y de los clientes y otras opciones de comunicación y seguridad.

5. Configurar cuentas de usuario

   A MobileTogether Server siempre se accede con una cuenta de usuario. Por tanto, es necesario configurar cuentas de usuario correctamente. Hay dos tipos de acceso:

   - *Acceso del administrador:* el administrador accede a MobileTogether Server por la interfaz web para llevar a cabo tareas administrativas como configuración

de las opciones de comunicación y de seguridad y gestión de cuentas de usuario.

- *Acceso del usuario final:* el usuario final accede a MobileTogether Server desde el dispositivo móvil y lo utiliza para descargar soluciones de MobileTogether en el cliente. Dependiendo de la cuenta de usuario utilizada, el usuario final podrá acceder a unas soluciones u otras.

6. Implementar soluciones de MobileTogether en MobileTogether Server

   Las soluciones de MobileTogether se implementan desde la aplicación MobileTogether Designer. Consulte el *Manual del usuario de MobileTogether Designer* para obtener más información.

7. Configurar las aplicaciones MobileTogether Client para acceder a MobileTogether Server

   Debe configurar las aplicaciones MobileTogether Client del dispositivo móvil para conectarse a MobileTogether Server. La información necesaria para configurar las aplicaciones MobileTogether Client se enumera en el apartado Información para clientes. También puede consultar el *Manual del usuario de MobileTogether Client* para obtener más información.

Dirección IP del servidor y configuración de red del servidor de seguridad
Su servidor puede tener una dirección IP pública (a la que se puede acceder por Internet) y privada (a la que se puede acceder desde una red privada, como la red inalámbrica de la red de su empresa). Si un cliente móvil intenta conectarse por Internet usando la dirección IP privada del servidor, la conexión no funcionará. Esto se debe a que la dirección IP privada no se conoce en Internet y no se puede resolver. Si utiliza una dirección IP privada, el dispositivo cliente debería tener acceso a la red privada.

Para asegurarse de que el acceso al servidor sea posible, tiene dos opciones:

- Asignar al servidor una dirección IP pública para que se pueda acceder a él por Internet. El dispositivo cliente debe utilizar esta dirección IP pública para acceder al servidor.
- Si utiliza un servidor de seguridad e instala MobileTogether Server en un servidor con una dirección IP privada (dentro de la red privada), utilice el servidor de seguridad de la red para reenviar las solicitudes a una combinación de puerto y dirección IP pública del servidor MobileTogether Server. El dispositivo cliente debe utilizar la dirección IP pública.

También debería asegurarse de configurar el servidor de seguridad para permitir acceso al puerto de servidor utilizado para la comunicación con MobileTogether Client. Los puertos que utiliza MobileTogether Server se especifican en la página Configuración de la interfaz web de MobileTogether Server. En el dispositivo cliente este es el puerto que se debe usar como puerto de servidor para el acceso.

Consejo: en la mayoría de los servidores de seguridad el puerto `80` está abierto por defecto.

Por tanto, si tiene problemas para configurar el servidor de seguridad y el puerto `80` no está conectado a ningún otro dispositivo, puede utilizarlo como puerto de MobileTogether Server para comunicarse con los clientes.

Altova MobileTogether Server

Instalación y configuración de MobileTogether Server

3 Instalación y configuración de MobileTogether Server

En esta sección describimos el proceso de instalación y de asignación de licencias, entre otros procedimientos de configuración. Esta sección incluye varios apartados:

- Instalación y configuración en Windows
- Instalación y configuración en Linux
- Instalación y configuración en macOS
- Configurar cifrado SSL

3.1 Instalación y configuración en Windows

Esta sección explica cómo instalar MobileTogether Server y asignarle licencias en sistemas Windows.

Instalación en Windows

- Requisitos del sistema
- Instalar MobileTogether Server
- Altova LicenseServer
- Versiones de LicenseServer
- Licencia de prueba
- Ubicación de la carpeta de aplicación

Asignación de licencias en Windows

- Iniciar el controlador de servicios ServiceController
- Iniciar LicenseServer
- Iniciar MobileTogether Server
- Registrar MobileTogether Server
- Asignar licencias

3.1.1 Instalación en Windows

El proceso de instalación y configuración de MobileTogether Server en Windows se describe a continuación.

▼ Requisitos del sistema

▼ *Windows*

Windows 7 SP1 con actualización de la plataforma, Windows 8, Windows 10

▼ *Windows Server*

Windows Server 2008 R2 SP1 con actualización de la plataforma o superior

▼ Instalar MobileTogether Server

Para instalar MobileTogether Server descargue el paquete de instalación del centro de descargas de Altova (http://www.altova.com/es/download.html), ejecútelo y siga las instrucciones que aparecen en pantalla.

Una vez completada la instalación, el ejecutable de MobileTogether Server estará en esta ubicación predeterminada:

```
<CarpetaArchivosPrograma>\Altova\MobileTogetherServer4.1\bin
```

\MobileTogetherServer.exe

- Altova LicenseServer

  - Para que MobileTogether Server funcione debe tener asignada una licencia desde un servidor Altova LicenseServer de la red.
  - El programa de instalación de MobileTogether Server para sistemas Windows ofrece una opción para descargar e instalar Altova LicenseServer junto con MobileTogether Server.
  - Si en la red ya hay instalado un servidor Altova LicenseServer, no necesita instalar otro LicenseServer a no ser que se necesite una versión más reciente (ver el siguiente apartado *versiones de LicenseServer*).
  - Durante el proceso de instalación de MobileTogether Server, puede seleccionar si también se instala Altova LicenseServer.

  Para más información sobre cómo registrar MobileTogether Server y asignarle licencias con Altova LicenseServer, consulte la sección Asignación de licencias en Windows.

- Versiones de LicenseServer

  - Los productos servidor de Altova deben tener una licencia con la versión de LicenseServer correspondiente a la versión de MobileTogether Server instalada o con una versión posterior de LicenseServer.
  - La versión de LicenseServer correspondiente a la versión de MobileTogether Server aparece en pantalla durante la instalación de MobileTogether Server. Puede instalar esta versión de LicenseServer junto con MobileTogether Server o puede instalar LicenseServer por separado.
  - Antes de instalar una versión nueva de LicenseServer, es necesario desinstalar versiones anteriores. El programa de instalación de LicenseServer se encarga de esto automáticamente si detecta versiones más recientes en el sistema.
  - Las versiones de LicenseServer son compatibles y funcionan con versiones más antiguas de MobileTogether Server.
  - Si instala una versión nueva de MobileTogether Server y la versión de LicenseServer que está instalada es anterior a la que le corresponde, instale la versión más reciente que está siempre disponible en el sitio web de Altova.
  - Cuando se desinstala LicenseServer, todos los datos de registro y asignación de licencias almacenados en la versión antigua de LicenseServer se guardan en una base de datos en el equipo servidor. Estos datos se importan de forma automática a la siguiente versión que se instale en el equipo.
  - El número de versión de LicenseServer siempre aparece al final de la página de configuración de LicenseServer.

    Versión actual: 2.5

- Licencia de prueba

  Durante el proceso de instalación tendrá la opción de solicitar una licencia de prueba de 30

días para MobileTogether Server. Altova le enviará un correo electrónico con la licencia de prueba a la dirección de correo que usted indique en el formulario.

▼ Ubicación de la carpeta de la aplicación

La aplicación se instalará en esta carpeta:

Windows 7, 8 y 10	`C:\Archivos de programa\Altova\`
Versión de 32 bits en sistemas operativos de 64 bits	`C:\Archivos de programa (x86)\Altova\`

3.1.2 Asignación de licencias en Windows

Para poder trabajar con MobileTogether Server es necesario asignarle una licencia con Altova LicenseServer. La asignación de licencias es un proceso de dos pasos:

1. El primero consiste en **registrar MobileTogether Server** con LicenseServer desde MobileTogether Server.
2. El segundo paso consiste en **asignar una licencia** a MobileTogether Server desde LicenseServer.

A continuación encontrará información más detallada al respecto.

▼ Iniciar el controlador de servicios ServiceController

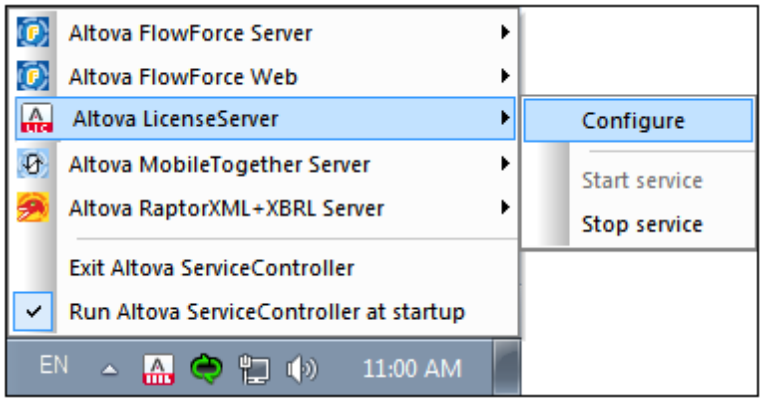
Altova ServiceController se inicia para arrancar Altova LicenseServer y Altova MobileTogether Server.

Altova ServiceController (en adelante *ServiceController*) es una práctica aplicación que sirve para iniciar, detener y configurar los servicios de Altova **en sistemas Windows**.

ServiceController se instala con Altova LicenseServer y con *los productos servidor de Altova que se instalan como servicios* (FlowForce Server, RaptorXML(+XBRL) Server y Mobile Together Server). Se puede iniciar haciendo clic en **Inicio | Altova LicenseServer | Altova ServiceController**. (Este comando también está en las carpetas del menú **Inicio** de *los productos servidor de Altova que se instalan como servicios* (FlowForce Server, RaptorXML(+XBRL) Server y Mobile Together Server).) Una vez iniciado, podrá acceder a ServiceController desde la bandeja del sistema (*imagen siguiente*).

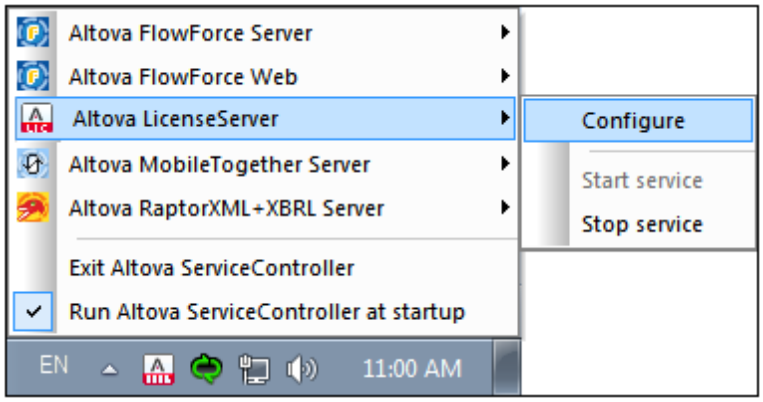
Si quiere que ServiceController se inicie automáticamente nada más iniciar sesión en el sistema, haga clic en el icono de ServiceController de la bandeja del sistema para abrir el menú de opciones de **ServiceController** (*imagen siguiente*) y active la opción **Run Altova**

ServiceController at Startup (*Ejecutar Altova ServiceController al inicio*), que de todas maneras es la opción predeterminada. Para cerrar ServiceController haga clic en el icono de ServiceController de la bandeja del sistema y en el menú haga clic en la opción **Exit Altova ServiceController** (Salir de Altova ServiceController).



- Iniciar LicenseServer

  Para iniciar LicenseServer haga clic en el icono de **ServiceController** en la bandeja del sistema, pase el puntero del ratón por encima de la opción **Altova LicenseServer** del menú emergente (*imagen siguiente*) y seleccione el comando **Start service** en el submenú. Si LicenseServer ya está en ejecución, este comando estará deshabilitado.



- Registrar MobileTogether Server

  Para registrar MobileTogether Server desde la interfaz de la línea de comandos utilice el comando `licenseserver`:

  `MobileTogetherServer licenseserver [opciones]` *`NombreServidor-O--Dirección-IP`*

  Por ejemplo, si `localhost` es el nombre del servidor donde está instalado LicenseServer:

  `MobileTogetherServer licenseserver localhost`

  Otra opción es registrar MobileTogether Server desde la pestaña Opciones de la interfaz web

de MobileTogether Server. Estos son los pasos que debe seguir: (i) Inicie MobileTogether Server con el controlador de servicios de Altova ServiceController (*véase el punto anterior*); (ii) Introduzca la contraseña para acceder a la página de configuración web; (iii) Seleccione el nombre o la dirección del servidor LicenseServer y haga clic en el botón **Registrarse con LicenseServer**.

Una vez finalizado el proceso de registro, abra la pestaña de gestión de servidores de la página de configuración de LicenseServer para asignar una licencia a MobileTogether Server.

▼ Asignar licencias

Tras registrarse con LicenseServer, MobileTogether Server aparecerá en la lista de la pestaña de gestión de servidores **Server Management** de la página de configuración de LicenseServer. En esta pestaña puede asignar una licencia a MobileTogether Server.

Nota sobre núcleos y licencias
La asignación de licencias a productos servidor de Altova depende de cuántos núcleos de procesador tiene el equipo donde se ejecuta el producto servidor de Altova. Por ejemplo, un procesador dual tiene dos núcleos, un procesador *quad* tiene cuatro núcleos, un procesador *hexa-core* tiene seis núcleos, y así sucesivamente. El número de núcleos de la licencia asignada a un producto debe ser mayor o igual al número de núcleos disponibles en dicho equipo servidor, ya sea un servidor físico o un equipo virtual.

Por ejemplo, si un servidor tiene ocho núcleos (un procesador *octa-core*), deberá comprar una licencia para ocho núcleos. También puede combinar varias licencias para alcanzar el número de núcleos necesario. Es decir, puede usar dos licencias para cuatro núcleos para un servidor *octa-core* en lugar de una licencia para ocho núcleos, por ejemplo.

Si usa un equipo servidor con gran cantidad de núcleos, pero tiene un bajo volumen de procesamiento, también puede crear un equipo virtual que tenga adjudicados menos núcleos y comprar una licencia para ese menor número de núcleos. No obstante, dicha implementación será menos rápida que si utilizara todos los núcleos disponibles en el servidor.

Nota: cada licencia de los productos servidor de Altova se puede usar de forma simultánea en un equipo como máximo (en el equipo donde está instalado el producto servidor de Altova), incluso si la capacidad de la licencia no está agotada. Por ejemplo, si utiliza una licencia para 10 núcleos para un equipo cliente que tiene 6 núcleos, los 4 núcleos restantes de la licencia no se pueden usar simultáneamente en otro equipo cliente.

Nota: debido a sus funciones de servicios, MobileTogether Server Advanced Edition solo puede ejecutarse en equipos con **dos o más núcleos**.

Licencias de MobileTogether Server
Las licencias de MobileTogether Server funciona en base al número de núcleos CPU que tenga el equipo donde se ejecuta MobileTogether Server. Las licencias basadas en el número de núcleos permiten conectar un número ilimitado de dispositivos al servidor. Sin embargo, si marca la casilla *Limit to single thread execution*, entonces solo se podrá conectar a MobileTogether Server un máximo de un dispositivo. Esto puede ser útil en tareas de evaluación y de pruebas a pequeña escala. No obstante, si estando marcada esta casilla, se conecta otro dispositivo a MobileTogether Server, este otro dispositivo se hará con la licencia. El primer dispositivo ya no se podrá conectar y recibirá un mensaje de error

a tal efecto.

3.2 Instalación y configuración en Linux

Esta sección explica cómo instalar MobileTogether Server y asignarle licencias en sistemas Linux (Debian, Ubuntu, CentOS, RedHat).

Instalación en Linux

- Requisitos del sistema
- Desinstalar versiones antiguas de los productos servidor de Altova
- Descargar el paquete de instalación para Linux
- Instalar MobileTogether Server
- Altova LicenseServer
- Versiones de LicenseServer
- Licencia de prueba

Asignación de licencias en Linux

- Iniciar LicenseServer
- Iniciar MobileTogether Server
- Registrar MobileTogether Server
- Asignar licencias

3.2.1 Instalación en Linux

El proceso de instalación y configuración de MobileTogether Server en Linux se describe a continuación.

▼ Requisitos del sistema

▼ *Linux*

- CentOS 6 o superior
- RedHat 6 o superior
- Debian 7 o superior
- Ubuntu 12.04 o superior

Las bibliotecas que aparecen a continuación son un requisito previo para la instalación y ejecución de la aplicación. Si los paquetes que aparecen en esta tabla no están en su equipo Linux, ejecute el comando `yum` (o `apt-get` si procede) para instalarlos.

Requisito para	CentOS, RedHat	Debian	Ubuntu
LicenseServer	krb5-libs	libgssapi-krb5-2	libgssapi-krb5-2
MobileTogether Server Advanced Edition	qt4, krb5-libs, qt-x11	libqtgui4, libgssapi-krb5-2	libqtgui4, libgssapi-krb5-2

▼ Desinstalar versiones antiguas de los productos servidor de Altova

En la interfaz de la línea de comandos de Linux puede comprobar si ya hay productos servidor de Altova instalados en el equipo. Para ello use este comando:

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

Si MobileTogether Server no está instalado, continúe con la instalación tal y como se describe más abajo.

Si MobileTogether Server ya está instalado y quiere instalar una versión más reciente, antes debe desinstalar la versión previa con este comando:

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

Si quiere desinstalar una versión previa de Altova LicenseServer, use este comando:

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

Descargar el paquete de instalación para Linux

Los paquetes de instalación de MobileTogether Server para sistemas Linux se pueden descargar del sitio web de Altova.

Distribución	Extensión del paquete
Debian 7 y superior	`.deb`
Ubuntu12.04 y superior	`.deb`
CentOS 6 y superior	`.rpm`
RedHat 6 y superior	`.rpm`

Tras descargarlo, copie el paquete de instalación en cualquier directorio del sistema Linux. Para ejecutar MobileTogether Server es necesario tener instalado Altova LicenseServer, que también se puede descargar del sitio web de Altova.

Instalar MobileTogether Server

En una ventana de la Terminal, cambie al directorio donde copió el paquete de instalación para Linux. Por ejemplo, si lo copió en un directorio del usuario llamado `MiAltova` (ubicado en `/home/User` por ejemplo), cambie a ese directorio con esta línea de comandos:

```
cd /home/User/MiAltova
```

Instale MobileTogether Server con este comando:

```
[Debian]:   sudo dpkg --install mobiletogetherserver-4.1-debian.deb
[Ubuntu]:   sudo dpkg --install mobiletogetherserver-4.1-ubuntu.deb
[CentOS]:   sudo rpm -ivh mobiletogetherserver-4.1-1.x86_64.rpm
[RedHat]:   sudo rpm -ivh mobiletogetherserver-4.1-1.x86_64.rpm
```

La aplicación MobileTogether Server se instala en este directorio:

```
/opt/Altova/MobileTogetherServer4.1
```

- Altova LicenseServer

  Para poder ejecutar los productos servidores de Altova, incluido MobileTogether Server, es necesario asignarles una licencia con un servidor Altova LicenseServer de la red.

  En los sistemas Linux es necesario instalar Altova LicenseServer por separado. Por tanto, descargue Altova LicenseServer del sitio web de Altova y copie el paquete de instalación en cualquier directorio. Siga las instrucciones anteriores para instalar LicenseServer (*ver apartado anterior*).

```
[Debian]:   sudo dpkg --install licenseserver-2.5-debian.deb
[Ubuntu]:   sudo dpkg --install licenseserver-2.5-ubuntu.deb
[CentOS]:   sudo rpm -ivh licenseserver-2.5-1.x86_64.rpm
[RedHat]:   sudo rpm -ivh licenseserver-2.5-1.x86_64.rpm
```

  La aplicación LicenseServer se instala en este directorio:

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

  Consulte el apartado siguiente Asignación de licencias en Linux para obtener información sobre cómo registrar MobileTogether Server con Altova LicenseServer y asignarle licencias.

- Versiones de LicenseServer

  - Los productos servidor de Altova deben tener una licencia con la versión de LicenseServer correspondiente a la versión de MobileTogether Server instalada o con una versión posterior de LicenseServer.
  - La versión de LicenseServer correspondiente a la versión de MobileTogether Server aparece en pantalla durante la instalación de MobileTogether Server. Puede instalar esta versión de LicenseServer junto con MobileTogether Server o puede instalar LicenseServer por separado.
  - Antes de instalar una versión nueva de LicenseServer, es necesario desinstalar versiones anteriores. El programa de instalación de LicenseServer se encarga de esto automáticamente si detecta versiones más recientes en el sistema.
  - Las versiones de LicenseServer son compatibles y funcionan con versiones más antiguas de MobileTogether Server.
  - Si instala una versión nueva de MobileTogether Server y la versión de LicenseServer que está instalada es anterior a la que le corresponde, instale la versión más reciente que está siempre disponible en el sitio web de Altova.
  - Cuando se desinstala LicenseServer, todos los datos de registro y asignación de licencias almacenados en la versión antigua de LicenseServer se guardan en una base de datos en el equipo servidor. Estos datos se importan de forma automática a la siguiente versión que se instale en el equipo.
  - El número de versión de LicenseServer siempre aparece al final de la página de configuración de LicenseServer.

    Versión actual: 2.5

- Licencia de prueba

  Durante el proceso de instalación tendrá la opción de solicitar una licencia de prueba de 30 días para MobileTogether Server. Altova le enviará un correo electrónico con la licencia de prueba a la dirección de correo que indique en el formulario.

3.2.2 Asignación de licencias en Linux

Para poder trabajar con MobileTogether Server es necesario asignarle una licencia con Altova LicenseServer. La asignación de licencias es un proceso de dos pasos:

1. El primero consiste en **registrar MobileTogether Server** con LicenseServer desde MobileTogether Server.
2. El segundo paso consiste en **asignar una licencia** a MobileTogether Server desde LicenseServer.

A continuación encontrará información más detallada al respecto.

- Iniciar LicenseServer

  Para poder registrar MobileTogether Server con LicenseServer y asignarle una licencia, LicenseServer debe estar en ejecución como servicio. Inicie LicenseServer como servicio con este comando:

[< Debian 8]	**sudo /etc/init.d/licenseserver start**
[≥ Debian 8]	**sudo systemctl start licenseserver**
[< CentOS 7]	**sudo initctl start licenseserver**
[≥ CentOS 7]	**sudo systemctl start licenseserver**
[< Ubuntu 15]	**sudo initctl start licenseserver**
[≥ Ubuntu 15]	**sudo systemctl start licenseserver**
[RedHat]	**sudo initctl start licenseserver**

  Si por cualquier motivo necesita detener LicenseServer, use el mismo comando pero sustituya **stop** por **start**. Por ejemplo:

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

- Iniciar MobileTogether Server

  Inicie MobileTogether Server como demonio con este comando:

[< Debian 8]	**sudo /etc/init.d/mobiletogetherserver start**
[≥ Debian 8]	**sudo systemctl start mobiletogetherserver**
[< CentOS 7]	**sudo initctl start mobiletogetherserver**
[≥ CentOS 7]	**sudo systemctl start mobiletogetherserver**
[< Ubuntu 15]	**sudo initctl start mobiletogetherserver**
[≥ Ubuntu 15]	**sudo systemctl start mobiletogetherserver**
[RedHat]	**sudo initctl start mobiletogetherserver**

Cuando se inicia por primera vez, MobileTogether Server se inicia en un puerto aleatorio y abre la página de configuración de la interfaz gráfica.

Si el explorador web está en el mismo equipo que MobileTogether Server, la URL de la página de configuración es:

file:///var/opt/Altova/MobileTogetherServer2018/MobileTogetherweb.html

Si el explorador web está en otro equipo, puede extraer la URL de la página de configuración del archivo de registro:

grep running /var/opt/Altova/MobileTogetherServer2018/data/mtweb.log

- Registrar MobileTogether Server

  Para registrar MobileTogether Server desde la interfaz de la línea de comandos utilice el comando `licenseserver`:

  sudo /opt/Altova/MobileTogetherServer4.1/bin/mobiletogetherserver licenseserver [opciones] *NombreServidor-O-Dirección-IP*

  Por ejemplo, si el nombre del servidor donde está instalado LicenseServer es `localhost`:

  sudo /opt/Altova/MobileTogetherServer4.1/bin/mobiletogetherserver licenseserver localhost

  En el comando anterior `localhost` es el nombre del servidor donde está instalado LicenseServer. Observe también la ubicación del ejecutable de MobileTogether Server:

  /opt/Altova/MobileTogetherServer4.1/bin/

  Otra opción es registrar MobileTogether Server desde la pestaña Opciones de la interfaz web de MobileTogether Server. Estos son los pasos que debe seguir: (i) Inicie MobileTogether Server con el controlador de servicios de Altova ServiceController (*véase el punto anterior*); (ii) Introduzca la contraseña para acceder a la página de configuración web; (iii) Seleccione el nombre o la dirección del servidor LicenseServer y haga clic en el botón **Registrarse con LicenseServer**.

  Una vez completado el registro, abra la pestaña **Server Management** de la página de configuración de LicenseServer para asignar una licencia a MobileTogether Server.

- Asignar licencias

  Tras registrarse con LicenseServer, MobileTogether Server aparecerá en la lista de la

pestaña de gestión de servidores **Server Management** de la página de configuración de LicenseServer. En esta pestaña puede asignar una licencia a MobileTogether Server.

Nota sobre núcleos y licencias
La asignación de licencias a productos servidor de Altova depende de cuántos núcleos de procesador tiene el equipo donde se ejecuta el producto servidor de Altova. Por ejemplo, un procesador dual tiene dos núcleos, un procesador *quad* tiene cuatro núcleos, un procesador *hexa-core* tiene seis núcleos, y así sucesivamente. El número de núcleos de la licencia asignada a un producto debe ser mayor o igual al número de núcleos disponibles en dicho equipo servidor, ya sea un servidor físico o un equipo virtual.

Por ejemplo, si un servidor tiene ocho núcleos (un procesador *octa-core*), deberá comprar una licencia para ocho núcleos. También puede combinar varias licencias para alcanzar el número de núcleos necesario. Es decir, puede usar dos licencias para cuatro núcleos para un servidor *octa-core* en lugar de una licencia para ocho núcleos, por ejemplo.

Si usa un equipo servidor con gran cantidad de núcleos, pero tiene un bajo volumen de procesamiento, también puede crear un equipo virtual que tenga adjudicados menos núcleos y comprar una licencia para ese menor número de núcleos. No obstante, dicha implementación será menos rápida que si utilizara todos los núcleos disponibles en el servidor.

Nota: cada licencia de los productos servidor de Altova se puede usar de forma simultánea en un equipo como máximo (en el equipo donde está instalado el producto servidor de Altova), incluso si la capacidad de la licencia no está agotada. Por ejemplo, si utiliza una licencia para 10 núcleos para un equipo cliente que tiene 6 núcleos, los 4 núcleos restantes de la licencia no se pueden usar simultáneamente en otro equipo cliente.

Nota: debido a sus funciones de servicios, MobileTogether Server Advanced Edition solo puede ejecutarse en equipos con **dos o más núcleos**.

Licencias de MobileTogether Server
Las licencias de MobileTogether Server funciona en base al número de núcleos CPU que tenga el equipo donde se ejecuta MobileTogether Server. Las licencias basadas en el número de núcleos permiten conectar un número ilimitado de dispositivos al servidor. Sin embargo, si marca la casilla *Limit to single thread execution*, entonces solo se podrá conectar a MobileTogether Server un máximo de un dispositivo. Esto puede ser útil en tareas de evaluación y de pruebas a pequeña escala. No obstante, si estando marcada esta casilla, se conecta otro dispositivo a MobileTogether Server, este otro dispositivo se hará con la licencia. El primer dispositivo ya no se podrá conectar y recibirá un mensaje de error a tal efecto.

3.2.3 Notas sobre configuración del entorno

Carpetas

A continuación enumeramos carpetas importantes de su sistema MobileTogether Server.

- *Directorio raíz de instalación*

  /opt/Altova/MobileTogetherServer4.1/

- *Archivos de bases de datos, licencias y soluciones*

  /var/opt/Altova/MobileTogetherServer

- *Parámetros del entorno*

  /etc/profile.d/jdbc.sh
  El archivo de parámetros del entorno debe definirse en función del entorno de cada usuario. La ruta de acceso anterior es un ejemplo solamente.
  Nota: el archivo de parámetros del entorno establece las variables para **todos los usuarios** del sistema.

Bases de datos basadas en archivos

Las bases de datos basadas en archivos (como las bases de datos SQLite) deben residir en la carpeta que se definió en la pestaña ***Opciones*** de MobileTogether Server como directorio de trabajo del lado servidor. La carpeta predeterminada para este tipo de bases de datos es:

/var/opt/Altova/MobileTogetherServer/SolutionFiles

Conexiones JDBC

Cuando trabaje con este tipo de conexiones debe tener en cuenta estos aspectos:

- Debe tener instalado Java Runtime Environment o el kit de desarrollo de software.
- Debe tener instalados controladores JDBC para la base de datos de destino.
- Debe establecer correctamente estas variables de entorno:
  - `CLASSPATH`: para encontrar los archivos jar.
  - `PATH`: para buscar el entorno JRE, aunque a veces no es necesaria, dependiendo de la instalación.
  - `JAVA_HOME`: a veces no es necesaria, dependiendo de la instalación.

Nota
En servidores Linux solamente son compatibles las conexiones de base de datos de tipo JDBC.

Lista de archivos importantes

Puede copiar este script de shell en la carpeta **/opt/Altova/MobileTogetherServer4.1/etc**

para no sobrescribir los archivos de configuración actuales. Realice los cambios que necesite en el script. Las partes que aparecen resaltadas en azul son propias del entorno y deberán ajustarse.

- Script de shell

```
#- 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/iseries/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:./:
```

3.3 Instalación y configuración en macOS

Esta sección explica cómo instalar MobileTogether Server y asignarle licencias en sistemas macOS.

Instalación en macOS

- Requisitos del sistema
- Desinstalar versiones previas de productos servidor de Altova
- Descargar el paquete de instalación para macOS
- Instalar MobileTogether Server
- Altova LicenseServer
- Versiones de LicenseServer
- Licencia de prueba

Asignación de licencias en macOS

- Iniciar LicenseServer
- Iniciar MobileTogether Server
- Registrar MobileTogether Server
- Asignar licencias

3.3.1 Instalación en macOS

El proceso de instalación y configuración de MobileTogether Server en macOS se describe a continuación.

▼ Requisitos del sistema

▼ *(Mac) OS X, macOS*

OS X 10.10 o superior
Java for OS X, macOS (versión más reciente)

▼ Instalar Java for OS X, macOS

Para poder ejecutar MobileTogether Server es necesario tener instalado Java para OS X, macOS. Puede encontrar la versión más reciente en http://support.apple.com/kb/DL1572. Para saber cuál es la versión de Java más reciente para OS X, macOS que ofrece Apple, busque Java para OS X, macOS en el sitio web de Apple (puede que esta versión de Java no sea la más reciente de Sun Microsystems, pero se trata de la versión que necesita instalar.)

▼ Desinstalar versiones antiguas de los productos servidor de Altova

Antes de desinstalar MobileTogether Server es necesario detener el servicio con este comando:

```
sudo launchctl unload /Library/LaunchDaemons/
```

```
com.altova.MobileTogetherServer4.1.plist
```

Para comprobar si el servicio se detuvo correctamente, abra la terminal del Monitor de actividad y compruebe que MobileTogether Server no está en la lista. En la terminal de Aplicaciones haga clic con el botón derecho en el icono de MobileTogether Server y seleccione **Mover a la papelera**. La aplicación se envía a la papelera pero debe quitar la aplicación de la carpeta `usr`. Para ello puede utilizar este comando:

```
sudo rm -rf /usr/local/Altova/MobileTogetherServer4.1/
```

Si necesita desinstalar una versión antigua de Altova LicenseServer, antes debe detener el servicio con este comando:

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

Para comprobar si el servicio se detuvo correctamente, abra la terminal del Monitor de actividad y confirme que LicenseServer no está en la lista. Después desinstale LicenseServer siguiendo las instrucciones dadas más arriba para MobileTogether Server.

- Descargar el archivo de imagen de disco

  Descargue el archivo de imagen de disco (`.dmg`) del sitio web de Altova (http://www.altova.com/es/download.html).

- Instalar MobileTogether Server

  Haga clic en el archivo de imagen de disco (`.dmg`) para abrirlo. El programa de instalación de MobileTogether Server aparece como unidad virtual en el equipo. En esta unidad virtual nueva haga doble clic en el paquete de instalación (`.pkg`). Siga las instrucciones que aparecen en pantalla y acepte el contrato de licencia. Para expulsar la unidad cuando termine la instalación, haga clic con el botón derecho en la unidad y seleccione **Expulsar**.

  El paquete de MobileTogether Server se instalará en esta carpeta:
  `/usr/local/Altova/MobileTogetherServer4.1` (archivos binarios de la aplicación)
  `/var/Altova/MobileTogetherServer` (archivos de datos como bases de datos y registros)

  El demonio de MobileTogether Server se inicia automáticamente después de la instalación y de que se reinicie el equipo. Puede iniciar MobileTogether Server como demonio con este comando:

  ```
  sudo launchctl load /Library/LaunchDaemons/
  com.altova.MobileTogetherServer4.1.plist
  ```

  Tras iniciar el demonio MobileTogether Server, podrá abrir la página de la interfaz web de MobileTogether Server para configurar MobileTogether Server (en la carpeta **Aplicaciones** haga doble clic en el icono de MobileTogether Server).

- Altova LicenseServer

Para poder ejecutar los productos servidor de Altova, incluido MobileTogether Server, es necesario asignarles una licencia desde un servidor Altova LicenseServer que esté instalado en la red.

El paquete de instalación de Altova LicenseServer está disponible en la unidad virtual creado en el paso anterior. Para instalar Altova LicenseServer haga doble clic en el paquete de instalación que está en la unidad virtual y siga las instrucciones que aparecen en pantalla. También debe aceptar el contrato de licencia para poder continuar con la instalación.

Altova LicenseServer también puede descargarse desde el sitio web de Altova (http://www.altova.com/es/download.html) e instalarse por separado.

El paquete de LicenseServer se instalará en esta carpeta:
`/usr/local/Altova/LicenseServer`

Para obtener más información sobre cómo registrar MobileTogether Server con Altova LicenseServer y asignarle una licencia, consulte el apartado Asignación de licencias en macOS.

Versiones de LicenseServer

- Los productos servidor de Altova deben tener una licencia con la versión de LicenseServer correspondiente a la versión de MobileTogether Server instalada o con una versión posterior de LicenseServer.
- La versión de LicenseServer correspondiente a la versión de MobileTogether Server aparece en pantalla durante la instalación de MobileTogether Server. Puede instalar esta versión de LicenseServer junto con MobileTogether Server o puede instalar LicenseServer por separado.
- Antes de instalar una versión nueva de LicenseServer, es necesario desinstalar versiones anteriores. El programa de instalación de LicenseServer se encarga de esto automáticamente si detecta versiones más recientes en el sistema.
- Las versiones de LicenseServer son compatibles y funcionan con versiones más antiguas de MobileTogether Server.
- Si instala una versión nueva de MobileTogether Server y la versión de LicenseServer que está instalada es anterior a la que le corresponde, instale la versión más reciente que está siempre disponible en el sitio web de Altova.
- Cuando se desinstala LicenseServer, todos los datos de registro y asignación de licencias almacenados en la versión antigua de LicenseServer se guardan en una base de datos en el equipo servidor. Estos datos se importan de forma automática a la siguiente versión que se instale en el equipo.
- El número de versión de LicenseServer siempre aparece al final de la página de configuración de LicenseServer.

Versión actual: 2.5

Licencia de prueba

Durante el proceso de instalación tendrá la opción de solicitar una licencia de prueba de 30 días para MobileTogether Server. Altova le enviará un correo electrónico con la licencia de prueba a la dirección de correo que indique en el formulario.

3.3.2 Asignación de licencias en macOS

Para poder trabajar con MobileTogether Server es necesario asignarle una licencia con Altova LicenseServer. La asignación de licencias es un proceso de dos pasos:

1. El primero consiste en **registrar MobileTogether Server** con LicenseServer desde MobileTogether Server.
2. El segundo paso consiste en **asignar una licencia** a MobileTogether Server desde LicenseServer.

A continuación encontrará información más detallada al respecto.

▼ Iniciar LicenseServer

Para registrar y asignar una licencia correctamente a MobileTogether Server, LicenseServer debe estar en ejecución como demonio. Inicie LicenseServer como demonio con este comando:

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

Si por cualquier motivo necesita detener LicenseServer, use el mismo comando pero sustituya **load** por **unload**. Por ejemplo:

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

▼ Iniciar MobileTogether Server

El demonio de MobileTogether Server se inicia automáticamente tras instalarlo y reiniciar el equipo. Use este comando para iniciar MobileTogether Server como demonio:

```
sudo launchctl load /Library/LaunchDaemons/
com.altova.MobileTogetherServer4.1.plist
```

Si necesita detener MobileTogether Server por cualquier motivo, use este comando:

```
sudo launchctl unload /Library/LaunchDaemons/
com.altova.MobileTogetherServer4.1.plist
```

Para configurar MobileTogether Server, abra su interfaz web (Opciones) de una de las siguientes maneras:

- Abra en el Finder la carpeta de aplicaciones y haga doble clic en el icono de MobileTogether Server <%MTVERSION%
- Introduzca la URL de la página de la interfaz web en la barra de direcciones de un navegador web: **http://*<serverIPAddressOrName>*:8085**

Nota sobre el servidor de seguridad (firewall)
Asegúrese de que el servidor de seguridad no bloquea la dirección del puerto.

Registrar MobileTogether Server

Para registrar MobileTogether Server desde la interfaz de la línea de comandos utilice el comando `licenseserver`:

```
sudo /usr/local/Altova/MobileTogetherServer4.1/bin/MobileTogetherServer
licenseserver [opciones] NombreServidor-O-Dirección-IP
```

Por ejemplo, si el nombre del servidor donde está instalado LicenseServer es `localhost`:

```
sudo /usr/local/Altova/MobileTogetherServer4.1/bin/MobileTogetherServer
licenseserver localhost
```

En el comando anterior `localhost` es el nombre del servidor donde está instalado LicenseServer. Observe también la ubicación del ejecutable de MobileTogether Server:

```
/usr/local/Altova/MobileTogetherServer4.1/bin/
```

Otra opción es registrar MobileTogether Server desde la pestaña Opciones de la interfaz web de MobileTogether Server. Estos son los pasos que debe seguir: (i) Inicie MobileTogether Server con el controlador de servicios de Altova ServiceController (*véase el punto anterior*); (ii) Introduzca la contraseña para acceder a la página de configuración web; (iii) Seleccione el nombre o la dirección del servidor LicenseServer y haga clic en el botón **Registrarse con LicenseServer**.

Una vez completado el registro, abra la pestaña **Server Management** de la página de configuración de LicenseServer para asignar una licencia a MobileTogether Server..

Asignar licencias

Tras registrarse con LicenseServer, MobileTogether Server aparecerá en la lista de la pestaña de gestión de servidores **Server Management** de la página de configuración de LicenseServer. En esta pestaña puede asignar una licencia a MobileTogether Server.

Nota sobre núcleos y licencias
La asignación de licencias a productos servidor de Altova depende de cuántos núcleos de procesador tiene el equipo donde se ejecuta el producto servidor de Altova. Por ejemplo, un procesador dual tiene dos núcleos, un procesador *quad* tiene cuatro núcleos, un procesador *hexa-core* tiene seis núcleos, y así sucesivamente. El número de núcleos de la licencia asignada a un producto debe ser mayor o igual al número de núcleos disponibles en dicho equipo servidor, ya sea un servidor físico o un equipo virtual.

Por ejemplo, si un servidor tiene ocho núcleos (un procesador *octa-core*), deberá comprar una licencia para ocho núcleos. También puede combinar varias licencias para alcanzar el número de núcleos necesario. Es decir, puede usar dos licencias para cuatro núcleos para un servidor *octa-core* en lugar de una licencia para ocho núcleos, por ejemplo.

Si usa un equipo servidor con gran cantidad de núcleos, pero tiene un bajo volumen de procesamiento, también puede crear un equipo virtual que tenga adjudicados menos núcleos y comprar una licencia para ese menor número de núcleos. No obstante, dicha

implementación será menos rápida que si utilizara todos los núcleos disponibles en el servidor.

Nota: cada licencia de los productos servidor de Altova se puede usar de forma simultánea en un equipo como máximo (en el equipo donde está instalado el producto servidor de Altova), incluso si la capacidad de la licencia no está agotada. Por ejemplo, si utiliza una licencia para 10 núcleos para un equipo cliente que tiene 6 núcleos, los 4 núcleos restantes de la licencia no se pueden usar simultáneamente en otro equipo cliente.

Nota: debido a sus funciones de servicios, MobileTogether Server Advanced Edition solo puede ejecutarse en equipos con **dos o más núcleos**.

Licencias de MobileTogether Server
Las licencias de MobileTogether Server funciona en base al número de núcleos CPU que tenga el equipo donde se ejecuta MobileTogether Server. Las licencias basadas en el número de núcleos permiten conectar un número ilimitado de dispositivos al servidor. Sin embargo, si marca la casilla *Limit to single thread execution*, entonces solo se podrá conectar a MobileTogether Server un máximo de un dispositivo. Esto puede ser útil en tareas de evaluación y de pruebas a pequeña escala. No obstante, si estando marcada esta casilla, se conecta otro dispositivo a MobileTogether Server, este otro dispositivo se hará con la licencia. El primer dispositivo ya no se podrá conectar y recibirá un mensaje de error a tal efecto.

3.3.3 Notas sobre configuración del entorno

Carpetas

A continuación enumeramos carpetas importantes de su sistema MobileTogether Server.

- *Directorio raíz de instalación*

  /usr/local/Altova/MobileTogetherServer4.1/

- *Archivos de bases de datos, licencias y soluciones*

  /var/Altova/MobileTogetherServer

- *Parámetros del entorno*

  /Library/LaunchDaemons/com.altova.MobileTogetherServer.plist
  El archivo de parámetros del entorno debe definirse en función del entorno de cada usuario. La ruta de acceso anterior es un ejemplo solamente.
  Nota: estas variables del entorno solamente se establecen para el proceso de MobileTogether Server y por tanto no afectan a los demás usuarios.

Bases de datos basadas en archivos

Las bases de datos basadas en archivos (como las bases de datos SQLite) deben residir en la carpeta que se definió en la pestaña ***Opciones*** de MobileTogether Server como directorio de trabajo del lado servidor. La carpeta predeterminada para este tipo de bases de datos es:

/var/opt/Altova/MobileTogetherServer/SolutionFiles

Conexiones JDBC

Cuando trabaje con este tipo de conexiones debe tener en cuenta estos aspectos:

- Debe tener instalado Java Runtime Environment o el kit de desarrollo de software.
- Debe tener instalados controladores JDBC para la base de datos de destino.
- Debe establecer correctamente estas variables de entorno:
  - **CLASSPATH**: para encontrar los archivos jar.
  - **PATH**: para buscar el entorno JRE, aunque a veces no es necesaria, dependiendo de la instalación.
  - **JAVA_HOME**: a veces no es necesaria, dependiendo de la instalación.

> **Nota**
> En servidores macOS solamente son compatibles las conexiones de base de datos de tipo JDBC.

Lista de archivos importantes

El archivo `Plist` se instala en la carpeta `/Library/LaunchDaemons`. Las partes resaltadas en azul son propias del entorno y deberán ajustarse:

Archivo Plist

```
<?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/MobileTogetherServer4.1/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/iseries/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 Configurar cifrado SSL

Si desea cifrar la comunicación entre MobileTogether Server y las aplicaciones MobileTogether Client con el protocolo SSL, será necesario:

- Generar una clave privada SSL y crear un archivo de certificado de clave pública SSL
- Configurar MobileTogether Server para la comunicación con cifrado SSL.

Más abajo encontrará instrucciones para hacerlo.

MobileTogether utiliza el kit de herramientas OpenSSL de código abierto para gestionar el cifrado SSL. Por tanto, los pasos que se describen en las instrucciones solo funcionarán en equipos con OpenSSL. El kit de herramientas OpenSSL suele estar instalado por defecto en la mayoría de las distribuciones de Linux y en equipos macOS, pero también se puede instalar en equipos Windows. En la wiki de OpenSSL encontrará enlaces para descargar a los binarios de instalación.

---

1. Generar una clave privada

   SSL requiere tener instalada una **clave privada** en MobileTogether Server. Esta clave privada se utilizará para cifrar todos los datos que se envíen a las aplicaciones MobileTogether Client. Para crear la clave privada utilice este comando de OpenSSL:

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

   Esto crea un archivo llamado **private.key**, que contiene la clave privada. Recuerde dónde guarda el archivo porque lo necesitará para (i) generar la solicitud de firma de certificado (CSR) y (ii) instalarlo en MobileTogether Server (*consultar paso nº 8*).

2. Solicitudes de firma de certificado (CSR)

   La solicitud de firma de certificado (CSR) se envía a una entidad de certificación (como VeriSign o Thawte) para solicitar un certificado de clave pública. La CSR se basa en la clave privada y contiene información sobre su compañía. Cree una CSR con este comando de OpenSSL:

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

   Este comando aporta el archivo de clave privada `private.key` creado en el paso nº1.

   Durante la generación de la CSR deberá indicar datos sobre su compañía. La entidad de certificación utilizará estos datos para verificar su identidad:

   - *País*
   - *Localidad (ciudad donde está situada su compañía)*
   - *Organización (nombre de su compañía).* No utilice caracteres especiales porque el certificado no será válido.
   - *Nombre común (nombre DNS de su servidor).* Debe ser idéntico al nombre

oficial de su servidor (es decir, debe ser el nombre DNS que utilizarán las aplicaciones cliente para conectarse al servidor).
- *Contraseña de comprobación.* Deje este campo vacío.

3. Comprar un certificado SSL

   Compre un certificado SSL de una entidad de certificación reconocida, como VeriSign o Thawte. En adelante utilizamos el procedimiento de VeriSign, pero es similar al de otras entidades de certificación:

   - Visite el sitio web de VeriSign.
   - Haga clic en **Buy SSL Certificates**.
   - Hay varios tipos de certificados SSL a la venta. Para MobileTogether Server es suficiente un certificado Secure Site o Secure Site Pro. Como no existe una barra de dirección verde no será necesaria una comprobación extendida (EV).
   - Siga los pasos y rellene el formulario de compra con sus datos.
   - Cuando se le solicite la CSR (creada en el paso nº2), copie y pegue el contenido del archivo **`my.csr`** en el formulario.
   - Efectúe el pago con una tarjeta de crédito válida.

   Tiempo de espera para obtener el certificado
   El certificado de una entidad de certificación SSL suele tardar **dos o tres días laborales**. Tenga esto en cuenta a la hora de configurar MobileTogether Server.

4. Recibir la clave pública de la entidad de certificación

   La autoridad de certificación elegida terminará el proceso de registro en dos o tres días laborales. Entre tanto es posible que reciba algún correo electrónico o llamada telefónica para comprobar si tiene autorización para solicitar un certificado SSL para su dominio DNS.

   Una vez completado el proceso de registro y autorización, recibirá un correo electrónico con la clave pública de su certificado SSL. Esta clave pública estará en texto sin formato o será un archivo **`.cer`**.

5. Guardar la clave pública en un archivo

   Para poder usarla con MobileTogether Server la clave pública debe estar guardada en un archivo **`.cer`**. Si recibió la clave pública como texto sin formato, copie y pegue todas las líneas de la clave, desde `--BEGIN CERTIFICATE--` hasta `--END CERTIFICATE--` en un archivo de texto que llamaremos **`miCertificado.cer`**.

6. Guardar los certificados intermedios de la autoridad de certificación en un archivo

   Para completar el certificado SSL necesitará otros dos certificados: el certificado intermedio principal y el certificado intermedio secundario. En el sitio web de su autoridad de certificación encontrará el contenido de los certificados intermedios:

- Certificados intermedios de Verisign: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657&actp=LIST&viewlocale=en_US
- Certificados intermedios de Verisign para su producto Secure Site: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR1735

Copie y pegue los dos certificados intermedios en sendos archivos de texto y guárdelos en el equipo.

7. Combinar los certificados en un solo archivo de certificado de clave pública

   Ahora cuenta con tres archivos de certificado:

   - La clave pública (`miCertificado.cer`)
   - El certificado intermedio secundario
   - El certificado intermedio principal

   Todos contienen bloques de texto entre líneas similares a estas:

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

   Ahora copie y pegue los tres certificados en un solo archivo, uno detrás del otro. El orden de aparición es importante: (i) primero la clave pública, (ii) después el certificado intermedio secundario y (iii) por último el certificado intermedio principal. Compruebe que no hay líneas vacías entre un certificado y el siguiente.

   ```
   --BEGIN CERTIFICATE--
     clave pública de miCertificado.cer (paso nº5)
   --END CERTIFICATE--
   --BEGIN CERTIFICATE--
     certificado intermedio secundario (paso nº6)
   --END CERTIFICATE--
   --BEGIN CERTIFICATE--
     certificado intermedio principal (paso nº6)
   --END CERTIFICATE--
   ```

   Guarde el texto resultante en un archivo llamado **`publickey.cer`**, que es ya el certificado de clave pública de su certificado SSL. Incluye el certificado de clave pública y la cadena de confianza (es decir, los certificados intermedios utilizados por la entidad de certificación para firmar el certificado). El archivo de certificado de clave pública se instalará en el servidor MobileTogether Server junto con la clave privada (*paso nº8*).

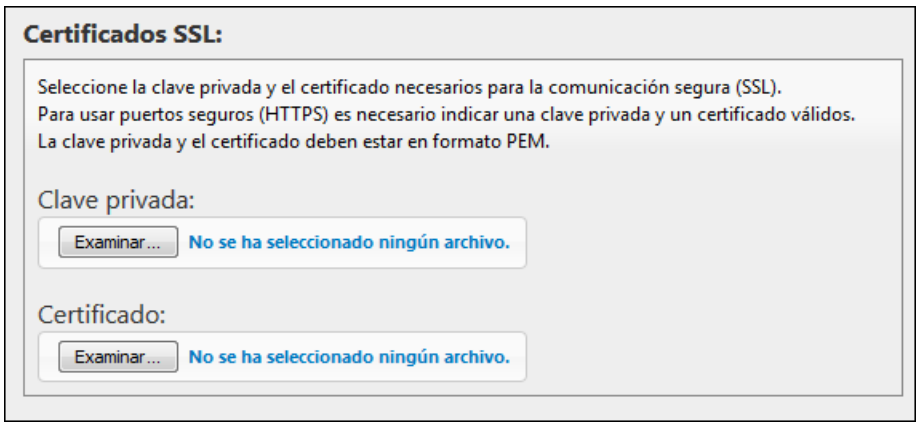
8. Instalar el certificado SSL en MobileTogether Server

   El certificado SSL es un conjunto de certificados compuesto por estos archivos:

   - `private.key`: que contiene el certificado de clave privada
   - `publickey.cer`: que contiene el certificado de clave pública y los certificados intermedios de la entidad de certificación (el principal y el secundario)

Siga estas instrucciones para instalar estos certificados SSL en MobileTogether Server:

- Inicie sesión en la interfaz web de MobileTogether Server (puerto `8085` del servidor).
- Abra la pestaña **Opciones**.
- En la sección *Certificados SSL* (*imagen siguiente*), cargue los dos archivos de certificados.



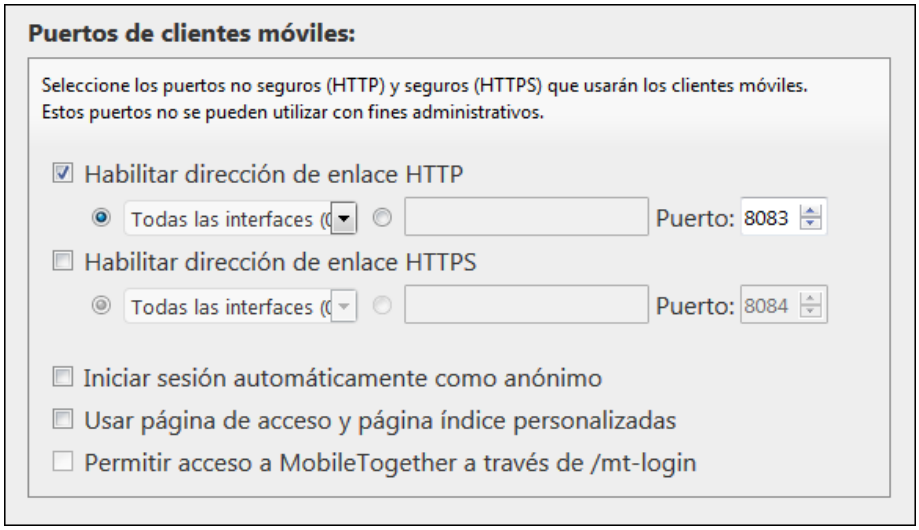
  - Seleccione **`private.key`** para la clave privada
  - Seleccione **`publickey.cer`** para el certificado

- Haga clic en el botón **Guardar** situado al final de la sección *Configuración general*.

9. Configurar el puerto HTTPS del servidor

   Tras instalar el certificado SSL podrá especificar un puerto del servidor para la comunicación SSL con los clientes.

   - Inicie sesión en la interfaz web de MobileTogether Server (puerto `8085` del servidor).
   - Abra la pestaña **Opciones**.
   - En la sección *Puertos de clientes móviles* (*imagen siguiente*) habilite e indique cuál es el puerto HTTPS.



Asegúrese de que el servidor de seguridad, si se utiliza, esté configurado para permitir el acceso a MobileTogether Server por el puerto HTTPS.

10. Probar la comunicación SSL

    Ahora puede usar cualquier herramienta de pruebas para comprobar si la comunicación segura con el servidor por HTTPS funciona correctamente. Por ejemplo, puede usar el sitio de pruebas https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp

    Esta herramienta comprueba y confirma si (i) el certificado de calve pública se construyó correctamente con la cadena de confianza y si (ii) se puede establecer la conexión con el servidor a través del servidor de seguridad.

11. Habilitar las aplicaciones MobileTogether Client para usar SSL

    En las aplicaciones MobileTogether Client que se comuniquen con servidores MobileTogether Server que tengan habilitado el cifrado SSL, debe marcar la casilla Cifrado SSL. Para más información consulte la documentación de MobileTogether Client.

Altova MobileTogether Server

Procedimientos del servidor

4 Procedimientos del servidor

Esta sección se ocupa de procedimientos clave del servidor, dando por hecho que MobileTogether Server ya tenga asociada una licencia. Sin embargo, recuerde que para poder acceder a MobileTogether Server, es necesario iniciar y ejecutar LicenseServer y MobileTogether Server como servicios.

- Iniciar Altova LicenseServer
- Iniciar MobileTogether Server
- Configurar cifrados SSL
- Configurar puertos del administrador y de clientes móviles
- Usuarios y roles
- Privilegios disponibles
- Configurar el servidor de seguridad
- Estadísticas de uso de soluciones
- Información para clientes
- Copias de seguridad y restaurar datos de MobileTogether Server

4.1 Iniciar Altova LicenseServer

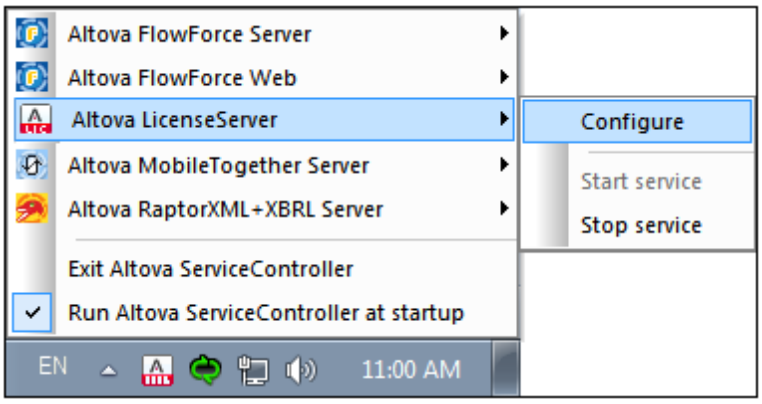
Los productos servidor de Altova(i) FlowForce Server; (ii) RaptorXML(+XBRL) Server; (iii) MobileTogether Server; (iv) MapForce Server; (v) StyleVision Server deben tener asignada una licencia con un servidor Altova LicenseServer de la red para poder ejecutarse. LicenseServer debe ejecutarse continuamente como servicio para que las instalaciones conectadas de MobileTogether Server se puedan ejecutar. Si se detiene LicenseServer también se detendrán todas las instalaciones de MobileTogether Server conectadas. Si esto ocurre, deberá volver a iniciar.

Siga estas instrucciones para iniciar o detener LicenseServer en el sistema operativo correspondiente.

Windows

Inicie LicenseServer a través del controlador de servicios Altova ServiceController, que está disponible en la bandeja del sistema.

Primero haga clic en **Inicio | Todos los programas | Altova LicenseServer | Altova ServiceController** para iniciar el controlador de servicios. El icono de Altova ServiceController aparecerá a continuación en la bandeja del sistema (*imagen siguiente*). Si selecciona el comando **Run Altova ServiceController at Startup**, Altova ServiceController se iniciará cuando se inicie el sistema y su icono estará en la bandeja del sistema de ahora en adelante.



Para iniciar LicenseServer, haga clic en el icono de Altova ServiceController en la bandeja del sistema y después seleccione **Altova LicenseServer** en el menú que aparece (*imagen anterior*). Después seleccione **Start Service** para iniciar LicenseServer como servicio. Si LicenseServer ya está en ejecución, el comando **Start Service** no estará habilitado.

Para detener LicenseServer, seleccione el comando **Stop Service** del submenú (*imagen anterior*).

Linux

Ejecute este comando en una ventana de terminal para iniciar LicenseServer como servicio en sistemas Linux:

```
[Debian]:          sudo /etc/init.d/licenseserver start
[Ubuntu]:          sudo initctl start licenseserver
[CentOS 6]:        sudo initctl start licenseserver
[CentOS 7]:        sudo systemctl start licenseserver
[RedHat]:          sudo initctl start licenseserver
```

Para detener LicenseServer, reemplace **start** por **stop** en el comando.

macOS

Ejecute este comando en una ventana de terminal para iniciar LicenseServer en sistemas macOS:

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

Para detener LicenseServer, utilice este comando:

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

4.2 Iniciar MobileTogether Server

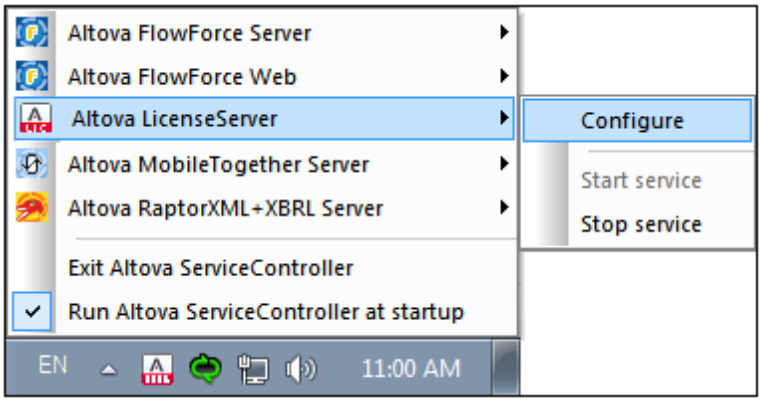
MobileTogether Server debe iniciarse como servicio para poder ejecutarse.

A continuación encontrará instrucciones para iniciar la aplicación como servicio en el sistema operativo correspondiente.

Windows

MobileTogether Server se puede iniciar desde el controlador de servicios Altova ServiceController, que está disponible en la bandeja del sistema.

Primero haga clic en **Inicio | Todos los programas | Altova LicenseServer | Altova ServiceController** para iniciar el controlador de servicios. El icono de Altova ServiceController aparecerá a continuación en la bandeja del sistema (*imagen siguiente*). Si selecciona el comando **Run Altova ServiceController at Startup**, Altova ServiceController se iniciará cuando se inicie el sistema y su icono estará en la bandeja del sistema de ahora en adelante.



Para iniciar MobileTogether Server, haga clic en el icono de Altova ServiceController en la bandeja del sistema y después seleccione **MobileTogether Server** en el menú que aparece (*imagen anterior*). Después seleccione **Start Service** para iniciar MobileTogether Server como servicio. Si MobileTogether Server ya está en ejecución, el comando **Start Service** no estará habilitado.

Para detener MobileTogether Server, seleccione el comando **Stop Service** del submenú (*imagen anterior*).

Linux

Ejecute este comando en una ventana de terminal para iniciar MobileTogether Server como servicio en sistemas Linux:

```
[Debian]:          sudo /etc/init.d/mobiletogetherserver start
[Ubuntu]:          sudo initctl start mobiletogetherserver
[CentOS 6]:        sudo initctl start mobiletogetherserver
[CentOS 7]:        sudo systemctl start mobiletogetherserver
```

```
[RedHat]:          sudo initctl start mobiletogetherserver
```

Para detener MobileTogether Server, reemplace **start** por **stop** en el comando.

macOS

Ejecute este comando en una ventana de terminal para iniciar MobileTogether Server en sistemas macOS:

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

Para detener MobileTogether Server, utilice este comando:

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

4.3 Configurar cifrado SSL

Si desea cifrar la comunicación entre MobileTogether Server y las aplicaciones MobileTogether Client con el protocolo SSL, será necesario:

- Generar una clave privada SSL y crear un archivo de certificado de clave pública SSL
- Configurar MobileTogether Server para la comunicación con cifrado SSL.

Más abajo encontrará instrucciones para hacerlo.

MobileTogether utiliza el kit de herramientas OpenSSL de código abierto para gestionar el cifrado SSL. Por tanto, los pasos que se describen en las instrucciones solo funcionarán en equipos con OpenSSL. El kit de herramientas OpenSSL suele estar instalado por defecto en la mayoría de las distribuciones de Linux y en equipos macOS, pero también se puede instalar en equipos Windows. En la wiki de OpenSSL encontrará enlaces para descargar a los binarios de instalación.

---

1. Generar una clave privada

   SSL requiere tener instalada una **clave privada** en MobileTogether Server. Esta clave privada se utilizará para cifrar todos los datos que se envíen a las aplicaciones MobileTogether Client. Para crear la clave privada utilice este comando de OpenSSL:

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

   Esto crea un archivo llamado **private.key**, que contiene la clave privada. Recuerde dónde guarda el archivo porque lo necesitará para (i) generar la solicitud de firma de certificado (CSR) y (ii) instalarlo en MobileTogether Server (*consultar paso nº 8*).

2. Solicitudes de firma de certificado (CSR)

   La solicitud de firma de certificado (CSR) se envía a una entidad de certificación (como VeriSign o Thawte) para solicitar un certificado de clave pública. La CSR se basa en la clave privada y contiene información sobre su compañía. Cree una CSR con este comando de OpenSSL:

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

   Este comando aporta el archivo de clave privada `private.key` creado en el paso nº1.

   Durante la generación de la CSR deberá indicar datos sobre su compañía. La entidad de certificación utilizará estos datos para verificar su identidad:

   - *País*
   - *Localidad (ciudad donde está situada su compañía)*
   - *Organización (nombre de su compañía).* No utilice caracteres especiales porque el certificado no será válido.
   - *Nombre común (nombre DNS de su servidor).* Debe ser idéntico al nombre

oficial de su servidor (es decir, debe ser el nombre DNS que utilizarán las aplicaciones cliente para conectarse al servidor).
- *Contraseña de comprobación.* Deje este campo vacío.

3. Comprar un certificado SSL

   Compre un certificado SSL de una entidad de certificación reconocida, como VeriSign o Thawte. En adelante utilizamos el procedimiento de VeriSign, pero es similar al de otras entidades de certificación:

   - Visite el sitio web de VeriSign.
   - Haga clic en **Buy SSL Certificates**.
   - Hay varios tipos de certificados SSL a la venta. Para MobileTogether Server es suficiente un certificado Secure Site o Secure Site Pro. Como no existe una barra de dirección verde no será necesaria una comprobación extendida (EV).
   - Siga los pasos y rellene el formulario de compra con sus datos.
   - Cuando se le solicite la CSR (creada en el paso nº2), copie y pegue el contenido del archivo **`my.csr`** en el formulario.
   - Efectúe el pago con una tarjeta de crédito válida.

   Tiempo de espera para obtener el certificado
   El certificado de una entidad de certificación SSL suele tardar **dos o tres días laborales**. Tenga esto en cuenta a la hora de configurar MobileTogether Server.

4. Recibir la clave pública de la entidad de certificación

   La autoridad de certificación elegida terminará el proceso de registro en dos o tres días laborales. Entre tanto es posible que reciba algún correo electrónico o llamada telefónica para comprobar si tiene autorización para solicitar un certificado SSL para su dominio DNS.

   Una vez completado el proceso de registro y autorización, recibirá un correo electrónico con la clave pública de su certificado SSL. Esta clave pública estará en texto sin formato o será un archivo **`.cer`**.

5. Guardar la clave pública en un archivo

   Para poder usarla con MobileTogether Server la clave pública debe estar guardada en un archivo **`.cer`**. Si recibió la clave pública como texto sin formato, copie y pegue todas las líneas de la clave, desde `--BEGIN CERTIFICATE--` hasta `--END CERTIFICATE--` en un archivo de texto que llamaremos **`miCertificado.cer`**.

6. Guardar los certificados intermedios de la autoridad de certificación en un archivo

   Para completar el certificado SSL necesitará otros dos certificados: el certificado intermedio principal y el certificado intermedio secundario. En el sitio web de su autoridad de certificación encontrará el contenido de los certificados intermedios:

- Certificados intermedios de Verisign: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657&actp=LIST&viewlocale=en_US
- Certificados intermedios de Verisign para su producto Secure Site: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR1735

Copie y pegue los dos certificados intermedios en sendos archivos de texto y guárdelos en el equipo.

7. Combinar los certificados en un solo archivo de certificado de clave pública

   Ahora cuenta con tres archivos de certificado:

   - La clave pública (`miCertificado.cer`)
   - El certificado intermedio secundario
   - El certificado intermedio principal

   Todos contienen bloques de texto entre líneas similares a estas:

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

   Ahora copie y pegue los tres certificados en un solo archivo, uno detrás del otro. El orden de aparición es importante: (i) primero la clave pública, (ii) después el certificado intermedio secundario y (iii) por último el certificado intermedio principal. Compruebe que no hay líneas vacías entre un certificado y el siguiente.

   ```
   --BEGIN CERTIFICATE--
     clave pública de miCertificado.cer (paso nº5)
   --END CERTIFICATE--
   --BEGIN CERTIFICATE--
     certificado intermedio secundario (paso nº6)
   --END CERTIFICATE--
   --BEGIN CERTIFICATE--
     certificado intermedio principal (paso nº6)
   --END CERTIFICATE--
   ```

   Guarde el texto resultante en un archivo llamado **`publickey.cer`**, que es ya el certificado de clave pública de su certificado SSL. Incluye el certificado de clave pública y la cadena de confianza (es decir, los certificados intermedios utilizados por la entidad de certificación para firmar el certificado). El archivo de certificado de clave pública se instalará en el servidor MobileTogether Server junto con la clave privada (*paso nº8*).

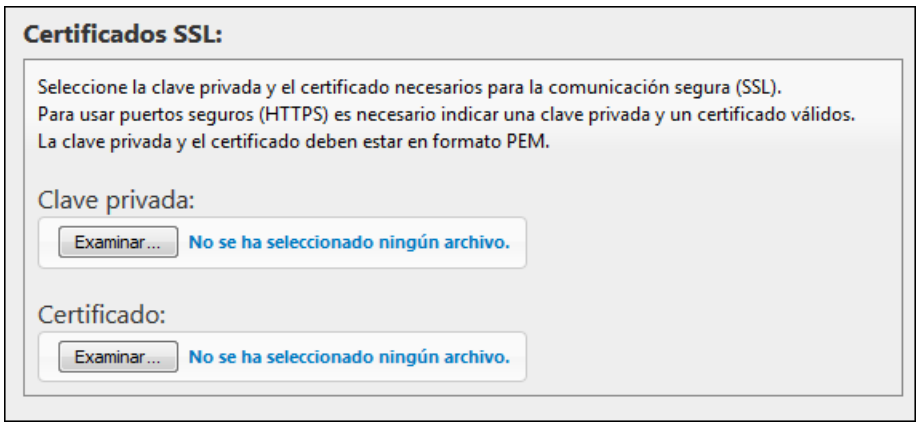
8. Instalar el certificado SSL en MobileTogether Server

   El certificado SSL es un conjunto de certificados compuesto por estos archivos:

   - `private.key`: que contiene el certificado de clave privada
   - `publickey.cer`: que contiene el certificado de clave pública y los certificados intermedios de la entidad de certificación (el principal y el secundario)

Siga estas instrucciones para instalar estos certificados SSL en MobileTogether Server:

- Inicie sesión en la interfaz web de MobileTogether Server (puerto `8085` del servidor).
- Abra la pestaña **Opciones**.
- En la sección *Certificados SSL* (*imagen siguiente*), cargue los dos archivos de certificados.



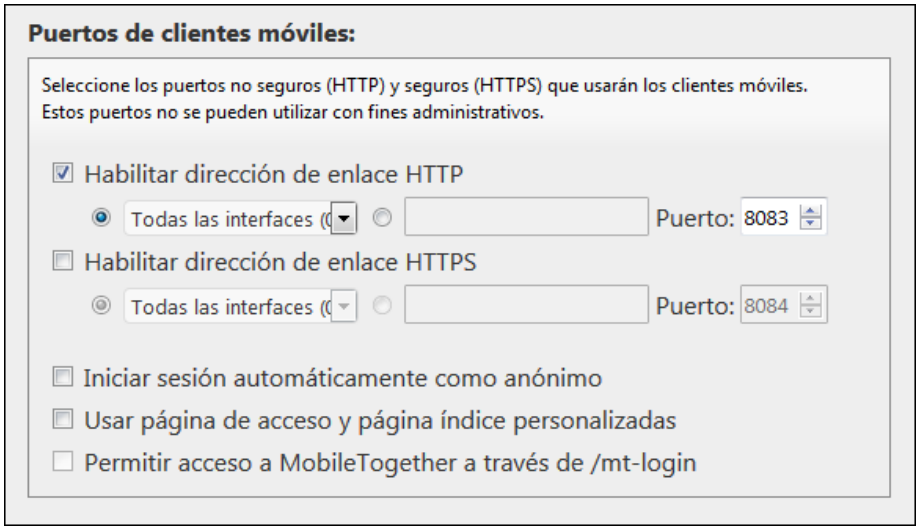
  - Seleccione **`private.key`** para la clave privada
  - Seleccione **`publickey.cer`** para el certificado

- Haga clic en el botón **Guardar** situado al final de la sección *Configuración general*.

9. Configurar el puerto HTTPS del servidor

   Tras instalar el certificado SSL podrá especificar un puerto del servidor para la comunicación SSL con los clientes.

   - Inicie sesión en la interfaz web de MobileTogether Server (puerto `8085` del servidor).
   - Abra la pestaña **Opciones**.
   - En la sección *Puertos de clientes móviles* (*imagen siguiente*) habilite e indique cuál es el puerto HTTPS.



Asegúrese de que el servidor de seguridad, si se utiliza, esté configurado para permitir el acceso a MobileTogether Server por el puerto HTTPS.

10. Probar la comunicación SSL

    Ahora puede usar cualquier herramienta de pruebas para comprobar si la comunicación segura con el servidor por HTTPS funciona correctamente. Por ejemplo, puede usar el sitio de pruebas https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp

    Esta herramienta comprueba y confirma si (i) el certificado de calve pública se construyó correctamente con la cadena de confianza y si (ii) se puede establecer la conexión con el servidor a través del servidor de seguridad.

11. Habilitar las aplicaciones MobileTogether Client para usar SSL

    En las aplicaciones MobileTogether Client que se comuniquen con servidores MobileTogether Server que tengan habilitado el cifrado SSL, debe marcar la casilla Cifrado SSL. Para más información consulte la documentación de MobileTogether Client.

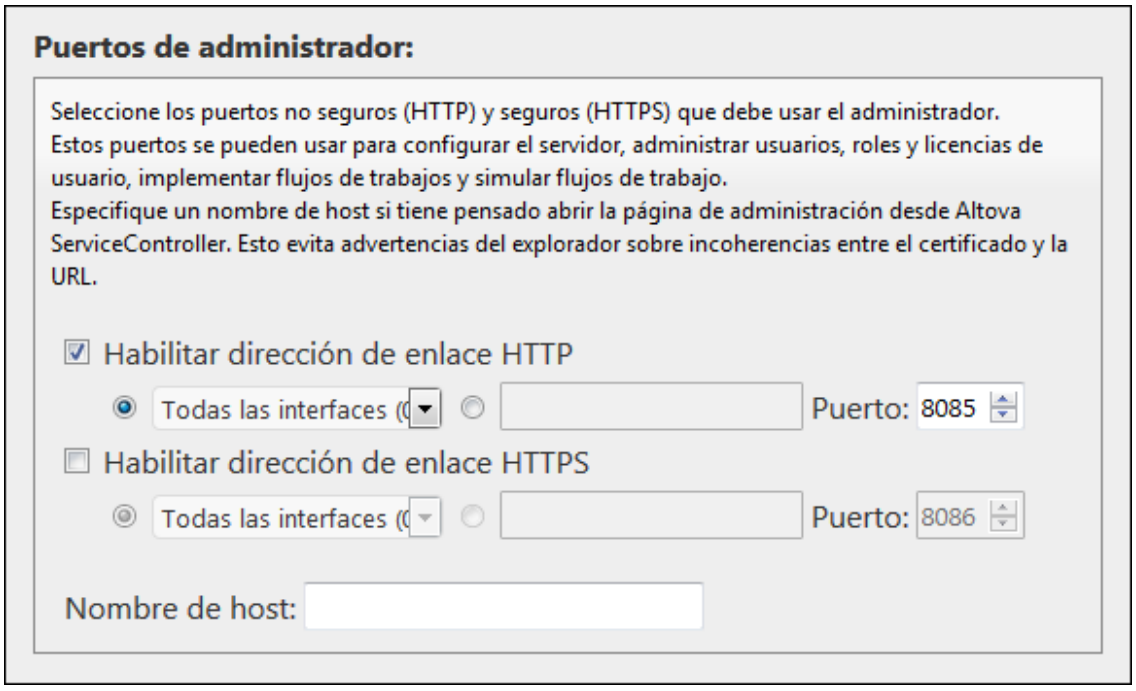
4.4 Configurar puertos del administrador y de clientes móviles

Los puertos del administrador se usan para conectarse a la interfaz web de MobileTogether Server, mientras que los puertos del cliente móvil son los que utiliza el dispositivo cliente móvil para conectarse a los servicios de MobileTogether Server.

Configurar puertos de administrador

Los puertos de administrador permiten acceder al servidor para:

- conectarse a la interfaz web del servidor y llevar a cabo tareas administrativas, como configurar Usuarios y roles, por ejemplo.
- implementar en el servidor diseños de MobileTogether (como soluciones de MobileTogether). MobileTogether Designer tiene una opción de configuración para especificar la dirección y el puerto del servidor MobileTogether Server donde se deben implementar los diseños.



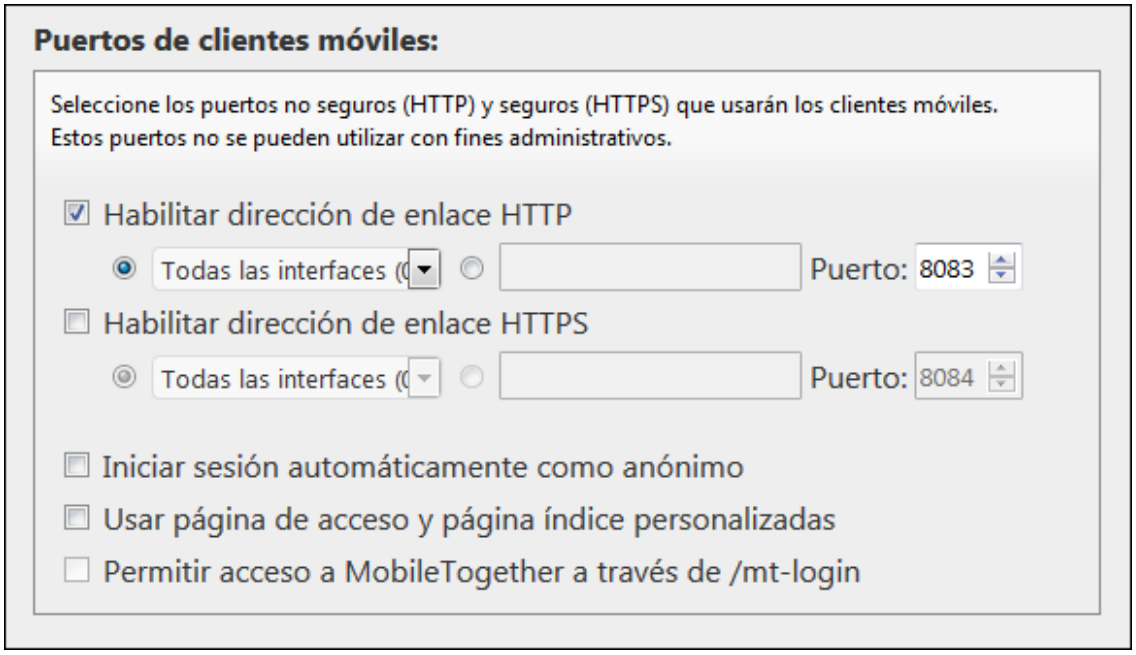
El puerto HTTP es el puerto no seguro, mientras que el puerto HTTPS es el puerto seguro. Para usar HTTPS deberá configurar antes el cifrado SSL. Si configura el puerto HTTPS y desea evitar advertencias del explorador web sobre conflictos entre el certificado SSL y la URL, entonces especifique el nombre de host del equipo donde se abrirá la página de configuración de MobileTogether Server.

Puede especificar si el servidor usará una dirección IP concreta o todas las interfaces y

direcciones IP. Si se debe usar una sola dirección IP, introdúzcala en el campo del segundo botón de opción.

Configurar puertos del cliente móvil

Estos son los puertos que utilizarán los dispositivos móviles para conectarse al servidor. El puerto HTTP es el puerto no seguro, mientras que el puerto HTTPS es el puerto seguro. Para usar HTTPS deberá configurar antes el cifrado SSL. Puede especificar si el servidor usará una dirección IP concreta o todas las interfaces y direcciones IP. Si se debe usar una sola dirección IP, introdúzcala en el campo del segundo botón de opción.



Iniciar sesión automáticamente como anónimo

Si marca esta opción, los clientes iniciarán sesión automáticamente con la cuenta anonymous. La página de acceso se omite y aparece directamente la primera página del servidor. La primera página es la página estándar donde se puede ver la carpeta raíz o una página personalizada y definida previamente (*ver siguiente punto*). Si **no marca** esta opción, el cliente deberá iniciar sesión utilizando las credenciales adecuadas desde la página de acceso predeterminada. Si marca esta opción, recuerde que debe asignar los privilegios correspondientes para anonymous.

Usar página de acceso y página índice personalizadas

Marque esta opción si desea utilizar una página de acceso y una página índice personalizadas. Es decir, con esta opción puede diseñar un punto de entrada particular para los clientes. Estos son los pasos que debe seguir para conseguirlo:

1. Cree las dos páginas como páginas HTML y llámelas **`login.html`** y **`index.html`** respectivamente.
2. Guarde estos dos archivos en la carpeta **`index`** situada en la carpeta de datos de la

aplicación MobileTogether Server (*ver tabla más abajo*). Si tiene otros archivos, como archivos de imágenes y archivos CSS, guárdelos en una subcarpeta de la carpeta **index** (por ejemplo, en una carpeta llamada **static**).

Linux	`/var/opt/Altova/MobileTogetherServer`
Mac	`/var/Altova/MobileTogetherServer`
Windows 7, 8, 10	`C:\ProgramData\Altova\MobileTogetherServer`

A continuación puede ver fragmentos de código de una página de acceso y de una página de índice. Son páginas muy básicas pero si lo desea puede modificar el código a su gusto.

login.html

```
<html>
  <header>
    <title>Acceso personalizado</title>
  </header>
  <head>
    <meta http-equiv="Cache-Control" content="no-store" />
  </head>
  <body>
    <div>
      <h1>Iniciar sesión</h1>
      <p>Página básica y personalizada para acceso de clientes a
MobileTogether Server. Modifique esta página a su gusto y utilice la
subcarpeta Static para guardar hojas de estilos CSS, imágenes, etc.</p>
      <form method="post" action="/do_login" name="loginform">
        <table>
          <tbody>
            <!-- Usuario que debe iniciar sesión -->
            <tr><td>Usuario:</td></tr>
            <tr><td><input type="text" name="username" size="30"></td></
tr>
            <!-- Contraseña del usuario -->
            <tr><td>Contraseña:</td></tr>
            <tr><td><input type="password" name="password" size="30"></
td></tr>
            <!-- Datos de dominio Active Directory -->
            <tr><td> </td></tr>
            <tr><td>Inicio de sesión de Active Directory:</td></tr>
            <tr>Sufijo del dominio: <td><input type="providernamesuffix"
name="providernamesuffix" value=""></td></tr>
            <tr>Prefijo del dominio: <td><input
type="providernameprefix" name="providernameprefix" value=""></td></tr>

            <!-- Botón Iniciar sesión -->
            <tr><td><input type="submit" value="Iniciar sesión"></td></
tr>
          </tbody>
        </table>
        <!-- Página a la que se conduce después de iniciar sesión. -->
        <input type="hidden" name="from_page" value="/index"></
```

```
input><br>
      </form>
    </div>
  </body>
</html>
```

index.html

```
<html>
  <header>
    <title>Página índice personalizada</title>
  </header>
  <head>
    <meta http-equiv="Cache-Control" content="no-store" />
    <title>Página índice personalizada</title>
  </head>
  <body>
    <img src="/index/static/logo.png"></img><hr/>
    <a href="/do_logout">Cerrar sesión</a>
    <p>MobileTogether: Acceso personalizado</p>
    <div><a href='/run?d=/public/About'>Iniciar la aplicación About</
a></div>
    <div><a href='/run?d=/public/DateCalc'>Iniciar la aplicación Date
Calculator</a></div>
    <div><a href='/run?d=/public/WorldPopulation'>Iniciar la aplicación
World Population Statics</a></div>
  </body>
</html>
```

Permitir acceso a MobileTogether mediante /mt-login

Marque esta opción si quiere que el inicio de sesión se lleve a cabo por la página de acceso y la página índice predeterminadas y no por las páginas personalizadas. Esta opción permite almacenar los archivos **login.html** y **index.html** en la ubicación designada pero utilizar las páginas predeterminadas. Puede que el explorador del cliente necesite que se vacíe el caché del explorador o de lo contrario esta opción no surtirá efecto.

4.5 Usuarios y roles

Una cuenta de usuario viene definida por un nombre y una contraseña de inicio de sesión y tiene asociado un conjunto de derechos de acceso. Los usuarios de MobileTogether Server acceden al servidor para realizar tareas administrativas o como usuarios finales desde dispositivos cliente.

Los derechos de acceso del usuario vienen dados por los privilegios que este tiene concedidos. Los usuarios reciben privilegios de dos maneras: (i) heredándolos de roles de los que el usuario es miembro o (ii) directamente mediante asignaciones directas.

Un rol viene definido por un conjunto de privilegios. Los roles reciben privilegios mediante asignaciones directas o heredándolos de otro rol del cual es miembro. Los privilegios no son más que derechos de acceso a las diferentes funciones administrativas y a los servicios de MobileTogether Server (p. ej. el derecho a gestionar las opciones de configuración del servidor, a establecer la contraseña propia o a ejecutar simulaciones en el servidor).

Mediante el uso de roles podemos definir privilegios de forma jerárquica para los usuarios. Por ejemplo, el rol `AdminSimple` puede permitir el privilegio *Gestionar opciones de configuración del servidor*. Si `AdminSimple` es miembro de `AdminAvanzado`, heredará el privilegio de gestionar las opciones de configuración del servidor y podrá tener además el privilegio *Mantenimiento de usuarios, roles y privilegios.* Para ver una lista de privilegios consulte este apartado.

▼ ¿Qué es un usuario?

Un usuario se define por medio de una combinación de nombre de usuario y contraseña. Los usuarios pueden acceder a MobileTogether Server de dos maneras diferentes:

- *por la interfaz web:* la interfaz web es la interfaz de administración de MobileTogether Server. Para acceder a ella es necesario indicar un nombre de usuario y una contraseña. Es decir, se accede al servidor como usuario.
- *por la interfaz del servicio*: la interfaz del servicio HTTP expone los servicios de MobileTogether Server a la aplicación MobileTogether Client en un dispositivo móvil. El usuario accede a la interfaz del servicio indicando un nombre de usuario y una contraseña. Los servicios expuestos suelen estar relacionados con el acceso a soluciones de MobileTogether y a sus datos.

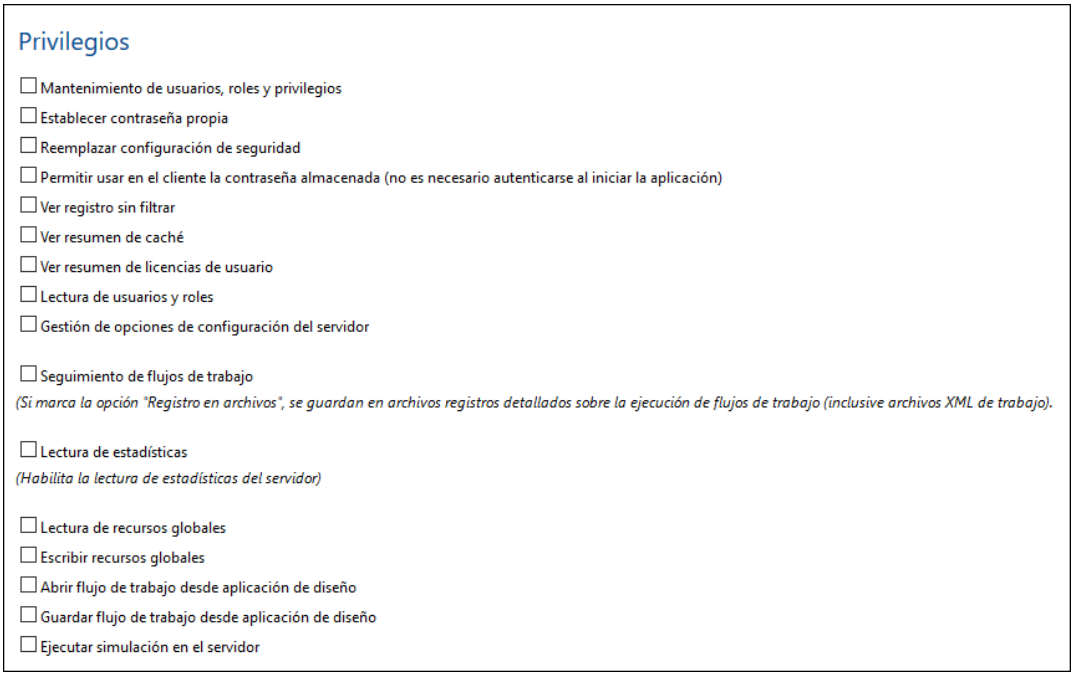
Hay dos usuarios predeterminados:

`root`	**`root`** es el usuario administrador inicial. Se trata del usuario con más poder en un principio, ya que dispone de todos los privilegios y tiene capacidad para agregar otros usuarios y configurar roles. Su combinación inicial de nombre de usuario y contraseña es: **`root-root`**. La contraseña puede cambiarse en todo momento.
`anonymous`	**`anonymous`** es una cuenta para usuarios anónimos que accedan a servicios expuestos a través de la interfaz del servicio HTTP. No se puede utilizar para acceder a la interfaz web y no dispone de contraseña inicial.

▼ ¿Qué es un privilegio?

Un privilegio es una actividad para cuya realización se dio permiso a un usuario. En MobileTogether Server hay un número fijo de privilegios y un usuario puede no tener asignado ningún privilegio o tener asignados todos los privilegios disponibles. Sin embargo, se recomienda asignar los privilegios a través de los roles y no asignar privilegios a los usuarios directamente. El usuario que asigne privilegios y roles a otros usuarios debe tener este privilegio. En un principio es el usuario **root** quien lo tiene.

En esta imagen puede ver todos los privilegios disponibles en MobileTogether Server.



La pestaña *Usuarios y roles | Informes | Informes de privilegios* ofrece una lista completa de privilegios. En esta lista también podrá comprobar a qué usuarios se concedió cada privilegio de la lista.

▼ ¿Qué es un rol?

Un rol define un conjunto de privilegios y se puede asignar tanto a otro rol como a un usuario. Los privilegios de un rol son automáticamente los privilegios del rol o usuario al que se asignara el rol. Un usuario puede tener tantos roles como se necesiten. Es decir, un usuario tendrá todos los privilegios que se definieran en los roles que tenga asignados.

Estos son los roles predeterminados:

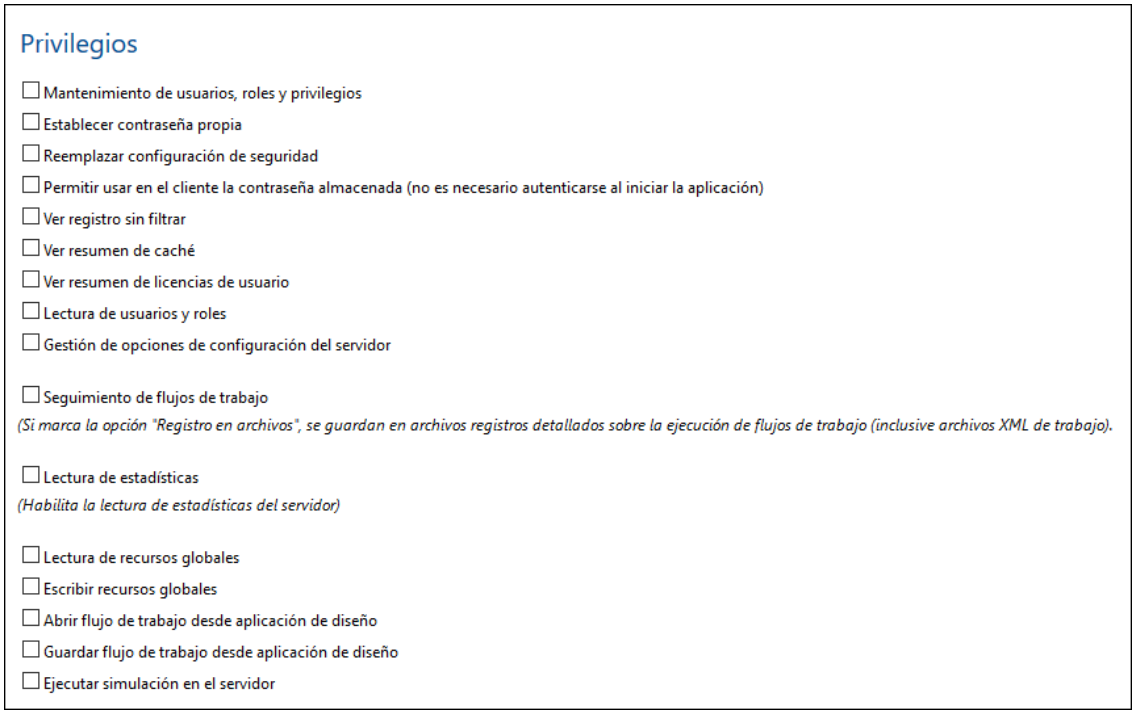
- **all** se asigna automáticamente a todos los usuarios, **incluido** el usuario **anonymous**.
- **authenticated** se asigna automáticamente a todos los usuarios, **excepto** al usuario **anonymous**. Es decir, a los usuarios con nombre y contraseña se les asigna el rol `authenticated`.
- **workflow-designer** se asigna a los usuarios que diseñan flujos de trabajo en MobileTogether Designer. Este rol permite al usuario abrir y guardar flujos de trabajo

y a ejecutar simulaciones en el servidor.

- **`workflow-user`** se asigna a los usuarios que ejecutan el flujo de trabajo en un dispositivo móvil. Este rol permite al usuario acceder a la interfaz del servicio e iniciar la solución en el cliente sin necesidad de iniciar sesión en el servidor.
- **`admin`** tiene todos los permisos y está pensado para usuarios con la función de administrador.

4.6 Privilegios disponibles

Los privilegios son derechos de acceso a las diferentes funciones administrativas y a los servicios de MobileTogether Server. Cuando un usuario inicia sesión en MobileTogether Server (a través de la interfaz web o de la interfaz del servicio), sus derechos de acceso vienen dados por sus privilegios. Los privilegios se asignan a los usuarios de forma directa o a través de roles (en la pestaña **Usuarios y roles** de la interfaz web).



A continuación describimos los privilegios disponibles en MobileTogether Server.

- *Mantenimiento de usuarios, roles y privilegios*

  El usuario que tenga este privilegio puede crear, eliminar y editar usuarios y roles, sus asignaciones de privilegios y sus contraseñas. Se trata de un privilegio administrativo y solamente se debería asignar a los administradores de MobileTogether. En la configuración predeterminada el único usuario que tiene este privilegio es el usuario `root`.

- *Establecer contraseña propia*

  El usuario que tenga este privilegio puede cambiar su propia contraseña. Los que no tengan este privilegio deberán solicitar al administrador que establezca sus contraseñas. En la configuración predeterminada el rol `authenticated` (y, por tanto, todos los usuarios excepto `anonymous`) poseen este privilegio.

- *Reemplazar configuración de seguridad*

  El usuario que tenga este privilegio puede cambiar los permisos en toda la jerarquía del contenedor sin necesidad de tener el permiso de seguridad "escritura". Esto permite a los administradores de MobileTogether recuperar el acceso a los recursos que dejaran de estar

disponible por error. Se trata de un privilegio administrativo y solamente se debería asignar a los administradores de MobileTogether. En la configuración predeterminada el único usuario que tiene este privilegio es el usuario `root`.

- *Permitir usar contraseña almacenada en cliente*

  El usuario que tenga este privilegio puede usar la contraseña almacenada en el cliente y no necesitará autenticarse.

- *Ver registro sin filtrar*

  En la configuración predeterminada los usuarios solamente pueden ver entradas del registro relacionadas con configuraciones para las que tengan permiso de "lectura". El usuario que tenga este privilegio puede leer todas las entradas del registro, incluso las que no estén asociadas a la configuración. En la configuración predeterminada el único usuario que tiene este privilegio es el usuario `root`.

- *Ver resumen de caché*

  El usuario que tenga este privilegio puede ver el resumen de caché en el servidor.

- *Ver resumen de licencias de usuario*

  El usuario que tenga este privilegio puede ver el resumen de licencias en el servidor.

- *Lectura de usuarios y roles*

  En la configuración predeterminada los usuarios solamente pueden ver su propia cuenta de usuario y los roles de los que son miembro. El usuario que tenga este privilegio puede leer todos los usuarios y roles definidos. En la configuración predeterminada el único usuario que tiene este privilegio es el usuario `root`.

- *Gestionar opciones de configuración del servidor*

  El usuario que tenga este privilegio puede editar las opciones de configuración del servidor.

- *Seguimientos de flujos de trabajo*

  El usuario que tenga este privilegio puede consultar un registro detallado de la ejecución del flujo de trabajo si está marcada la casilla *Registro en archivos* de la sección *Registro* de la pestaña **Opciones**.

- *Lectura de estadísticas*

  Las estadísticas del servidor se registran en una base de datos interna y se pueden leer con la solución **`statistics.mtd`**. Este privilegio permite al usuario leer las estadísticas del servidor. Primero debe activar la característica definiendo un valor distinto a cero para el número de días durante el que se deben registrar estadísticas. Consulte la descripción de la opción de configuración Estadísticas para obtener más información.

- *Lectura de recursos globales*

  El usuario que tenga este privilegio puede leer la configuración/el alias de recursos globales desde el servidor.

- *Escritura de recursos globales*

  El usuario que tenga este privilegio puede escribir/guardar la configuración/el alias de recursos globales en el servidor.

- *Abrir flujo de trabajo desde MobileTogether Designer*

  El usuario que tenga este privilegio puede abrir un archivo de diseño de MobileTogether desde el servidor. Los datos de inicio de sesión de host se introducen en MobileTogether Designer con el comando **Archivo | Abrir desde MobileTogether Server**.

- *Guardar flujo de trabajo desde MobileTogether Designer*

  El usuario que tenga este privilegio puede guardar/implementar archivos de diseño de MobileTogether en el servidor. Los datos de inicio de sesión de host se introducen en MobileTogether Designer con el comando **Archivo | Abrir desde MobileTogether Server**.

- *Ejecución de simulaciones en el servidor*

  El usuario que tenga este privilegio puede ejecutar simulaciones desde el explorador (y consultar una vista previa del resultado). Recuerde que el botón **Atrás** del explorador conduce a la vista del contenedor.

4.7 Configurar el servidor de seguridad

Dirección IP del servidor y configuración de red del servidor de seguridad
Su servidor puede tener una dirección IP pública (a la que se puede acceder por Internet) y privada (a la que se puede acceder desde una red privada, como la red inalámbrica de la red de su empresa). Si un cliente móvil intenta conectarse por Internet usando la dirección IP privada del servidor, la conexión no funcionará. Esto se debe a que la dirección IP privada no se conoce en Internet y no se puede resolver. Si utiliza una dirección IP privada, el dispositivo cliente debería tener acceso a la red privada.

Para asegurarse de que el acceso al servidor sea posible, tiene dos opciones:

- Asignar al servidor una dirección IP pública para que se pueda acceder a él por Internet. El dispositivo cliente debe utilizar esta dirección IP pública para acceder al servidor.
- Si utiliza un servidor de seguridad e instala MobileTogether Server en un servidor con una dirección IP privada (dentro de la red privada), utilice el servidor de seguridad de la red para reenviar las solicitudes a una combinación de puerto y dirección IP pública del servidor MobileTogether Server. El dispositivo cliente debe utilizar la dirección IP pública.

También debería asegurarse de configurar el servidor de seguridad para permitir acceso al puerto de servidor utilizado para la comunicación con MobileTogether Client. Los puertos que utiliza MobileTogether Server se especifican en la página Configuración de la interfaz web de MobileTogether Server. En el dispositivo cliente este es el puerto que se debe usar como puerto de servidor para el acceso.

Consejo: en la mayoría de los servidores de seguridad el puerto `80` está abierto por defecto. Por tanto, si tiene problemas para configurar el servidor de seguridad y el puerto `80` no está conectado a ningún otro dispositivo, puede utilizarlo como puerto de MobileTogether Server para comunicarse con los clientes.

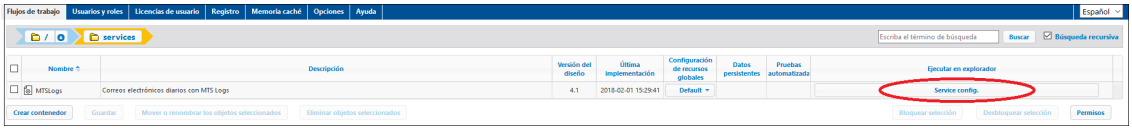
4.8 Configurar servicios

Un servicio servidor es una serie de acciones de MobileTogether que se implementa en **MobileTogether Server Advanced Edition** como solución (archivo `.mtd`). Las acciones definidas en el servicio se ejecutan cuando se cumple una serie especificada de condiciones de MobileTogether Server (o disparadores). En esta sección se explica cómo definir esos disparadores. Puede crear varios disparadores para un mismo servicio y puede habilitar o deshabilitar cualquiera de ellos.

Nota: el archivo de la solución (archivo `.mtd`) del servicio debe crearse en MobileTogether Designer. Para más detalles, consulte la documentación de MobileTogether Designer.

Acceder a la interfaz de configuración de un servicio

Si se ha implementado un servicio (desde MobileTogether Designer), este aparecerá en la pestaña de **Flujos de trabajo** junto al resto de soluciones. Un servicio se distingue de otras soluciones por el botón **Configuración del servicio** en la columna *Ejecutar en explorador* (*imagen siguiente*). A continuación se muestra un servicio llamado **`MTSLogs`** que se ha implementado en el contenedor **`/services`**. Para acceder a la interfaz de configuración (u opciones) del servicio, haga clic en **Configuración del servicio**.



La interfaz de configuración del sistema (opciones)

La interfaz de configuración (u opciones) del servicio permite definir y gestionar los desencadenadores que ejecutan el servicio (*imagen siguiente*).

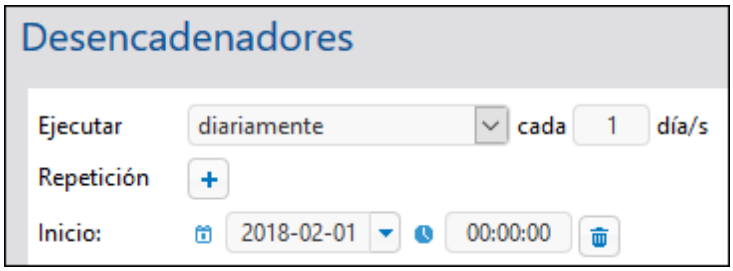
Puede crear los siguientes tipos de desencadenadores:

- *Desencadenadores temporizadores*, que permiten especificar a qué hora y con qué frecuencia dentro de un periodo de tiempo especificado desea que se ejecute el servicio.
- *Desencadenadores de sistema de archivos*, que permiten desencadenar un servicio al comprobar si existen cambios en un archivo o directorio del servidor.
- *Desencadenadores HTTP*, que permiten desencadenar un servicio al comprobar si existen cambios en un recurso localizado en una ubicación URI especificada.

Para añadir un desencadenador, haga clic en el botón del tipo de desencadenador correspondiente. En las secciones subordinadas de esta sección se describe con más detalle cada tipo de desencadenador. Una vez se ha creado un desencadenador, use los botones de la parte derecha del desencadenador para gestionarlo.

	Eliminar desencadenador.
	Duplicar desencadenador.
	Deshacer Borrar.

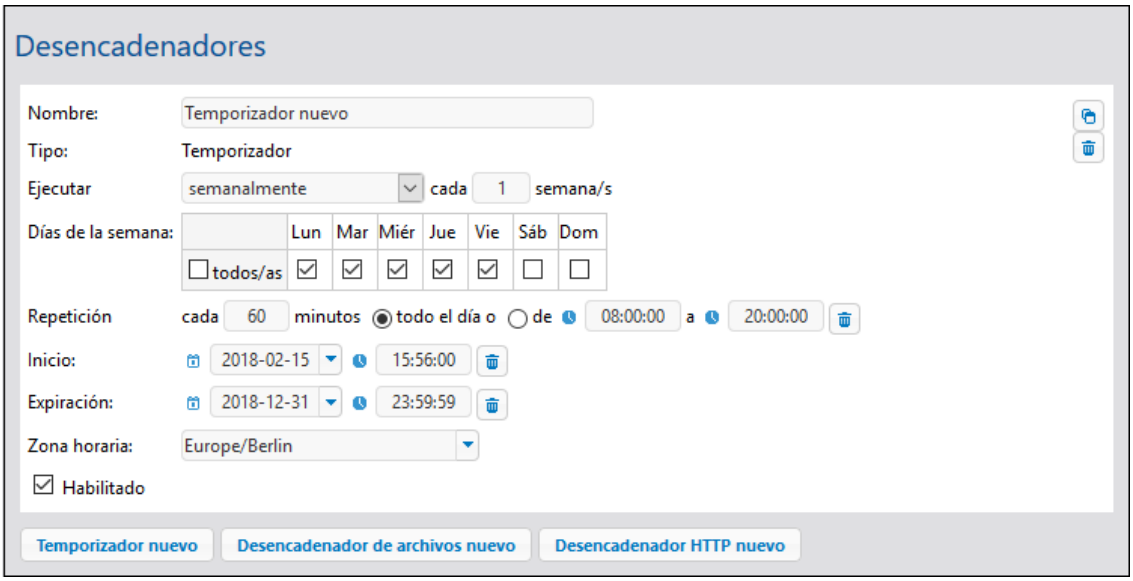
Junto a algunos campos se ven los botones y , que puede usar para establecer o eliminar el valor del campo del desencadenador. Por ejemplo, en la imagen siguiente no se ha establecido el valor *Repetir*, mientras que el valor Iniciar se ha establecido **`2018-01-26`**, **`00:00:00`**.



Guardar la configuración del servicio
Una vez configurados los desencadenadores del servicio, puede guardar dicha configuración haciendo clic en el botón **Guardar**, al final de la página.

4.8.1 Temporizadores

Un temporizador permite especificar a qué hora y con qué frecuencia dentro de un periodo de tiempo especificado desea que se ejecute el servicio. La imagen siguiente muestra cómo definir las opciones de un desencadenador temporizador.



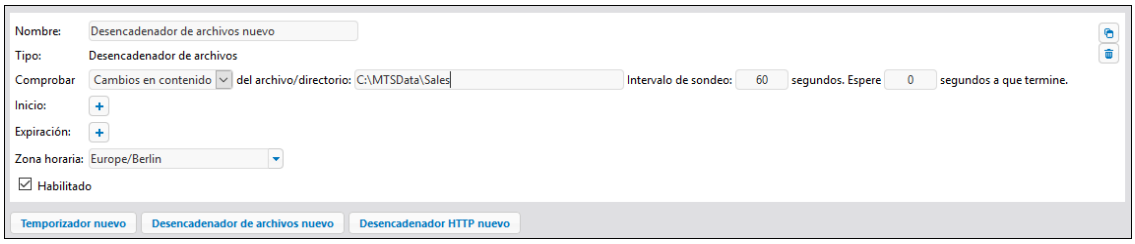
El temporizador se define con los siguientes parámetros:

- *Nombre:* el nombre del temporizador es una cadena que sirve como identificador del desencadenador.
- *Ejecutar:* define si el desencadenador debe iniciarse una vez o de forma periódica cada **N** número de días.
- *Repetición:* define la frecuencia del servicio con "cada **x** minutos" dentro de un periodo de tiempo especificado por usted.
- *Inicio, Expiración:* define respectivamente la hora de comienzo y de finalización del periodo dentro del cual se ejecuta el servicio.
- *Zona horaria:* especifica la zona horaria que corresponde a los valores de los campos *Inicio* y *Fin*.
- *Habilitado:* al hacer clic en esta casilla se habilita/deshabilita el desencadenador.

4.8.2 Desencadenadores de archivos

Un desencadenador de archivos permite comprobar si hay cambios dentro de un archivo o directorio, como archivos añadidos recientemente o modificados (no incluye archivos eliminados). Puede configurar el intervalo de sondeo y tiene la opción de determinar el momento de comienzo y de finalización del desencadenador. También puede usar comodines para filtrar archivos específicos del directorio. La imagen siguiente muestra cómo definir las opciones de un

desencadenador de sistema de archivos.

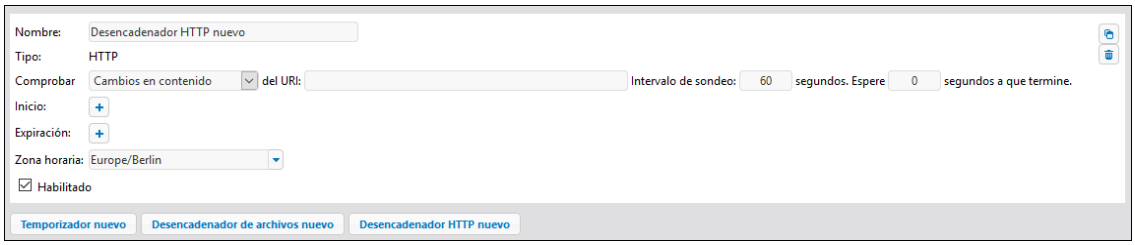


El desencadenador se define con los siguientes parámetros:

- *Nombre:* el nombre del temporizador es una cadena que sirve como identificador del desencadenador.
- *Controlar contenido*: calcula y almacena un código de comprobación de los archivos especificados dentro del directorio. Cuando haya pasado el intervalo de sondeo, el código de comprobación se vuelve a calcular y se compara con los valores almacenados. Si hay alguna diferencia, se inicia el desencadenador. Tenga en cuenta que esto puede aumentar considerablemente la carga del servidor cuando comprueba un directorio. El desencadenador también se inicia si se ha añadido un nuevo archivo al directorio o si alguna fecha ha cambiado.
- *Controlar fecha de modificación*: comprueba la marca de tiempo de la última modificación. Si esta ha cambiado, se inicia el desencadenador.
- *Intervalo de sondeo*: especifica la frecuencia en segundos con la que debe sondearse el archivo o directorio.
- *Esperar N segundos a que termine*: define el tiempo en segundos que esperará el servidor antes de iniciar el siguiente servicio.
- *Inicio, Expiración (opcional)*: define respectivamente la hora de comienzo y de finalización del periodo dentro del cual se ejecuta el servicio.
- *Zona horaria:* especifica la zona horaria que corresponde a los valores de los campos *Inicio* y *Fin*.
- *Habilitado:* al hacer clic en esta casilla se habilita/deshabilita el desencadenador.

4.8.3 Desencadenadores HTTP

Un desencadenador HTTP permite comprobar si ha habido cambios en una URI. Para ello comprueba si ha habido cambios en los campos de encabezado HTTP **`Last-Modified`** y **`Content-MD5`**. Puede configurar el intervalo de sondeo y tiene la opción de determinar el momento de comienzo y de finalización del desencadenador. La imagen siguiente muestra cómo definir las opciones de un desencadenador HTTP.



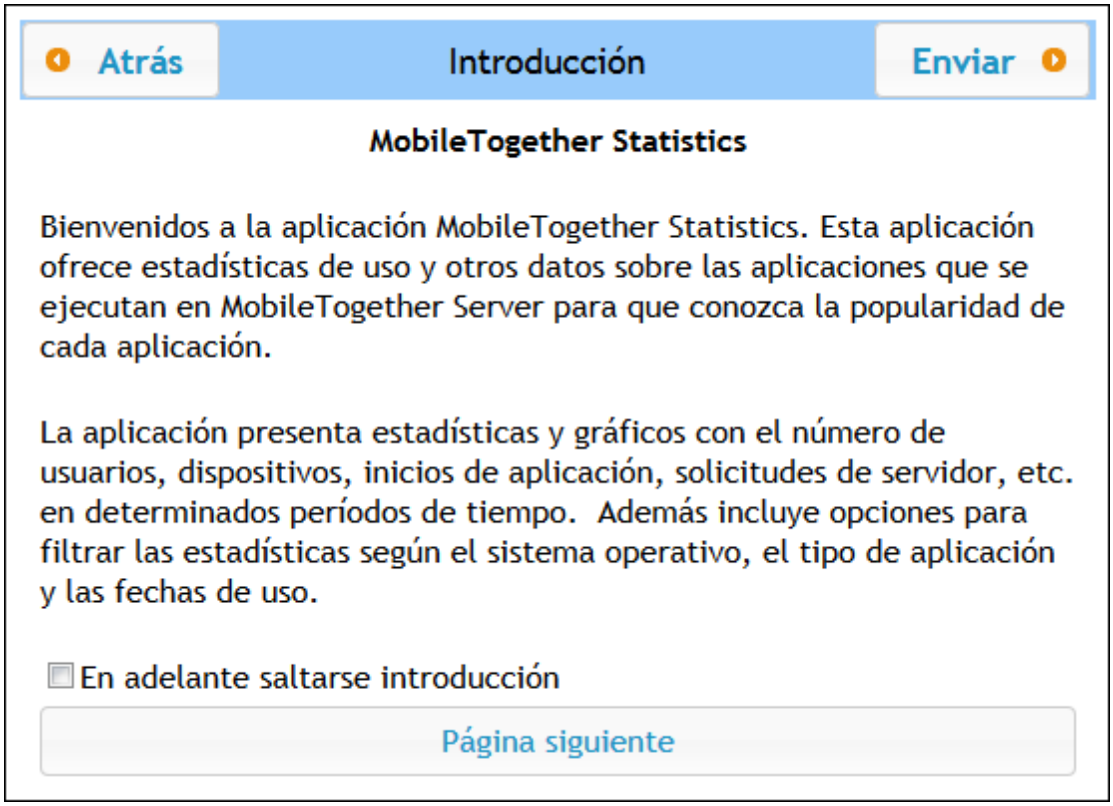
El desencadenador se define con los siguientes parámetros:

- *Nombre:* el nombre del temporizador es una cadena que sirve como identificador del desencadenador.
- *Controlar contenido*: Comprueba el encabezado HTTP opcional **`Content-MD5`**. Este es un resumen de 128 bits que se usa para verificar la integridad de un mensaje. Si el encabezado ha cambiado una vez ha pasado el intervalo de sondeo, el desencadenador se inicia. Si el servidor no proporciona el encabezado en la ubicación HTTP, se recupera el contenido y se le asigna un código de comprobación local. Esos códigos de comprobación se comparan en sondeos posteriores.
- *Controlar fecha de modificación*: comprueba el encabezado HTTP **`Last-Modified`**. Si falta el encabezado, se comprueba el encabezado **`Content-MD5`** (*punto anterior*).
- *Intervalo de sondeo*: especifica la frecuencia en segundos con la que debe sondearse la URI.
- *Esperar N segundos a que termine*: define el tiempo en segundos que esperará el servidor antes de iniciar el siguiente servicio.
- *Inicio, Expiración (opcional)*: define respectivamente la hora de comienzo y de finalización del periodo dentro del cual se ejecuta el servicio.
- *Zona horaria:* especifica la zona horaria que corresponde a los valores de los campos *Inicio* y *Fin*.
- *Habilitado:* al hacer clic en esta casilla se habilita/deshabilita el desencadenador.

4.9 Estadísticas de uso de soluciones

Las estadísticas de uso de las soluciones se pueden ver en la solución **Statistics**, situada por defecto en el contenedor **/admin**. La solución **Statistics** muestra gran variedad de estadísticas sobre las distintas soluciones durante el período de tiempo que seleccione el usuario. Además cuenta con varios filtros que le permitirán consultar datos de uso como el número de usuarios, el tipo de dispositivo o sistema operativo, períodos de máximo uso, etc.

En la imagen siguiente puede ver la página de introducción de la solución **Statistics**.



Configurar la solución Statistics

A partir de la versión 4.0 de MobileTogether Server la solución **Statistics** viene implementada en MobileTogether Server por defecto y se encuentra en el contenedor **/admin**.

Si tiene una versión de MobileTogether Server anterior a la versión 4.0 y quiere usar la solución **Statistics**, deberá seguir estas instrucciones :

1. Pásese a la versión 4.0 o a una versión superior de MobileTogether Server.
2. Inicie sesión en la interfaz de administración de MobileTogether Server desde un explorador web (introduciendo la URL **http://<direcciónIPoNombreDelServidor>:8085/**.

3. Introduzca sus datos de inicio de sesión y abra la pestaña Flujos de trabajo.
4. Haga clic en el botón **Crear contenedor**, introduzca el nombre de contenedor **admin** y haga clic en **Guardar y abrir**.
5. En MobileTogether Designer abra el archivo **Statistics.mtd** (situado en la carpeta **Solutions** de la carpeta de datos de MobileTogether Server (*ver tabla más abajo*).
6. Tras abrir el archivo **Statistics.mtd** en MobileTogether Designer, impleméntelo en el contenedor **/admin** de MobileTogether Server (esto se hace con el comando de menú **Archivo | Implementar en MobileTogether Server** de MobileTogether Designer).
7. En la interfaz de administración de MobileTogether Server abra la pestaña Opciones y, en el panel Estadísticas, defina un entero positivo como valor de la opción *Límite de las estadísticas* (esto activará el seguimiento de datos estadísticos).
8. Para poder consultar estadísticas de soluciones a partir de este momento concreto inicie la solución **Statistics** (en MobileTogether Server abra la pestaña Flujos de trabajo y después el contenedor **/admin**. Desde este contenedor puede iniciar la solución **Statistics**. Otra opción es introducir la URL **http://<direcciónIPoNombreDelServidor>:8085/run?d=/admin/Statistics/**.

Nota: la solución **Statistics** se puede implementar en cualquier contenedor. Para ejecutar la solución basta con modificar la URL de la solución para que apunte al contenedor correcto.

Ubicación de la carpeta de datos de la aplicación MobileTogether Server dependiendo del sistema operativo

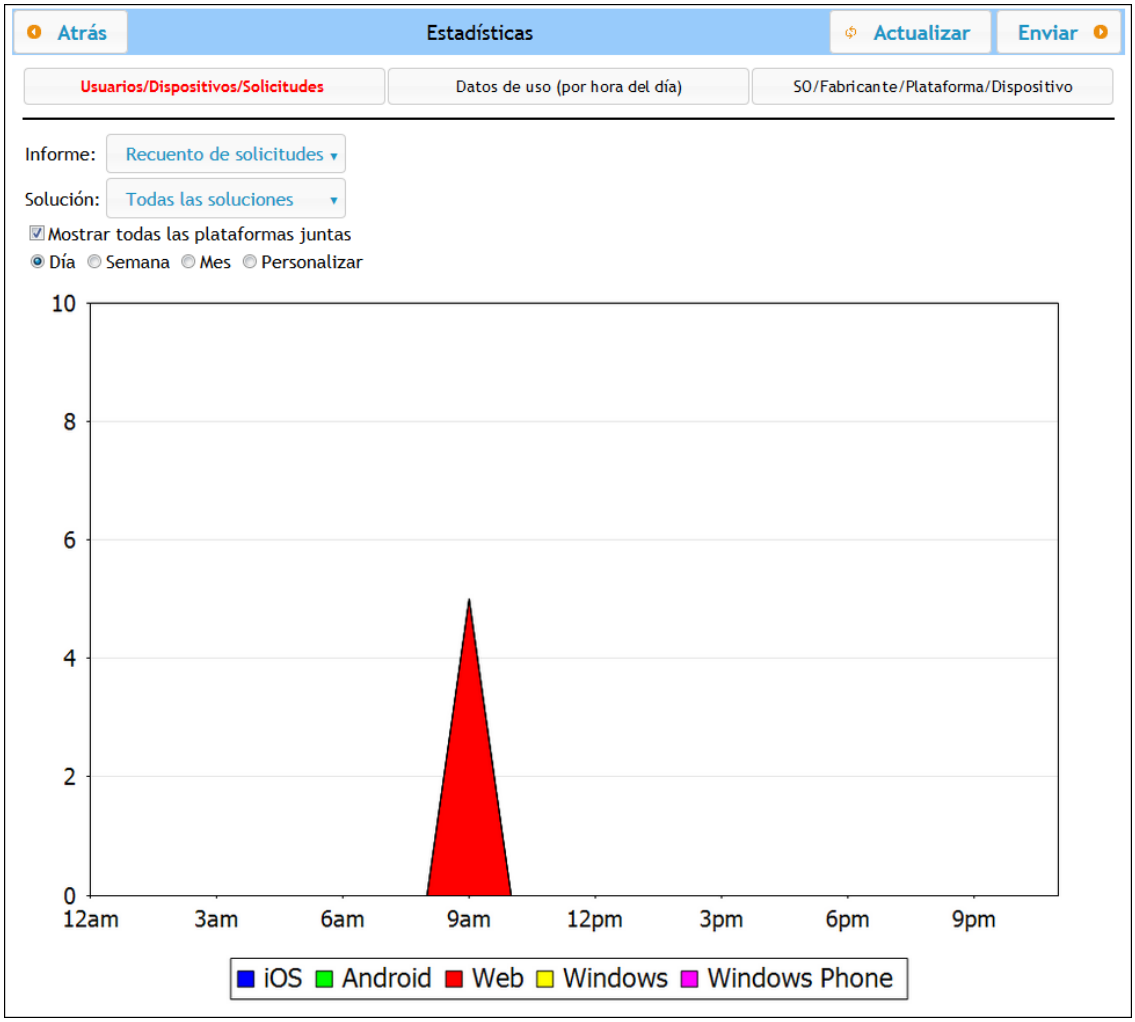
Linux	`/var/opt/Altova/MobileTogetherServer`
Mac	`/var/Altova/MobileTogetherServer`
Windows 7, 8, 10	`C:\ProgramData\Altova\MobileTogetherServer`

Descripción de la solución Statistics

La interfaz de la solución **Statistics** (*imagen siguiente*) está compuesta por tres pestañas:

- Usuarios/Dispositivos/Solicitudes
- Datos de uso (por hora del día)
- SO/Fabricante/Plataforma/Dispositivo

El nombre de la pestaña activa aparece en rojo (*imagen siguiente*).



Cada pestaña cuenta con un filtro llamado *Solución* y con uno o dos filtros más. El filtro *Solución* permite seleccionar una sola solución de las que están implementadas en el servidor. También puede seleccionar todas las soluciones. Los otros filtros sirven para seleccionar la categoría de estadísticas que se desea consultar. Y también puede seleccionar un período de tiempo concreto.

Usuarios/Dispositivos/Solicitudes
En el filtro *Informe* puede seleccionar estas opciones:

- *Usuarios:* el número de usuarios de cada plataforma.
- *Dispositivos*: el número de dispositivos de cada plataforma.
- *Recuento de solicitudes*: el número de solicitudes en cada plataforma.
- *Inicio de la solución*: número de veces que se inició la solución en cada plataforma.

Si selecciona la opción *Mostrar todas las plataformas juntas*, aparecerán todas las plataformas en un solo gráfico (iOS, Android, Web, Windows y Windows Phone) y cada una aparece en un color diferente. Si no selecciona la opción *Mostrar todas las plataformas juntas*, podrá ver un

gráfico para cada plataforma seleccionando la opción correspondiente en el filtro *Plataforma*.

Datos de uso (por hora del día)
Muestra la intensidad de uso de la solución seleccionada en un período de 24 horas de cada día de la semana anterior. El filtro *Plataforma* sirve para seleccionar la plataforma que desea consultar (iOS, Android, Web, Windows y Windows Phone). En el filtro *Informe* puede seleccionar estas opciones:

- *Usuarios:* el número de usuarios de cada segmento de tiempo.
- *Dispositivos*: el número de dispositivos de cada segmento de tiempo.
- *Recuento de solicitudes*: el número de solicitudes en cada segmento de tiempo.
- *Inicio de la solución:* el número de veces que se inició la solución en cada segmento de tiempo.

SO/Fabricante/Plataforma/Dispositivo

Muestra el porcentaje de uso de la solución seleccionada en el SO, el fabricante y el tipo de dispositivo seleccionados. Por ejemplo, si consulta las estadísticas de las diferentes plataformas, se representa el porcentaje que representa cada plataforma en el uso total de la solución. En todos los casos se usan gráficos circulares y cada instancia del criterio seleccionado es una porción del gráfico circular. En el filtro *Informe* puede seleccionar estas opciones:

- *SO:* cada sistema operativo aparece con un color diferente.
- *Fabricante:* cada fabricante aparece con un color diferente.
- *Plataforma:* cada plataforma aparece con un color diferente.
- *Tipo de dispositivo:* cada tipo de dispositivo aparece con un color diferente.

4.10 Información para clientes

La aplicación MobileTogether Client del dispositivo móvil deberá conectarse a MobileTogether Server y necesitará conocer esta información sobre el servidor:

Dirección IP	dirección IP de MobileTogether Server
Puerto	puerto HTTP o HTTPS especificado en la opción de configuración *Puertos de clientes móviles*
SSL	indica si la comunicación tiene cifrado SSL o no
Nombre de usuario	cuenta de usuario que se utiliza para acceder al servidor. Esto determinará los derechos de acceso. Consulte Usuarios y roles para obtener más información
Contraseña	contraseña de la cuenta de usuario

Nota: los datos que se guarden en el cliente web se guardan en el almacenamiento local (es decir, almacenamiento web) del explorador. Estos exploradores son compatibles con almacenamiento local HTML 5.0::

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

Actualizar configuración del servidor en dispositivos cliente

Para poder ejecutar una solución, el dispositivo cliente debe tener configuradas las opciones de acceso del servidor. Si cambiara la configuración del servidor (por ejemplo, imagine que el servidor MobileTogether Server se mueve a otro equipo con otra dirección IP), también será necesario cambiar la configuración del servidor en el dispositivo cliente. En MobileTogether Designer puede usar la función **`mt-server-config-url`** de MobileTogether para generar una URL que contenta la nueva configuración del servidor (por ejemplo **`mobiletogether://mt/change-settings?settings=<json encoded settings>`**). Después puede enviar un correo a los usuarios finales con la nueva URL. Cuando el usuario final pulse el enlace, se actualizará automáticamente la configuración del servidor en el cliente. Consulte el *Manual del usuario de MobileTogether Designer* para obtener más información.

4.11 Copias de seguridad y restaurar datos

En este apartado explicamos cómo crear copias de seguridad y restaurar datos en MobileTogether Server.

- Las copias de seguridad consisten en copiar archivos de datos de la aplicación que son esenciales en una ubicación segura.
- La restauración de datos consiste en copiar los archivos de la copia de seguridad en la nueva instalación de MobileTogether Server.
- Actualizar las conexiones de los clientes con el servidor.

Copias de seguridad de MobileTogether Server

Antes de empezar a crear la copia de seguridad es necesario detener el servicio MobileTogether Server. Esto es necesario para evitar conflictos entre el estado de la BD de los archivos activos y de los archivos de la copia de seguridad. Los archivos de MobileTogether Server que deben guardarse en la copia de seguridad están situados por defecto en la carpeta de datos de la aplicación (ver más abajo). Si lo prefiere, puede editar el archivo de configuración `.cfg` con un editor de texto en lugar de cambiar las opciones de configuración desde la interfaz web o la interfaz de la línea de comandos.

La ubicación de la carpeta de datos de la aplicación depende del sistema operativo y de la plataforma. A continuación puede ver la ubicación predeterminada de esta carpeta en cada sistema.

Linux	`/var/opt/Altova/MobileTogetherServer`
Mac	`/var/Altova/MobileTogetherServer`
Windows 7, 8, 10	`C:\ProgramData\Altova\MobileTogetherServer`

En la siguiente tabla puede ver los archivos y carpetas principales de la carpeta de datos de la aplicación.

cache	Directorio predeterminado para las memorias caché de las soluciones. Si no hay una memoria caché disponible, se recreará automáticamente en tiempo de ejecución.
logs	Directorio predeterminado para los archivos de registro que se crean cuando está habilitada la opción *Registro en archivos* y para los registros generales de MobileTogether Server.
SolutionFiles	Directorio predeterminado para los archivos XML o de imagen a los que se hace referencia en las soluciones implementadas.
cert.pem	Archivo PEM con el certificado necesario para la comunicación segura por SSL.
key.pem	Archivo PEM con la clave privada necesaria para la comunicación segura por SSL.

mobiletogether.db	Archivo de base de datos principal (SQLite) donde se almacena el sistema de objetos de MobileTogether Server, los datos de los usuarios, las soluciones implementadas, archivos, etc.
mobiletogetherlog.db	Archivo de base de datos (SQLite) donde se almacenan los registros de MobileTogether Server.
mobiletogetherserver.cfg	Archivo de configuración donde se almacenan las opciones de configuración globales de MobileTogether Server (número de puerto, directorio de soluciones, etc.)
mobiletogetherserver.licsid	Archivo con el id. del cliente LicenseServer registrado.
mobiletogetherserver.licsvr	Archivo con la dirección del servidor LicenseServer y del servidor de conmutación por error por si éste fallara.

Nota: antes de instalar cada versión nueva de MobileTogether Server, los archivos y carpetas de la tabla anterior se copian por defecto en una carpeta de copia de seguridad ubicada en la carpeta de datos de la aplicación (*ver más arriba*). El nombre de cada carpeta de copia seguridad incluye la fecha y la hora de la copia de seguridad. Si prefiere deshabilitar la creación automática de copias de seguridad antes de la próxima instalación, modifique la opción correspondiente en la pestaña **Opciones**.

Restaurar datos en MobileTogether Server

Siga estas instrucciones para restaurar una configuración previa de MobileTogether Server a partir de los archivos de la copia de seguridad:

1. Instale la misma versión de MobileTogether Server que la versión donde creó la copia de seguridad.
2. Detenga el servicio MobileTogether Server.
3. Copie los archivos de la copia de seguridad en las carpetas correspondientes de la nueva instalación.
4. Inicie el servicio MobileTogether Server.

Actualizar conexiones de los clientes con el servidor

Si movió MobileTogether Server a otro equipo (con otra configuración, como la dirección IP, por ejemplo), será necesario actualizar la configuración de los dispositivos cliente para que se puedan conectar a MobileTogether Server. Consulte el apartado Información para clientes para obtener más información.

4.12 Preguntas frecuentes

- *En nuestro servidor tenemos varios flujos de trabajo y ahora hay una solución nueva que utiliza una conexión ADO con una base de datos IBM DB2. El problema es que cuando un cliente intenta acceder a esta solución, MobileTogether Server se bloquea. Eliminar el flujo de trabajo no soluciona el problema. Lo único que funciona es reiniciar el servidor. Pero cada vez que un cliente accede a esta solución tenemos el mismo problema. ¿Qué ocurre?*

  Se trata de un problema conocido y está relacionado con las bases de datos en cuestión. Los flujos de trabajo que contienen conexiones ADO a bases de datos IBM DB2 o Informix hacen que el servidor se bloquee cuando el flujo de trabajo solicita al servidor acceder a la base de datos por primera vez. El problema persiste incluso después de eliminar la solución porque, al parecer, algunos datos de conexión se guardan en la memoria del servidor. Estos datos de conexión no se eliminan hasta que el servidor se reinicia.

Altova MobileTogether Server

Referencia de la interfaz web

5 Referencia de la interfaz web

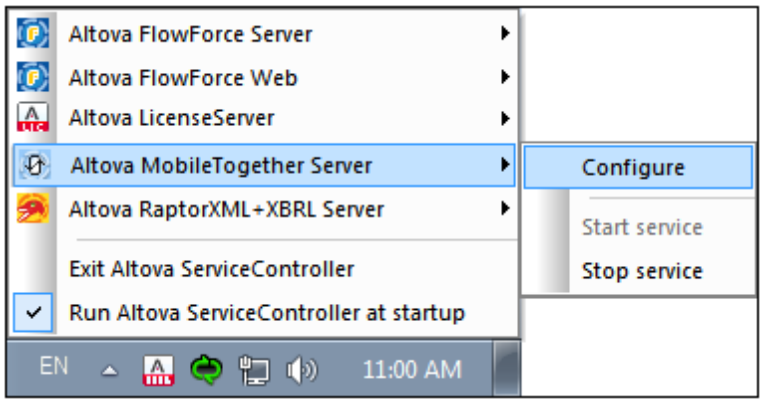
MobileTogether Server dispone de una interfaz web donde se pueden configurar todas las opciones del servidor. Esta interfaz web se puede abrir en cualquier explorador web y funciona con todos los sistemas operativos compatibles.

Acceso a la interfaz web de MobileTogether Server

A continuación puede ver cómo se accede a la interfaz web de MobileTogether Server en cada sistema compatible.

- Windows

  Haga clic en el icono **ServiceController** de la bandeja del sistema (*imagen siguiente*) y después en **Altova MobileTogether Server**. Esto abre un menú contextual donde debe elegir el comando **Configure**. Si todavía no se está ejecutando MobileTogether Server, elija la opción *Start Service* para iniciar MobileTogether Server.



  Introduzca su nombre de usuario y contraseña para iniciar sesión. La combinación de usuario y contraseña predeterminada es `root/root`. Si se definió el inicio de sesión de Active Directory a través de algún dominio, la página de acceso incluirá un cuadro combinado llamado *Acceso:* donde podrá (i) seleccionar uno de los dominios definidos o (ii) iniciar sesión directamente (y no a través del dominio).

  También puede introducir esta URL en un explorador web: **`http://<direcciónIPoNombreDelServidor>:8085/`**.

- Linux

  Introduzca la URL de la interfaz web en la barra de dirección del explorador y pulse **Entrar**. Esta es la URL predeterminada de la página de la interfaz web:
  `http://<direcciónIPoNombreDelServidor>:8085/`

Introduzca su nombre de usuario y contraseña para iniciar sesión. La combinación de usuario y contraseña predeterminada es `root/root`. Si se definió el inicio de sesión de Active Directory a través de algún dominio, la página de acceso incluirá un cuadro combinado llamado *Acceso:* donde podrá (i) seleccionar uno de los dominios definidos o (ii) iniciar sesión directamente (y no a través del dominio).

▼ macOS

Introduzca la URL de la interfaz web en la barra de dirección del explorador y pulse **Entrar**. Esta es la URL predeterminada de la página de la interfaz web:

`http://<direcciónIPoNombreDelServidor>:8085/`

Introduzca su nombre de usuario y contraseña para iniciar sesión. La combinación de usuario y contraseña predeterminada es `root/root`. Si se definió el inicio de sesión de Active Directory a través de algún dominio, la página de acceso incluirá un cuadro combinado llamado *Acceso:* donde podrá (i) seleccionar uno de los dominios definidos o (ii) iniciar sesión directamente (y no a través del dominio).

Pestañas de la interfaz web

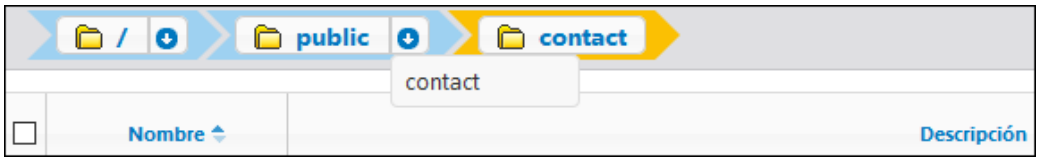
La interfaz web constituye una interfaz de administración de MobileTogether Server y las funciones administrativas disponibles se agrupan en las diferentes pestañas de la interfaz:

- **Flujos de trabajo:** en esta página podrá gestionar la estructura de contenedores del servidor y los permisos de cada contenedor.
- **Usuarios y roles:** aquí podrá configurar cuentas de usuario y roles y los privilegios que tengan asociados. En esta página se definen los derechos de acceso de cada usuario.
- **Licencias de usuario:** lista de dispositivos móviles que tienen asignadas licencias e información sobre las licencias.
- **Registro:** muestra las acciones del servidor registradas y ofrece filtros para navegar por la lista.
- **Memoria caché:** información detallada sobre las memorias caché disponibles en el servidor. Aquí puede activar, desactivar y eliminar memorias caché.
- **Opciones:** opciones de configuración de MobileTogether Server, como puertos de acceso, configuración del registro, tiempos de espera de la sesión.

5.1 Flujos de trabajo

La pestaña **Flujos de trabajo** (*imagen siguiente*) sirve como interfaz para gestionar la estructura de contenedores de la carpeta raíz de MobileTogether Server y definir los derechos de acceso (permisos) para cada contenedor. Los contenedores y carpetas pueden incluir contenedores subordinados y soluciones (también llamados archivos de diseño o `.mtd` files). Los archivos MTD no se añaden a los contenedores de MobileTogether Server desde la interfaz web del servidor sino que se implementan al servidor desde MobileTogether Designer. Durante la implementación es necesario especificar la ruta de acceso exacta del contenedor. En MobileTogether Designer puede examinar el sistema hasta encontrar el contenedor pertinente.

- La pestaña **Flujos de trabajo** contiene por defecto el contenedor raíz `"/"`.
- Al hacer clic en flecha **Abajo** junto al nombre de un contenedor se muestran los contenedores subordinados. Haga clic en un contenedor subordinado de la lista desplegable para acceder a él.
- Para acceder a un contenedor, haga clic en él.
- En la parte superior de la ventana se muestra el recorrido como "migas de pan" conforme va descendiendo por la jerarquía de los contenedores. La flecha **Abajo** de cada nivel muestra los contenedores subordinados de ese contenedor, lo que facilita la navegación entre contenedores.



- Para seleccionar un contenedor, haga clic en la casilla de verificación de dicho contenedor. Una vez seleccionado un contenedor, se puede renombrar, mover o eliminar (*imagen siguiente*).

▼ Características

La pestaña **Flujos de trabajo** contiene estos botones:

Crear contenedor	Crea un contenedor en la carpeta actual. Haga clic en un contenedor para abrirlo
Guardar	Guarda los cambios realizados (p. ej. cambios en la descripción de un contenedor)
Mover o renombrar los objetos seleccionados	Si se selecciona un objeto, se abre un cuadro de diálogo con el que puede (i) renombrar y/o (ii) mover el objeto al contenedor que seleccione. Si se seleccionan varios objetos, se abre un cuadro de diálogo que le permite trasladar esos objetos al contenedor que seleccione.
Eliminar	Elimina el contenedor o archivo seleccionado

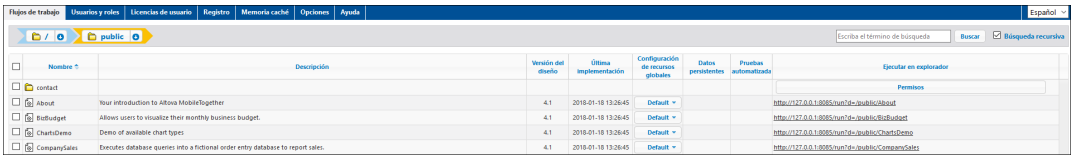
objetos seleccionados	
Bloquear selección	Las soluciones que están bloqueadas no se pueden sobrescribir con una nueva implementación. Si se intenta sobrescribir una solución bloqueada, MobileTogether Designer emite un error.
Desbloquear selección	Desbloquea una solución bloqueada.
Permisos	Determina qué usuarios/roles tienen acceso a cada contenedor y el nivel de acceso
Buscar	Busca el término de búsqueda indicado. Marque la casilla *Búsqueda recursiva* para buscar en los contenedores descendientes

Otras acciones:

- Para volver al principio de la jerarquía de contenedores haga clic en la carpeta primaria correspondiente en la ruta de acceso que aparece en la parte superior de la pestaña **Flujos de trabajo**.
- Haga clic en un contenedor para ver sus descendientes.
- Para ejecutar una solución haga clic en su URL.

Contenedor /public/

Haga clic en el contenedor **`public`** para ver su contenido (*imagen siguiente*). Este contenedor está predefinido en el sistema y contiene todos los archivos de diseño de muestra (soluciones) que vienen con el programa. Para ejecutar una solución haga clic en su URL.



Presentación del contenido de un contenedor

Los contenedores tienen contenedores subordinados y soluciones (es decir, archivos de diseño o `.mtd`). El contenido de cada contenedor se presenta en forma de tabla y las columnas de esta tabla muestran las propiedades de las soluciones:

- *Nombre:* nombre del archivo de la solución tal y como se guardó en MobileTogether Designer.
- *Aplicación, Versión de la aplicación:* estas columnas solamente aparecen si en el servidor se implementaron aplicaciones para la AppStore (consulte el *Manual del usuario de MobileTogether Designer*). Estas columnas incluyen el nombre de la aplicación para la AppStore y su número de versión.
- *Descripción:* breve descripción de la solución que se puede editar con solo hacer clic en este campo.
- *Versión del diseño:* número de versión de MobileTogether Designer en la que se creó la solución.
- *Última implementación:* fecha y hora de la última implementación de la solución.

- *Configuración de recursos globales*: recurso global definido para la solución e implementado en el servidor. Si no se especificó ningún recurso global, esta columna muestra el valor `Default` (configuración predeterminada).
- *Datos persistentes:* si durante la ejecución de la solución se realizaron cambios en los datos, esta columna tendrá el botón **Borrar datos**. Haga clic en este botón para deshacer los cambios realizados.
- *Prueba automatizada:* un icono en forma de rueda azul indica que la solución cuenta con al menos una ejecución de prueba para las pruebas automatizadas pero la ejecución de prueba no está activa. Un icono en forma de rueda rojo indica que al menos una de las ejecuciones de prueba disponibles está activa. Para activar una ejecución de prueba de un diseño o configurar cómo se debe reproducir la ejecución de prueba en el cliente, haga clic en el icono en forma de rueda de la solución (*imagen anterior*). Al hacer clic en el icono en forma de rueda aparece una página donde se enumeran todas las pruebas automatizadas de la solución (*ver más abajo*). Para más información sobre pruebas automatizadas consulte la documentación de MobileTogether Designer.
- *Ejecutar en explorador:* URL del servidor donde está implementado el archivo de la solución. Haga clic en esta URL para ejecutar la solución.Si la solución define servicios servidor, haga clic en el botón **Configuración del servicio** de esta columna para acceder a la interfaz de configuración del servicio.

Pruebas automatizadas

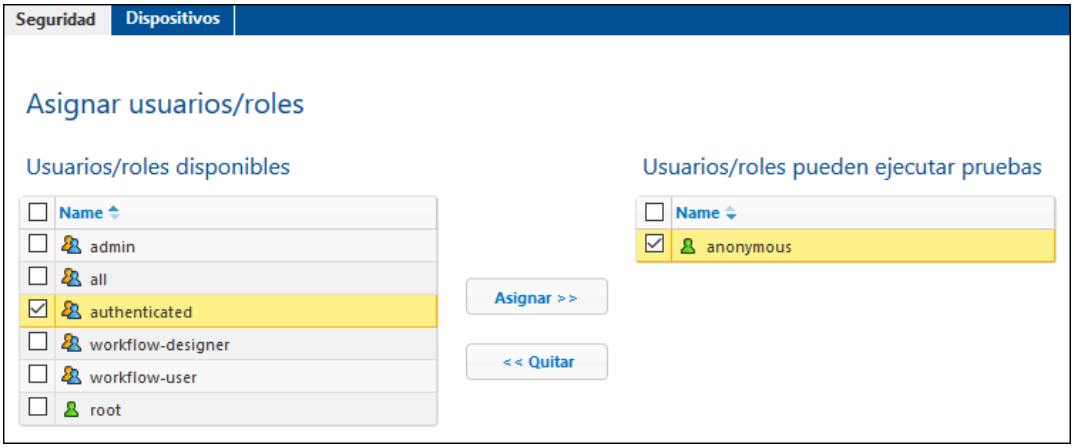
Al hacer clic en el icono de la columna *Prueba automatizada* de una solución, aparece una página donde se enumeran todas las pruebas automatizadas de la solución (*imagen siguiente*).

La página **Pruebas automatizadas** enumera todas las ejecuciones de prueba que se implementaron en el servidor para la solución seleccionada. Puede configurar las ejecuciones de prueba por separado para que se reproduzcan en los dispositivos cliente:

1. En la columna *Activa* marque las ejecuciones de prueba que desea activar. Estas ejecuciones de prueba se reproducirán en el cliente cuando el usuario inicie una solución. Si se seleccionan varias ejecuciones de prueba, entonces se reproducirán todas. Si se desactiva alguna de las ejecuciones de prueba de una solución, entonces en la página **Flujos de trabajo** el icono en forma de rueda de la columna *Prueba automatizada* del diseño aparecerá en color rojo.
2. Establezca la velocidad de la ejecución de prueba en la columna *Tipo de ejecución*.
3. Configure las opciones de registro que desea usar durante la reproducción. Para ello basta con marcar las casillas de las columnas pertinentes. Para más información sobre estas opciones consulte la sección *Pruebas automatizadas* de la documentación de MobileTogether Designer.
4. Para terminar haga clic en **Guardar**.

Si desea eliminar una ejecución de prueba, marque su casilla en la primera columna y haga clic en **Eliminar selección**.

Permisos
En la parte inferior de la página *Pruebas automatizadas* puede especificar: (i) qué usuarios y roles pueden realizar pruebas automatizadas para la solución seleccionada (en la pestaña *Seguridad*) y (ii) en qué dispositivos se pueden realizar pruebas automatizadas (pestaña *Dispositivos*).



- Los usuarios y roles se seleccionan en la pestaña Seguridad, los dispositivos en la pestaña Dispositivos (*imagen anterior*).
- Para asignar un usuario/rol o un dispositivo, selecciónelos en el panel izquierdo y haga clic en Asignar (*imagen anterior*).
- Elimine un usuario/rol o dispositivo de la lista Autorizados seleccionándolo y haciendo clic en **Quitar**.
- Puede asignar o quitar varios objetos seleccionados al mismo tiempo.
- Si no hay ningún dispositivo asignado en la lista Autorizados, las pruebas automatizadas para esa solución pueden realizarse en **todos** los dispositivos.

Nota: Todas las pruebas automatizadas que se hayan implementado en una versión del servidor previa a la versión 4.1 (publicada el 27de febrero de 2018) o superior reciben permisos de seguridad para todos los usuarios/roles; es decir, todos los usuarios/roles pueden ejecutar pruebas automatizadas, igual que antes de la actualización. Para las pruebas automatizadas que se implementen después de haber actualizado el servidor a la versión 4.1 no hay permisos asignados a ningún usuario/rol, por lo que es necesario especificar explícitamente qué usuarios/roles pueden ejecutar pruebas automatizadas.

Permisos

Los permisos son derechos de acceso que se pueden definir para cada contenedor del sistema. Estos permisos determinan qué usuarios y roles tienen acceso al contenedor y qué tipo de acceso tienen (lectura, escritura o uso). Puede definir estos derechos de acceso para el contenedor y para sus flujos de trabajo (o soluciones).

- *Reglas para heredar permisos*
  - Los contenedores heredan permisos de su contenedor primario.
  - Los usuarios heredan los permisos que se le asignaran directamente y los permisos de todos los roles a los que pertenece el usuario.
  - Las reglas de herencia de los usuarios tienen prioridad sobre las reglas de herencia del contenedor.
  - Si se vuelve a definir un permiso de un rol al que pertenece un usuario, se reemplazará la herencia del contenedor para dicho permiso.

El sistema comprueba los permisos del usuario cada vez que éste interactúa. Por tanto, el usuario no podrá acceder o editar contenidos si no tiene los permisos necesarios. Puede definir permisos para estos componentes:

Contenedores

- *Lectura:* el usuario puede ver los contenidos del contenedor y buscar objetos en el contenedor.
- *Lectura, Escritura:* además de leer objetos, el usuario puede crear objetos nuevos y eliminar objetos actuales.

Flujos de trabajo

- *Lectura:* el usuario puede ejecutar soluciones.
- *Lectura, Escritura:* además de ejecutar soluciones, el usuario puede escribir en los datos de la solución. Para modificar los datos del archivo, el usuario debe tener permiso de escritura en el contenedor correspondiente.

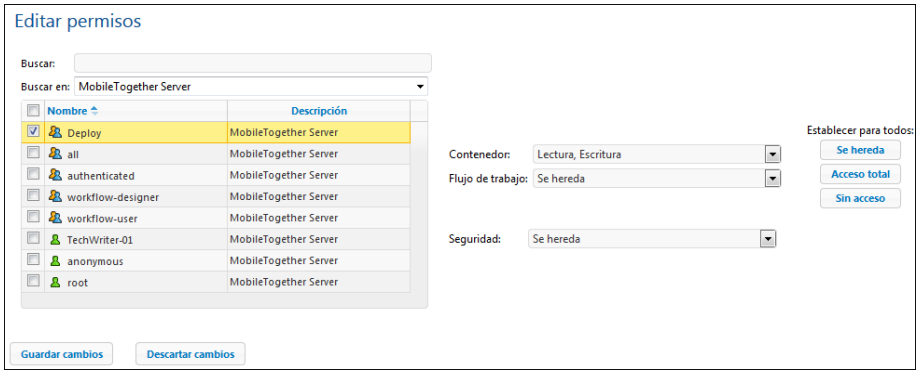
Nivel de seguridad

- *Lectura:* el usuario puede leer la lista de permisos de cualquier objeto secundario del contenedor.
- *Lectura, Escritura:* además de leer la lista de permisos, el usuario puede cambiar la lista de permisos de cualquier objeto secundario del contenedor.
- Los usuarios pueden leer por defecto los permisos que tiene asignados y los del rol al que pertenece solamente. Sin embargo, si se concede el privilegio *Lectura de usuarios y roles*, el usuario podrá leer todos los permisos.

- *Editar los permisos de un contenedor*
  1. Haga clic en el botón **Permisos** del contenedor para abrir la página de permisos del

contenedor seleccionado (*imagen siguiente*).

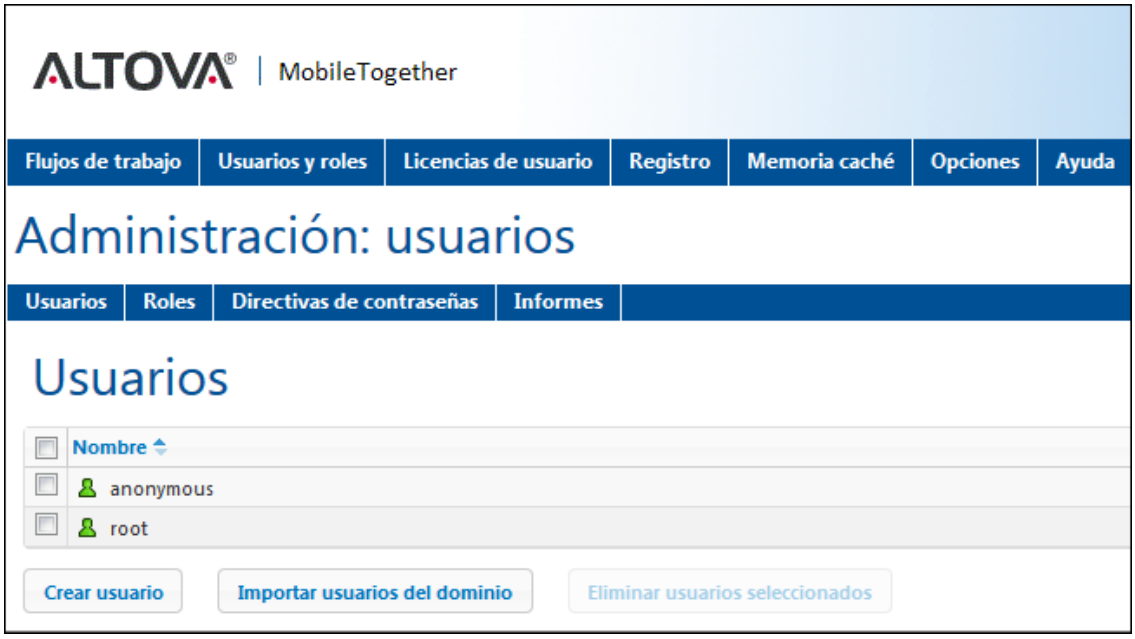
2. Para editar los derechos de acceso de un usuario/rol haga clic en su botón **Modificar** (*imagen anterior*). Para agregar permisos para un usuario/rol nuevo, haga clic en **Agregar permisos**. Estos dos botones abren el panel **Editar permisos**.



3. En el panel **Editar permisos** marque la casilla del usuario/rol que desea seleccionar en la tabla de la izquierda. Si está editando los permisos actuales, se heredarán los permisos de este usuario/rol. En cambio, si está añadiendo permisos nuevos, este usuario/rol se añadirá a la lista de usuarios/roles permitidos de este contenedor. En el cuadro combinado *Buscar en* puede seleccionar usuarios y roles que se definieron para MobileTogether Server o para todos los dominios habilitados (seleccione *MobileTogether Server* o *Windows* respectivamente). Los usuarios y roles de un dominio lo define el administrador del dominio y solamente estarán disponibles en este panel si se habilitó la opción *Inicio de sesión de Active Directory* en la pestaña **Opciones**.
4. Realice los cambios necesarios y haga clic en **Guardar cambios**. Recuerde que si selecciona la opción *Se hereda*, los permisos se heredarán del contenedor primario.

5.2 Usuarios y roles

La pestaña **Usuarios y roles** (*imagen siguiente*) está dividida a su vez en cuatro pestañas. En ellas podrá habilitar las cuentas de usuario que se deben administrar, configurar sus privilegios y consultar un resumen de las cuentas y los privilegios que tienen. Para más información consulte los apartados de esta sección.



▼ ¿Qué es un usuario?

Un usuario se define por medio de una combinación de nombre de usuario y contraseña. Los usuarios pueden acceder a MobileTogether Server de dos maneras diferentes:

- *por la interfaz web:* la interfaz web es la interfaz de administración de MobileTogether Server. Para acceder a ella es necesario indicar un nombre de usuario y una contraseña. Es decir, se accede al servidor como usuario.
- *por la interfaz del servicio*: la interfaz del servicio HTTP expone los servicios de MobileTogether Server a la aplicación MobileTogether Client en un dispositivo móvil. El usuario accede a la interfaz del servicio indicando un nombre de usuario y una contraseña. Los servicios expuestos suelen estar relacionados con el acceso a soluciones de MobileTogether y a sus datos.

Hay dos usuarios predeterminados:

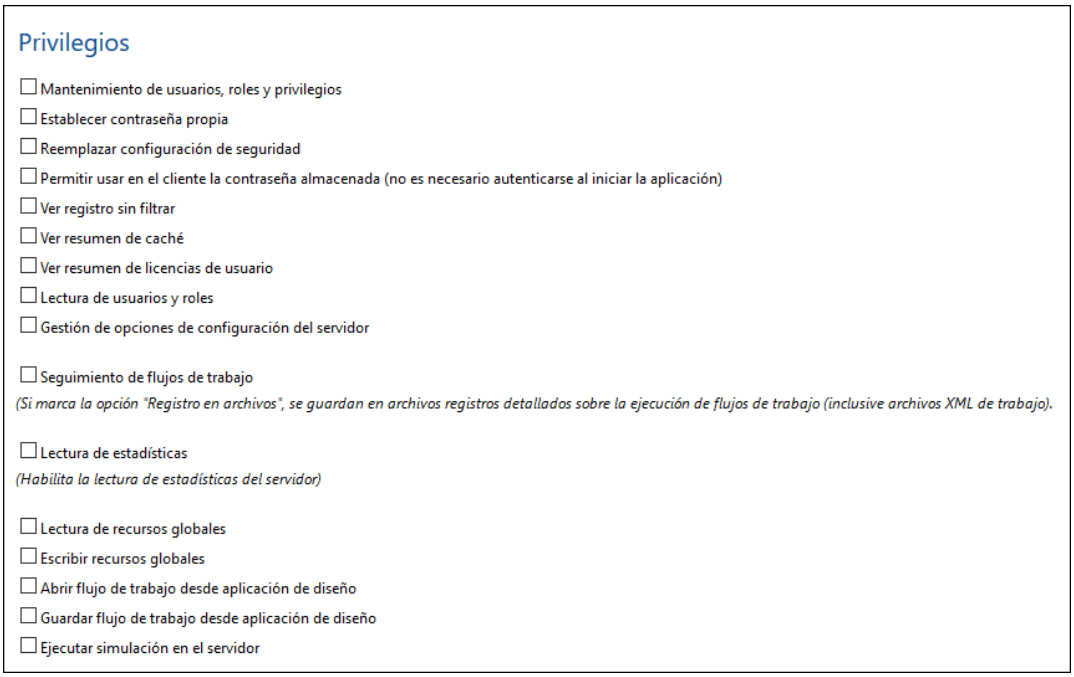
root	**root** es el usuario administrador inicial. Se trata del usuario con más poder en un principio, ya que dispone de todos los privilegios y tiene capacidad para agregar otros usuarios y configurar roles. Su

	combinación inicial de nombre de usuario y contraseña es: **root-root**. La contraseña puede cambiarse en todo momento.
anonymous	**anonymous** es una cuenta para usuarios anónimos que accedan a servicios expuestos a través de la interfaz del servicio HTTP. No se puede utilizar para acceder a la interfaz web y no dispone de contraseña inicial.

▼ ¿Qué es un privilegio?

Un privilegio es una actividad para cuya realización se dio permiso a un usuario. En MobileTogether Server hay un número fijo de privilegios y un usuario puede no tener asignado ningún privilegio o tener asignados todos los privilegios disponibles. Sin embargo, se recomienda asignar los privilegios a través de los roles y no asignar privilegios a los usuarios directamente. El usuario que asigne privilegios y roles a otros usuarios debe tener este privilegio. En un principio es el usuario **root** quien lo tiene.

En esta imagen puede ver todos los privilegios disponibles en MobileTogether Server.



La pestaña *Usuarios y roles | Informes | Informes de privilegios* ofrece una lista completa de privilegios. En esta lista también podrá comprobar a qué usuarios se concedió cada privilegio de la lista.

▼ ¿Qué es un rol?

Un rol define un conjunto de privilegios y se puede asignar tanto a otro rol como a un usuario. Los privilegios de un rol son automáticamente los privilegios del rol o usuario al que se asignara el rol. Un usuario puede tener tantos roles como se necesiten. Es decir, un

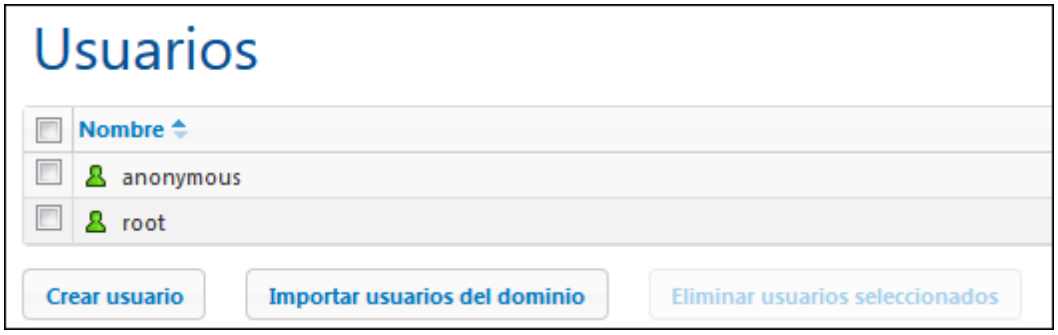
usuario tendrá todos los privilegios que se definieran en los roles que tenga asignados.

Estos son los roles predeterminados:

- **`all`** se asigna automáticamente a todos los usuarios, **incluido** el usuario **`anonymous`**.
- **`authenticated`** se asigna automáticamente a todos los usuarios, **excepto** al usuario **`anonymous`**. Es decir, a los usuarios con nombre y contraseña se les asigna el rol `authenticated`.
- **`workflow-designer`** se asigna a los usuarios que diseñan flujos de trabajo en MobileTogether Designer. Este rol permite al usuario abrir y guardar flujos de trabajo y a ejecutar simulaciones en el servidor.
- **`workflow-user`** se asigna a los usuarios que ejecutan el flujo de trabajo en un dispositivo móvil. Este rol permite al usuario acceder a la interfaz del servicio e iniciar la solución en el cliente sin necesidad de iniciar sesión en el servidor.
- **`admin`** tiene todos los permisos y está pensado para usuarios con la función de administrador.

5.2.1 Usuarios

La pestaña **Usuarios y roles | Usuarios** enumera todos los usuarios definidos en el sistema. Aquí podrá crear usuarios nuevos, acceder a sus propiedades y eliminar usuarios.



▼ ¿Qué es un usuario?

Un usuario se define por medio de una combinación de nombre de usuario y contraseña. Los usuarios pueden acceder a MobileTogether Server de dos maneras diferentes:

- *por la interfaz web:* la interfaz web es la interfaz de administración de MobileTogether Server. Para acceder a ella es necesario indicar un nombre de usuario y una contraseña. Es decir, se accede al servidor como usuario.
- *por la interfaz del servicio*: la interfaz del servicio HTTP expone los servicios de MobileTogether Server a la aplicación MobileTogether Client en un dispositivo móvil. El usuario accede a la interfaz del servicio indicando un nombre de usuario y una contraseña. Los servicios expuestos suelen estar relacionados con el acceso a soluciones de MobileTogether y a sus datos.

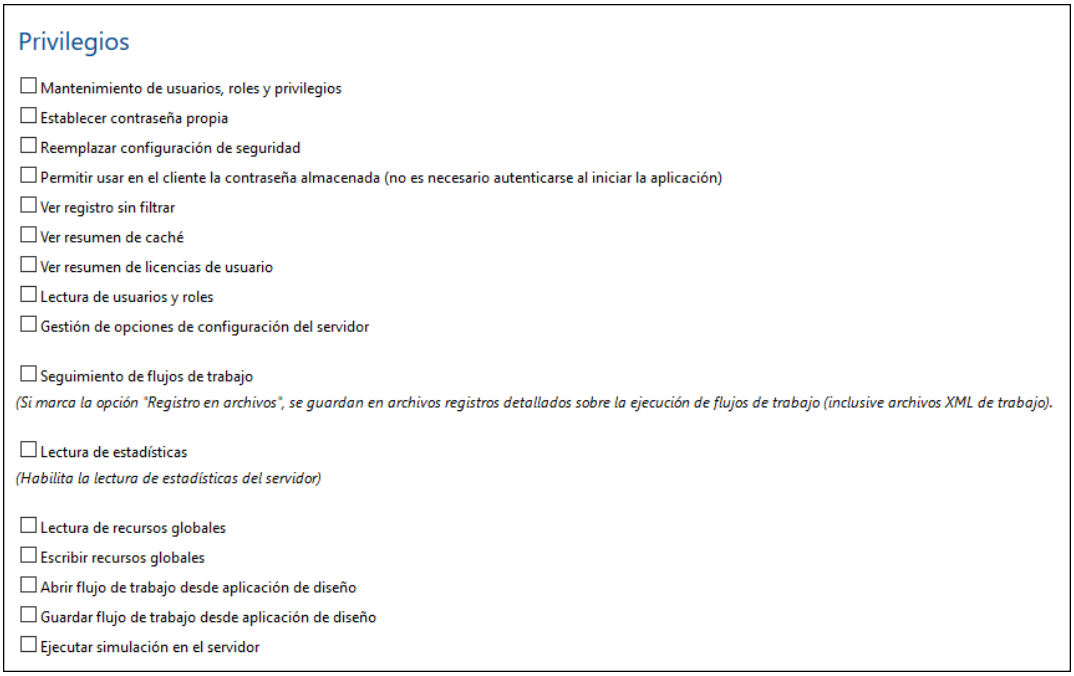
Hay dos usuarios predeterminados:

root	**root** es el usuario administrador inicial. Se trata del usuario con más poder en un principio, ya que dispone de todos los privilegios y tiene capacidad para agregar otros usuarios y configurar roles. Su combinación inicial de nombre de usuario y contraseña es: **root-root**. La contraseña puede cambiarse en todo momento.
anonymous	**anonymous** es una cuenta para usuarios anónimos que accedan a servicios expuestos a través de la interfaz del servicio HTTP. No se puede utilizar para acceder a la interfaz web y no dispone de contraseña inicial.

▼ ¿Qué es un privilegio?

Un privilegio es una actividad para cuya realización se dio permiso a un usuario. En MobileTogether Server hay un número fijo de privilegios y un usuario puede no tener asignado ningún privilegio o tener asignados todos los privilegios disponibles. Sin embargo, se recomienda asignar los privilegios a través de los roles y no asignar privilegios a los usuarios directamente. El usuario que asigne privilegios y roles a otros usuarios debe tener este privilegio. En un principio es el usuario **root** quien lo tiene.

En esta imagen puede ver todos los privilegios disponibles en MobileTogether Server.



La pestaña *Usuarios y roles | Informes | Informes de privilegios* ofrece una lista completa de privilegios. En esta lista también podrá comprobar a qué usuarios se concedió cada privilegio de la lista.

▼ ¿Qué es un rol?

Un rol define un conjunto de privilegios y se puede asignar tanto a otro rol como a un usuario. Los privilegios de un rol son automáticamente los privilegios del rol o usuario al que se asignara el rol. Un usuario puede tener tantos roles como se necesiten. Es decir, un usuario tendrá todos los privilegios que se definieran en los roles que tenga asignados.

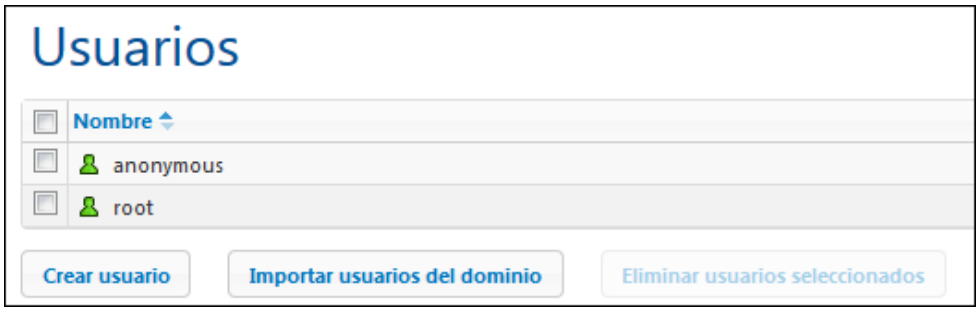
Estos son los roles predeterminados:

- **`all`** se asigna automáticamente a todos los usuarios, **incluido** el usuario **`anonymous`**.
- **`authenticated`** se asigna automáticamente a todos los usuarios, **excepto** al usuario **`anonymous`**. Es decir, a los usuarios con nombre y contraseña se les asigna el rol `authenticated`.
- **`workflow-designer`** se asigna a los usuarios que diseñan flujos de trabajo en MobileTogether Designer. Este rol permite al usuario abrir y guardar flujos de trabajo y a ejecutar simulaciones en el servidor.
- **`workflow-user`** se asigna a los usuarios que ejecutan el flujo de trabajo en un dispositivo móvil. Este rol permite al usuario acceder a la interfaz del servicio e iniciar la solución en el cliente sin necesidad de iniciar sesión en el servidor.
- **`admin`** tiene todos los permisos y está pensado para usuarios con la función de administrador.

Crear usuarios nuevos

Los usuarios que pueden crear usuarios nuevos son el usuario `root` y los usuarios que tengan el privilegio *Mantenimiento de usuarios, roles y privilegios*. Estas son las instrucciones para crear usuarios nuevos:

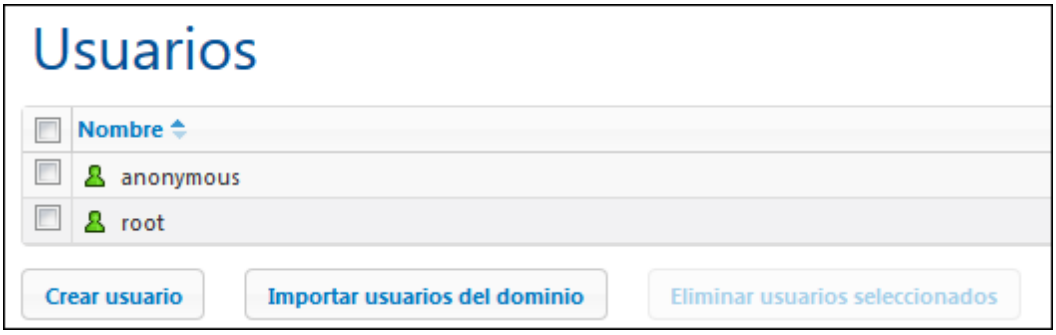
1. En la pestaña **Usuarios y roles | Usuarios** haga clic en el botón **Crear usuario** (*imagen siguiente*). Esto abre la pantalla **Crear usuario**.



2. En la pantalla **Crear usuario** escriba el nombre de usuario y la contraseña.
3. Para asignar privilegios al usuario puede seleccionar los privilegios directamente (marcando sus casillas) o asignar roles al usuario (*ver apartado siguiente*). El usuario tendrá los privilegios que se le asignen directamente más los que herede de todos los roles que tenga asignados. Recomendamos usar roles para asignar privilegios a los usuarios (*ver apartado siguiente*).
4. Seleccione una de las directivas de contraseñas definidas.
5. Para terminar haga clic en **Guardar** y el usuario aparecerá en la lista de usuarios. En adelante podrá editar sus propiedades con solo hacer clic en su nombre.

Importar usuarios del dominio

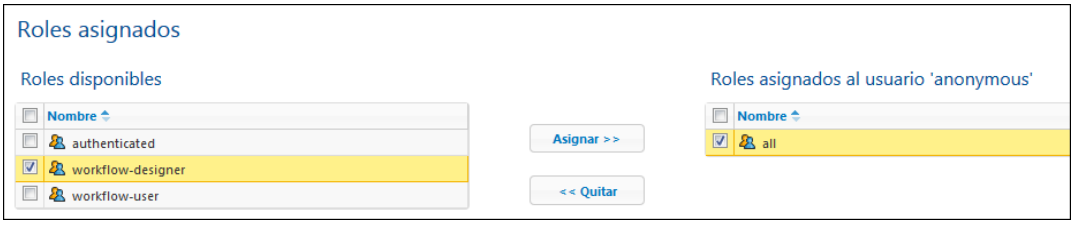
Si se habilitó la opción de inicio de sesión con Active Directory para un dominio concreto pero no se importaron los usuarios automáticamente, podrá importar los usuarios del dominio uno a uno desde esta pestaña. Esto se hace con el botón **Importar usuarios del dominio** (*imagen siguiente*). Este botón abre el cuadro de diálogo "Importar usuarios del dominio", donde puede buscar los usuarios que desea importar.



Una vez importado el usuario, podrá asignarle roles siguiendo el método estándar. El usuario nuevo podrá iniciar sesión en MobileTogether Server con el nombre de usuario y la contraseña de su dominio.

Asignar roles a un usuario

Los roles se asignan a los usuarios desde su página de propiedades. Para abrir esta página haga clic en el nombre del usuario en la pestaña **Usuarios y roles | Usuarios**. Al final de la página de propiedades encontrará el panel *Roles asignados* (*imagen siguiente*).

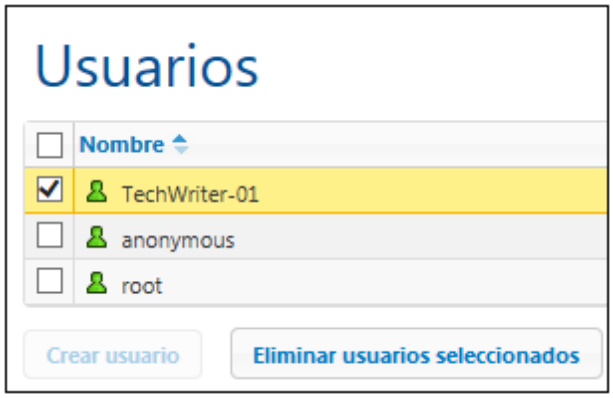


En la tabla de la izquierda aparecen todos los roles disponibles. En la tabla de la derecha aparecen todos los roles asignados al usuario seleccionado. Seleccione un rol (en la tabla de la izquierda) y haga clic en **Asignar**. Para quitar un rol asignado, selecciónelo en la tabla de la derecha y haga clic en **Quitar**.

Si desea ver una lista de privilegios del usuario haga clic en **Usuarios y roles | Informes | Informe de privilegios por usuario**.

Eliminar usuarios

Los usuarios que pueden eliminar usuarios son el usuario `root` y los usuarios que tengan el privilegio *Mantenimiento de usuarios, roles y privilegios.* Para eliminar un usuario, selecciónelo en la pestaña **Usuarios y roles | Usuarios** y haga clic en el botón **Eliminar usuarios seleccionados**.

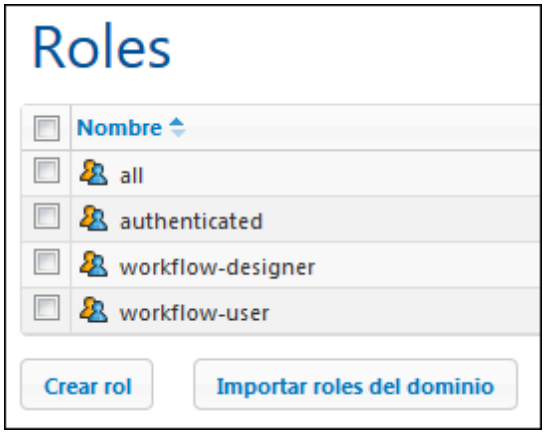


5.2.2 Roles

Un rol define un conjunto de privilegios y se puede asignar tanto a otro rol como a un usuario. Los privilegios de un rol son automáticamente los privilegios del rol o usuario al que se asignara el rol. Un usuario puede tener tantos roles como se necesiten. Es decir, un usuario tendrá todos los privilegios que se definieran en los roles que tenga asignados.

Estos son los roles predeterminados:

- **`all`** se asigna automáticamente a todos los usuarios, **incluido** el usuario **`anonymous`**.
- **`authenticated`** se asigna automáticamente a todos los usuarios, **`excepto`** al usuario **`anonymous`**. Es decir, a los usuarios con nombre y contraseña se les asigna el rol `authenticated`.
- **`workflow-designer`** se asigna a los usuarios que diseñan flujos de trabajo en MobileTogether Designer. Este rol permite al usuario abrir y guardar flujos de trabajo y a ejecutar simulaciones en el servidor.
- **`workflow-user`** se asigna a los usuarios que ejecutan el flujo de trabajo en un dispositivo móvil. Este rol permite al usuario acceder a la interfaz del servicio e iniciar la solución en el cliente sin necesidad de iniciar sesión en el servidor.
- **`admin`** tiene todos los permisos y está pensado para usuarios con la función de administrador.

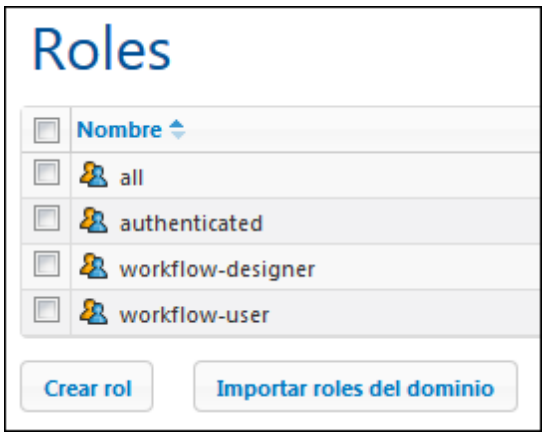


En la pestaña **Usuarios y roles | Roles** puede crear roles nuevos, editar sus propiedades y asignar roles a usuarios e incluso a otros roles. Haga clic en el nombre del rol para editar sus propiedades, seleccionar sus privilegios y asignar el rol a un usuario y a otros roles.

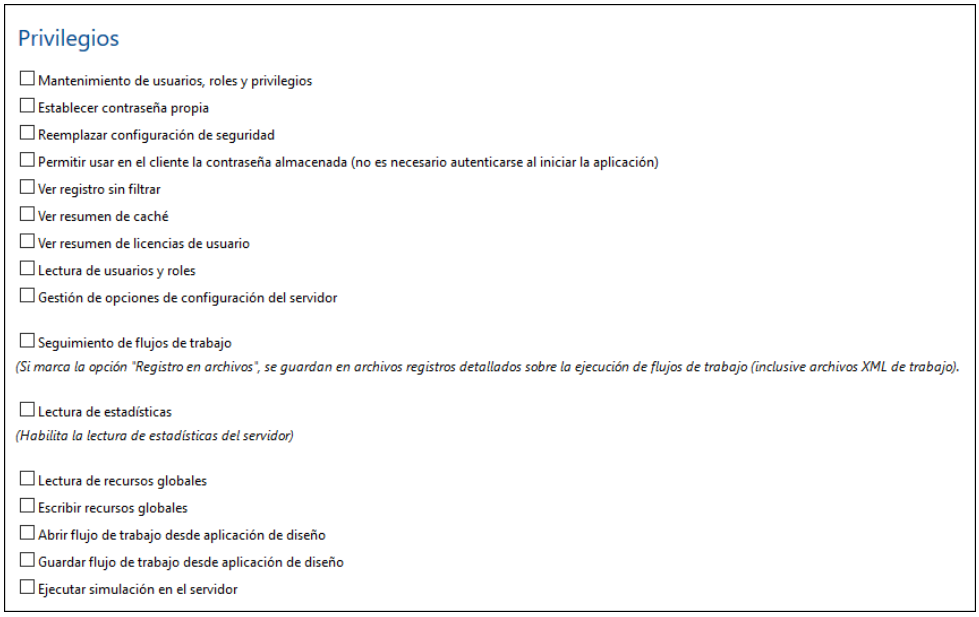
▼ Crear roles y definir sus privilegios

Los usuarios que pueden crear roles nuevos son el usuario `root` y todos los usuarios que tengan el privilegio *Mantenimiento de usuarios, roles y privilegios*. Siga estas instrucciones para crear un rol nuevo:

1. En la pestaña **Usuarios y roles | Roles** haga clic en **Crear rol** (*imagen siguiente*).



2. Ahora se abre la página **Crear rol**. El primer paso es escribir el nombre del rol.
3. Después debe definir sus privilegios marcando las casillas correspondientes.



4. Para terminar haga clic en **Guardar**.

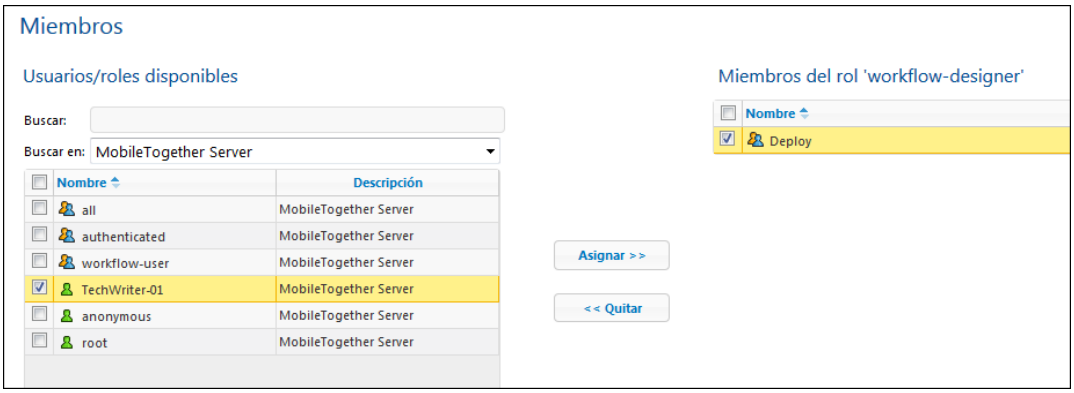
Después de guardar el rol podrá asignarle miembros en el panel *Miembros* situado al final de la página (*ver más abajo*). Los miembros de un rol pueden ser usuarios o roles. En adelante podrá editar las propiedades del rol con solo hacer clic en su nombre en la pestaña **Usuarios y roles | Roles**.

Si desea ver una lista de privilegios del rol haga clic en **Usuarios y roles | Informes | Informe de privilegios por usuario**.

Asignar miembros (usuarios o roles) a un rol

Los roles pueden tener miembros, que a su vez pueden ser otros roles o usuarios. Los miembros del rol heredan sus privilegios del rol al que pertenecen.

Para asignar un miembro a un rol, utilice los controles del panel *Miembros* situado al final de la página de propiedades del rol (*imagen siguiente*).



- En la tabla de la izquierda aparecen todos los usuarios y roles disponibles.
- En el cuadro combinado *Buscar en* puede seleccionar usuarios y roles que se definieron para MobileTogether Server o para todos los dominios habilitados (seleccione *MobileTogether Server* o *Windows* respectivamente). Los usuarios y roles de un dominio los define el administrador del dominio y solamente estarán disponibles si se habilitó la opción *Inicio de sesión de Active Directory* en la pestaña **Opciones**.
- En el campo *Buscar:* puede escribir el nombre del usuario o rol que desea buscar
- En la tabla de la derecha aparecen todos los usuarios y roles que son miembros del rol seleccionado.
- Seleccione el usuario/rol en la tabla de la izquierda y asígneselo al rol haciendo clic en el botón **Asignar**.
- Para quitar un usuario/rol asignado al rol, selecciónelo en la tabla de la derecha y haga clic en el botón **Quitar**.

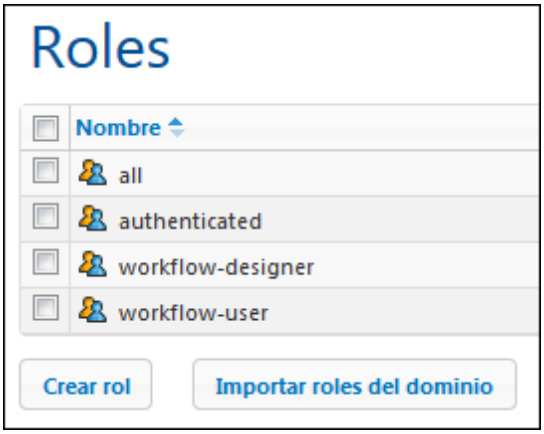
En la imagen anterior, por ejemplo, puede ver el panel *Miembros* del rol `workflow-designer`. Este rol solamente tiene un miembro: el rol `Deploy`, que heredará todos los privilegios del rol `workflow-designer`.

Recuerde que un usuario o rol puede tener asignados varios conjuntos de privilegios. Si añade un usuario o rol como miembro de varios roles diferentes, heredará los privilegios de todos los roles a los que pertenezca.

Si desea ver una lista de privilegios de un usuario o rol haga clic en **Usuarios y roles | Informes | Informe de privilegios por usuario**.

Importar roles del dominio

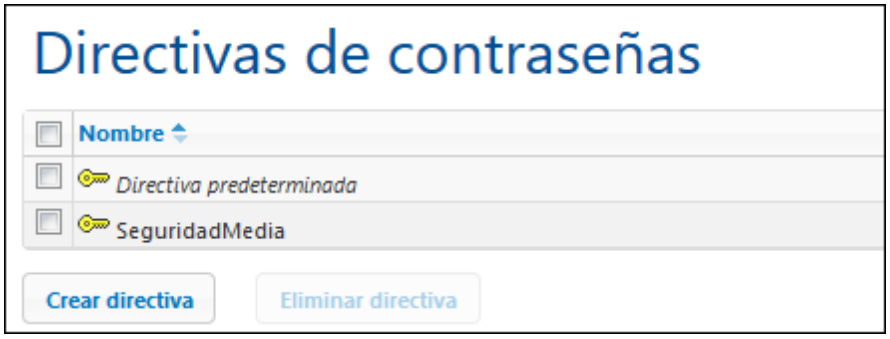
Si se habilitó la opción *Inicio de sesión de Active Directory* en la pestaña **Opciones** podrá importar los roles del dominio habilitado. Haga clic en el botón **Importar roles del dominio** (*imagen siguiente*) para abrir el cuadro de diálogo "Importar roles del dominio". Busque el rol que desea importar, selecciónelo y haga clic en **Importar selección**.



Después de importar el rol podrá asignarle privilegios igual que con cualquier otro rol del sistema.

5.2.3 Directivas de contraseñas

Una directiva de contraseñas define lo seguras que son las contraseñas que utilizan dicha directiva. Puede definir directivas de contraseñas propias y aplicar diferentes directivas a diferentes usuarios. La pestaña **Usuarios y roles | Directivas de contraseñas** enumera todas las directivas de contraseñas disponibles. Aquí podrá crear y eliminar directivas y asignarlas a los usuarios.

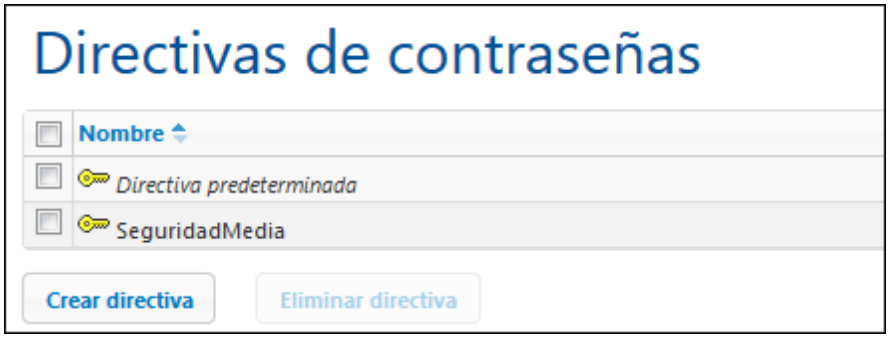


Nota: cada usuario nuevo recibe por defecto la **directiva de contraseñas predeterminada**, que no define ningún tipo de restricción y no permite cambios. Si prefiere que los usuarios tengan contraseñas más seguras que las definidas por la directiva predeterminada, cree una directiva más segura y asígnesela a los usuarios correspondientes.

▼ Crear una directiva de contraseñas

Los usuarios que pueden crear directivas de contraseñas nuevas son el usuario `root` y los usuarios que tengan el privilegio *Mantenimiento de usuarios, roles y privilegios*. Estas son las instrucciones para crear una directiva de contraseñas nueva:

1. En la pestaña **Usuarios y roles | Directivas de contraseñas** haga clic en el botón **Crear directiva** (*imagen siguiente*). Esto abre la pantalla **Crear directiva de contraseñas**.



2. El siguiente paso es indicar el nombre de la directiva.

3. Para definir las restricciones de las contraseñas, haga clic en el icono **+** situado junto a cada restricción (*Longitud total*, *Letras*, *Dígitos*) y escriba el valor que desea aplicar.

4. Para terminar haga clic en **Guardar**.

Una vez guardada, podrá asignar usuarios a la directiva desde el panel *Miembros* situado al final de la página (*ver más abajo*). En adelante, bastará con hacer clic en el nombre de una directiva en la pestaña **Usuarios y roles | Directivas de contraseñas** para editar sus propiedades.

▼ Asignar miembros (usuarios) a una directiva de contraseñas

Para aplicar una directiva de contraseñas a un usuario deberá el usuario como miembro de la directiva desde el panel *Miembros* (situado al final de la página de propiedades de la directiva).

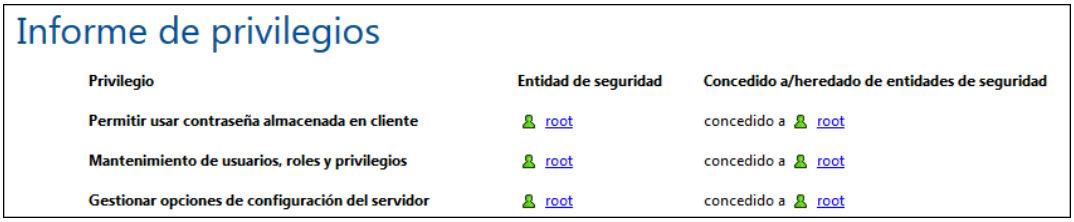
La tabla de la izquierda contiene todos los usuarios disponibles. La tabla de la derecha contiene todos los miembros que son miembros de la directiva. Seleccione el usuario que quiere asignar como miembro de la directiva (en la tabla izquierda) y haga clic en el botón **Asignar**. Para quitar un usuario ya asignado, selecciónelo en la tabla de la derecha y haga clic en **Quitar**. Por ejemplo, en la imagen anterior puede ver que la directiva `SeguridadMedia` tiene asignado un solo miembro: el usuario `TechWriter-01`.

5.2.4 Informes

La pestaña **Usuarios y roles | Informes** ofrece enlaces a informes de privilegios. Se trata de resúmenes prácticos con información sobre los privilegios que utiliza cada usuario o rol.

- Informe de privilegios

  El informe de privilegios enumera cada uno de los privilegios del sistema junto a los usuarios y roles que disponen de dicho privilegio. También indica de quién se hereda el privilegio en cada caso.

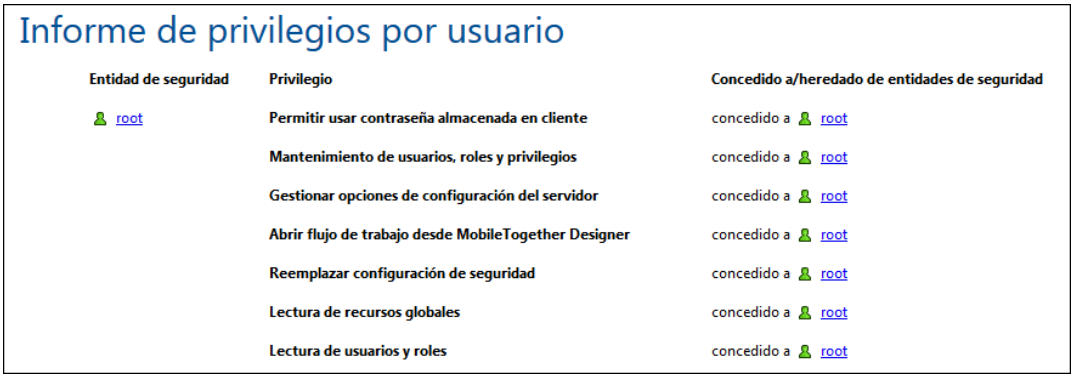


Informe de privilegios

Privilegio	Entidad de seguridad	Concedido a/heredado de entidades de seguridad
Permitir usar contraseña almacenada en cliente	root	concedido a root
Mantenimiento de usuarios, roles y privilegios	root	concedido a root
Gestionar opciones de configuración del servidor	root	concedido a root

- Informe de privilegios por usuario

  El informe de privilegios por usuario enumera cada uno de los usuarios/roles y un resumen de sus privilegios. También indica de quién hereda privilegios cada usuario/rol.



Informe de privilegios por usuario

Entidad de seguridad	Privilegio	Concedido a/heredado de entidades de seguridad
root	Permitir usar contraseña almacenada en cliente	concedido a root
	Mantenimiento de usuarios, roles y privilegios	concedido a root
	Gestionar opciones de configuración del servidor	concedido a root
	Abrir flujo de trabajo desde MobileTogether Designer	concedido a root
	Reemplazar configuración de seguridad	concedido a root
	Lectura de recursos globales	concedido a root
	Lectura de usuarios y roles	concedido a root

5.3 Licencias de usuario

En la pestaña **Licencias de usuario** puede obtener información sobre las licencias asignadas a los dispositivos que están conectados al servidor (*imagen siguiente*). Desde aquí podrá activar y desactivar licencias.

- Las licencias de MobileTogether Server permiten a un número determinado de dispositivos comunicarse con el servidor MobileTogether Server en un momento dado. Este número aparece en el campo *Licencias utilizadas*. Por ejemplo, en el ejemplo de la imagen el servidor tiene licencias para comunicarse con 8 dispositivos. Hay cinco dispositivos conectados y todos tienen asignada una licencia (la casilla *Activa* está marcada). Por tanto, el campo *Licencias utilizadas:* dice *5 (de 8)*.

- Cuando un dispositivo cliente se conecta al servidor, se le asigna automáticamente una licencia si el cuadro combinado *Modo de asignación de licencias* tiene el valor `Automático` (*ver imagen*). Si este cuadro combinado tuviera el valor `Manual` y un dispositivo nuevo se conectase al servidor, éste aparecerá en la lista de dispositivos conectados pero solamente tendrá asignada una licencia si el administrador marca la casilla *Activa* y hace clic en **Guardar**.

- Cuando se alcance el límite de licencias de usuario, no será posible asignar licencias a ningún dispositivo más. Para asignar licencias a más dispositivos, primero deberá desactivar la asignación de licencia de algún dispositivo (desactivando su licencia). El administrador puede activar y desactivar las licencias en cualquier momento para poder asignar licencias a otros dispositivos sin superar el límite de licencias.

Campos y columnas

A continuación describimos los campos y columnas de la pestaña **Licencias de usuario**.

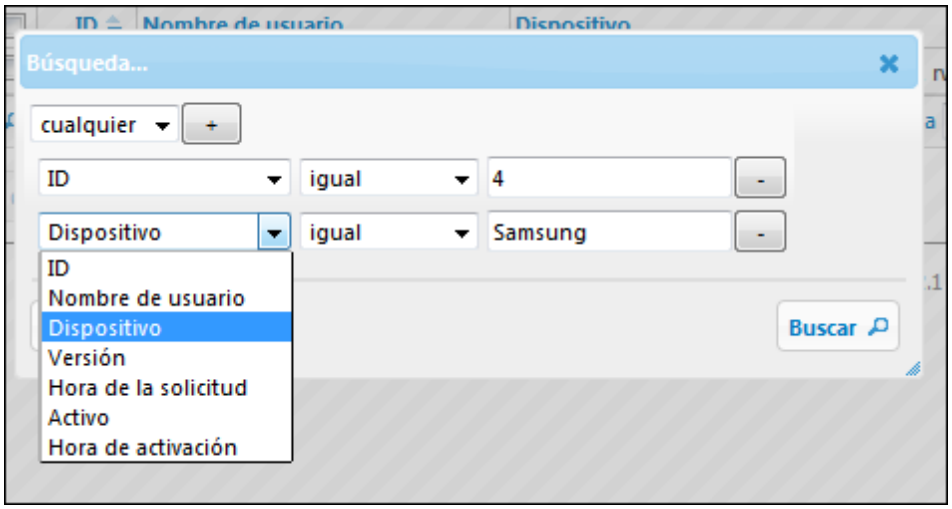
- *Modo de asignación de licencias:* `Automático` activa automáticamente una licencia para

los dispositivos nuevos que se conecten, siempre y cuando haya licencias libres. `Manual` requiere que el administrador active la licencia para el dispositivo y guarde los cambios para que surtan efecto.

- *ID:* número interno asignado al dispositivo con licencia.
- *Nombre de usuario:* nombre de usuario con el que el dispositivo cliente realizó la conexión e inició sesión en el servidor. El nombre de usuario determina qué privilegios se extienden al dispositivo cliente.
- *IP del cliente:* dirección IP del dispositivo cliente.
- *Dispositivo:* dispositivo cliente o explorador que solicitó la licencia.
- *Versión:* versión de la aplicación cliente MobileTogether Client del dispositivo móvil. Conocer este número de versión es importante para las tareas de depuración y de corrección de errores.
- *Activa:* esta casilla sirve para activar y desactivar licencias. Si cambia el estado de esta casilla, haga clic en **Guardar**.
- *Hora de solicitud, Hora de activación:* hora a la que se solicitó y se activó la licencia.

Búsquedas

Haga clic en el botón **Buscar** para abrir el cuadro de diálogo "Búsqueda" (*imagen siguiente*) y utilice los filtros disponibles para buscar lo que necesita.



- El cuadro combinado *todo/cualquier* indica si se debe cumplir cualquier criterio de búsqueda o todos los criterios definidos.
- El icono **+** situado junto al cuadro combinado *todo/cualquier* sirve para añadir criterios a la búsqueda.
- Cada criterio de búsqueda tiene tres partes: (i) un campo de búsqueda (p. ej. `Dispositivo`), (ii) una definición de relación (p. ej. `igual a`) y (iii) un valor (p. ej. `Samsung`).
- El valor dado (p. ej. `Samsung`) debe coincidir exactamente con el valor del campo de búsqueda pertinente (p. ej. `Dispositivo`).
- Si deja vacío el valor, se buscará una cadena vacía en el campo de búsqueda pertinente (p. ej. `Dispositivo`).
- Con el icono **-** puede borrar el criterio de búsqueda entero (p. ej. `Dispositivo es igual a Samsung`).

- Haga clic en **Buscar** para iniciar la búsqueda.
- Haga clic en **Restaurar** para ver todas las licencias de usuario otra vez.

5.4 Registro

En la pestaña **Registro** podrá consultar todas las acciones registradas en función del filtro seleccionado en la parte superior de la página. En las acciones registradas también se encuentran los cambios en las opciones del servidor (quién y dónde). Si desea ver todas las acciones registradas (no solo las advertencias y los errores), abra la pestaña **Opciones** y elija la opción **Información** en el campo *Gravedad mínima.* Las columnas del registro de cada diseño muestran el nombre del usuario, el dispositivo cliente (identificado por medio de un ID, cuyos datos se pueden ver en la pestaña **Licencias de usuario**), el número de versión de la aplicación MobileTogether Client que está en el dispositivo, la versión de MobileTogether Designer con la que se creó el diseño y la gravedad del mensaje (información, advertencia o error).

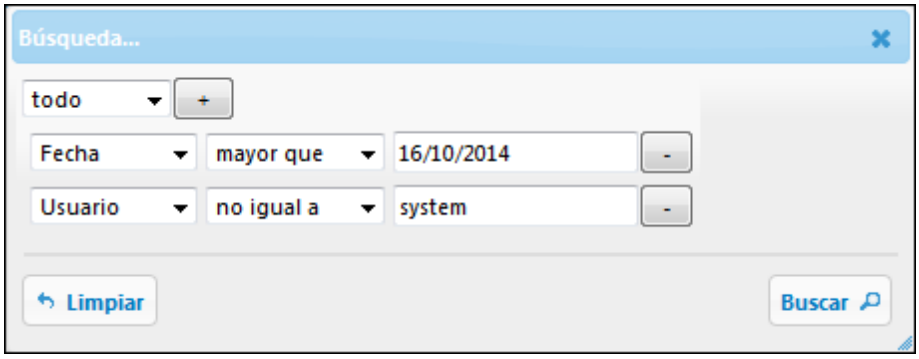
La vista del registro se puede filtrar:

- *Según la fecha:* puede consultar un período de tiempo concreto o un intervalo.
- *Según el nivel de gravedad:* los errores son el nivel de gravedad más alto (si elige esta opción, el registro muestra los errores solamente), seguidos de las advertencias (con esta opción se muestran las advertencias y los errores) y, por último, información (esta opción muestra errores, advertencias e información).
- *Según un criterio de búsqueda:* haga clic en el botón **Buscar** situado al principio y al final de la tabla del registro para abrir el cuadro de diálogo "Búsqueda" (*ver más abajo*). Para quitar el filtro definido por el criterio de búsqueda, haga clic en el icono **Volver a cargar** situado junto al botón **Buscar**.

Para eliminar registros basta con hacer clic en el botón **Eliminar todos** situado al principio de la página o definir un período de tiempo y después hacer clic en **Eliminar**.

Buscar mensajes del registro

Haga clic en el botón **Buscar** situado al principio y al final de la tabla del registro para abrir el cuadro de diálogo "Búsqueda" (*imagen siguiente*).



Por cada criterio de búsqueda seleccione un campo (p. ej. *Fecha* o *Usuario*), un operador (p. ej. *contiene* o *igual a*) y el valor que se debe buscar. Para agregar otro criterio de búsqueda haga clic en el botón **+**. Para eliminar un criterio de búsqueda haga clic en el botón **-**. El selector `todo` del primer cuadro combinado indica que deben cumplirse todos los criterios de búsqueda. El selector `cualquiera` especifica que pueden devolverse resultados que cumplan con cualquiera de los criterios de búsqueda definidos. Para iniciar la búsqueda haga clic en **Buscar**. Para eliminar el filtro de búsqueda haga clic en **Limpiar**.

5.5 Memoria caché

La pestaña **Memoria caché** ofrece información detallada sobre las memorias caché disponibles en el servidor. Una memoria caché es un archivo de datos que se genera a partir de una fuente de datos de un diseño en un momento dado. En la interfaz web de MobileTogether Server podrá consultar información sobre las memorias caché del servidor, activarlas, desactivarlas y eliminarlas.

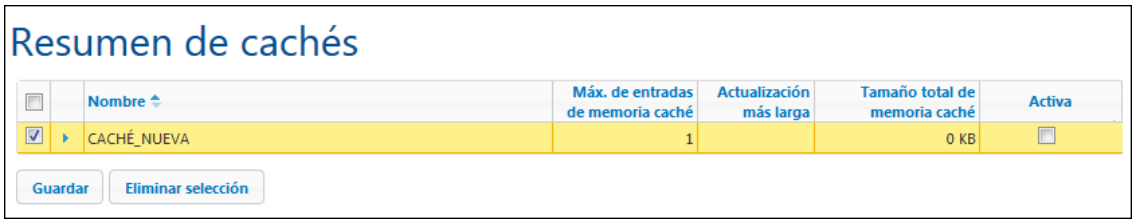
Crear memorias caché

Desde MobileTogether Designer puede definir memorias caché nuevas para las fuentes de datos: haga clic con el botón derecho en una fuente de datos del panel "Fuentes de página" y seleccione **Configurar memoria caché** al final del menú contextual. Los dos motivos para crear memorias caché son: (i) si una fuente de datos de la página genera informes con mucha lentitud (p. ej. si se trata de una base de datos de gran tamaño) o (ii) si una fuente de datos no se modifica con frecuencia. En casos así, la solución se ejecutará más rápido si los datos se toman de las memorias caché del servidor. Cuando cree la memoria caché también podrá especificar con qué frecuencia se actualiza. Así podrá asegurarse de que la memoria caché siempre está actualizada. Una vez definida en MobileTogether Designer, la memoria caché podrá ser utilizada por las fuentes de datos de otros diseños (siempre y cuando la estructura de datos subyacente sea compatible).

Si define una fuente de datos con una memoria caché, los datos almacenados en caché se utilizarán cuando se ejecute la solución. Las memorias caché se pueden usar tan pronto como se implemente la solución en el servidor.

Información y acciones disponibles

En la pestaña Memoria caché se enumeran todas las memorias caché disponibles en el servidor. Desde aquí podrá activar, desactivar y eliminar memorias.



- *Nombre:* el nombre se asigna a la memoria caché cuando ésta se crea en MobileTogether Designer y no se puede cambiar en MobileTogether Server. Puede usar la misma memoria caché en varios diseños si la estructura de datos es compatible. Para asignar la misma memoria caché a varios diseños debe utilizar MobileTogether Designer. Consulte el manual del usuario de MobileTogether Designer para obtener más información.

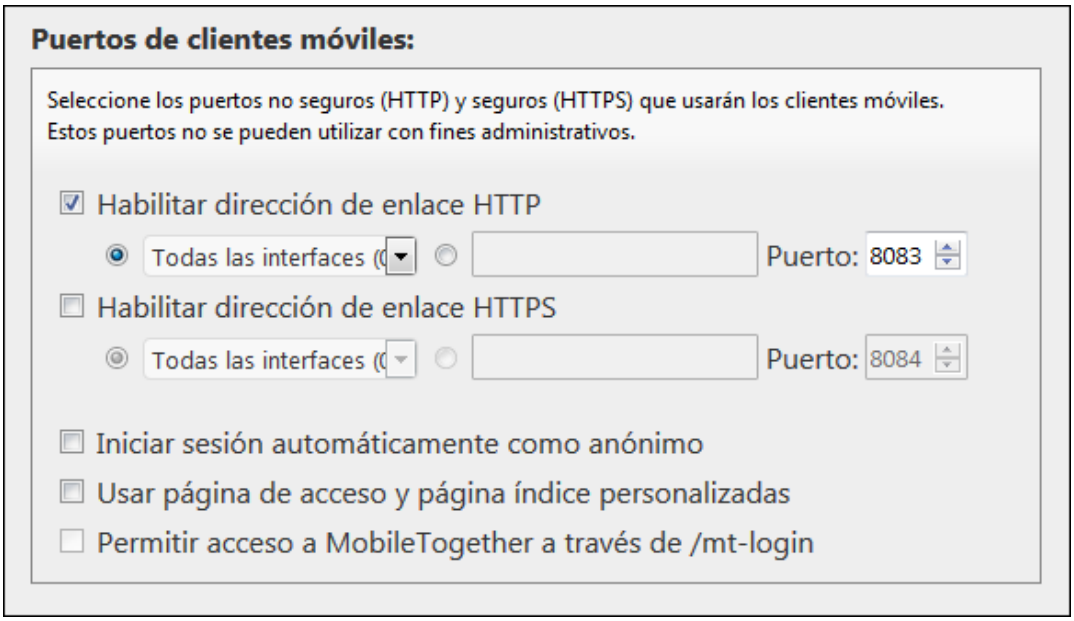
- *Máx de entradas de memoria caché:* la memoria caché se puede crear usando un conjunto de parámetros. Cada conjunto de parámetros genera una entrada de memoria caché y, si se especifican varios conjuntos de parámetros, se crearán varias entradas de caché. A la hora de definir la memoria caché, puede indicar el número máximo de entradas de caché para que el límite esté basado en la cantidad de espacio de servidor utilizado para las memorias caché de una fuente de datos concreta. Este número especifica cuántas entradas de caché se almacenarán antes de que se purgue la primera entrada y se anexe la entrada más reciente.
- *Tamaño total de memoria caché:* se trata del tamaño total (para todas las entradas de caché) asignado a la memoria caché en el disco duro (o cualquier otro medio). El tamaño de la memoria caché se asigna automáticamente.
- *Actualización más larga:* cada memoria caché se puede actualizar varias veces. Esta columna indica cuánto duró la actualización más larga.
- *Activa:* esta casilla sirve para activar o desactivar la memoria caché en el servidor. Si una memoria caché está desactivada, sus metadatos (propiedades) se mantienen en el servidor pero la memoria caché se vacía y no está disponible. Haga clic en **Guardar** para confirmar el cambio de estado de la memoria caché.
- Para eliminar una memoria caché del servidor, selecciónela y haga clic en el botón **Eliminar selección**. Si la memoria estaba definida para actualizarse periódicamente, en la próxima sesión de actualización se generará una memoria caché nueva.

5.6 Opciones

La pestaña **Opciones** incluye dos paneles de opciones de configuración: (i) el panel *Configuración general* y (ii) el panel *LicenseServer*. El panel *Configuración general* contiene varias secciones con diferentes opciones de configuración. Cuando cambie la configuración en este panel, asegúrese de hacer clic en el botón **Guardar** situado al final del panel para que el cambio surta efecto.

▼ Puertos de clientes móviles

Estos son los puertos que utilizarán los dispositivos móviles para conectarse al servidor. El puerto HTTP es el puerto no seguro, mientras que el puerto HTTPS es el puerto seguro. Para usar HTTPS deberá configurar antes el cifrado SSL. Puede especificar si el servidor usará una dirección IP concreta o todas las interfaces y direcciones IP. Si se debe usar una sola dirección IP, introdúzcala en el campo del segundo botón de opción.



Iniciar sesión automáticamente como anónimo
Si marca esta opción, los clientes iniciarán sesión automáticamente con la cuenta anonymous. La página de acceso se omite y aparece directamente la primera página del servidor. La primera página es la página estándar donde se puede ver la carpeta raíz o una página personalizada y definida previamente (*ver siguiente punto*). Si **no marca** esta opción, el cliente deberá iniciar sesión utilizando las credenciales adecuadas desde la página de acceso predeterminada. Si marca esta opción, recuerde que debe asignar los privilegios correspondientes para anonymous.

Usar página de acceso y página índice personalizadas
Marque esta opción si desea utilizar una página de acceso y una página índice personalizadas. Es decir, con esta opción puede diseñar un punto de entrada particular para los clientes. Estos son los pasos que debe seguir para conseguirlo:

1. Cree las dos páginas como páginas HTML y llámelas **login.html** y **index.html** respectivamente.
2. Guarde estos dos archivos en la carpeta **index** situada en la carpeta de datos de la aplicación MobileTogether Server (*ver tabla más abajo*). Si tiene otros archivos, como archivos de imágenes y archivos CSS, guárdelos en una subcarpeta de la carpeta **index** (por ejemplo, en una carpeta llamada **static**).

Linux	`/var/opt/Altova/MobileTogetherServer`
Mac	`/var/Altova/MobileTogetherServer`
Windows 7, 8, 10	`C:\ProgramData\Altova\MobileTogetherServer`

A continuación puede ver fragmentos de código de una página de acceso y de una página de índice. Son páginas muy básicas pero si lo desea puede modificar el código a su gusto.

login.html

```
<html>
  <header>
    <title>Acceso personalizado</title>
  </header>
  <head>
    <meta http-equiv="Cache-Control" content="no-store" />
  </head>
  <body>
    <div>
      <h1>Iniciar sesión</h1>
      <p>Página básica y personalizada para acceso de clientes a
MobileTogether Server. Modifique esta página a su gusto y utilice
la subcarpeta Static para guardar hojas de estilos CSS, imágenes,
etc.</p>
      <form method="post" action="/do_login" name="loginform">
        <table>
          <tbody>
            <!-- Usuario que debe iniciar sesión -->
            <tr><td>Usuario:</td></tr>
            <tr><td><input type="text" name="username" size="30"></
td></tr>
            <!-- Contraseña del usuario -->
            <tr><td>Contraseña:</td></tr>
            <tr><td><input type="password" name="password"
size="30"></td></tr>
            <!-- Datos de dominio Active Directory -->
            <tr><td> </td></tr>
            <tr><td>Inicio de sesión de Active Directory:</td></tr>

            <tr>Sufijo del dominio: <td><input
type="providernamesuffix" name="providernamesuffix" value=""></
td></tr>
            <tr>Prefijo del dominio: <td><input
type="providernameprefix" name="providernameprefix" value=""></
td></tr>
```

```
            <!-- Botón Iniciar sesión -->
            <tr><td><input type="submit" value="Iniciar sesión"></
td></tr>
          </tbody>
        </table>
        <!-- Página a la que se conduce después de iniciar sesión.
-->
        <input type="hidden" name="from_page" value="/index"></
input><br>
      </form>
    </div>
  </body>
</html>
```

index.html

```
<html>
  <header>
    <title>Página índice personalizada</title>
  </header>
  <head>
    <meta http-equiv="Cache-Control" content="no-store" />
    <title>Página índice personalizada</title>
  </head>
  <body>
    <img src="/index/static/logo.png"></img><hr/>
    <a href="/do_logout">Cerrar sesión</a>
    <p>MobileTogether: Acceso personalizado</p>
    <div><a href='/run?d=/public/About'>Iniciar la aplicación
About</a></div>
    <div><a href='/run?d=/public/DateCalc'>Iniciar la aplicación
Date Calculator</a></div>
    <div><a href='/run?d=/public/WorldPopulation'>Iniciar la
aplicación World Population Statics</a></div>
  </body>
</html>
```

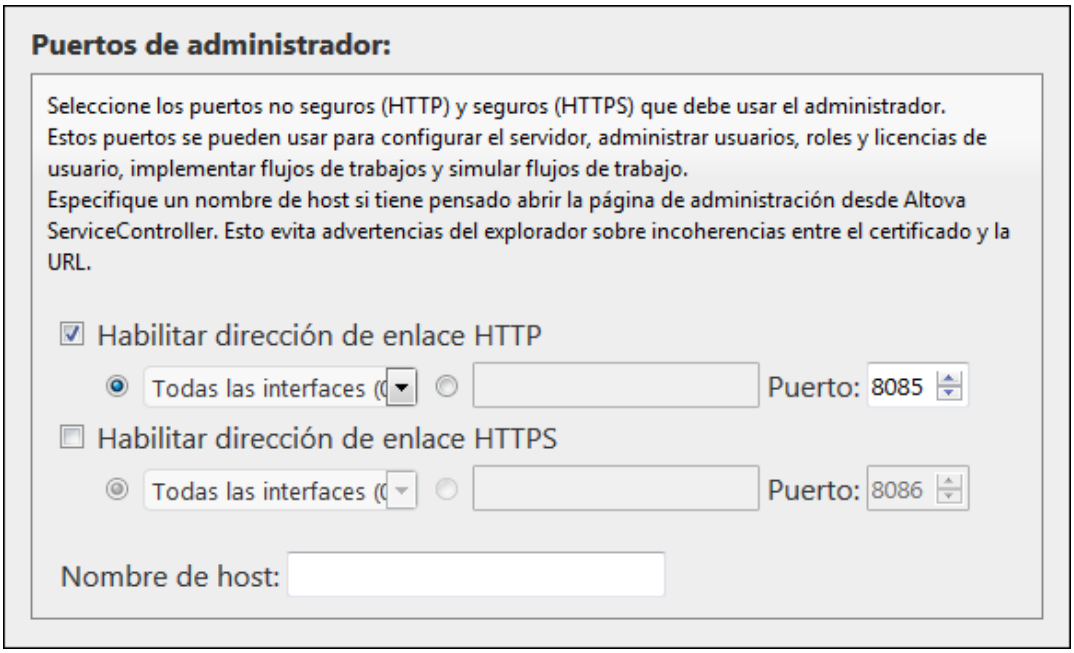
Permitir acceso a MobileTogether mediante /mt-login
Marque esta opción si quiere que el inicio de sesión se lleve a cabo por la página de acceso y la página índice predeterminadas y no por las páginas personalizadas. Esta opción permite almacenar los archivos **login.html** y **index.html** en la ubicación designada pero utilizar las páginas predeterminadas. Puede que el explorador del cliente necesite que se vacíe el caché del explorador o de lo contrario esta opción no surtirá efecto.

Puertos de administrador

Los puertos de administrador permiten acceder al servidor para:

- conectarse a la interfaz web del servidor y llevar a cabo tareas administrativas, como configurar Usuarios y roles, por ejemplo.
- implementar en el servidor diseños de MobileTogether (como soluciones de

MobileTogether). MobileTogether Designer tiene una opción de configuración para especificar la dirección y el puerto del servidor MobileTogether Server donde se deben implementar los diseños.

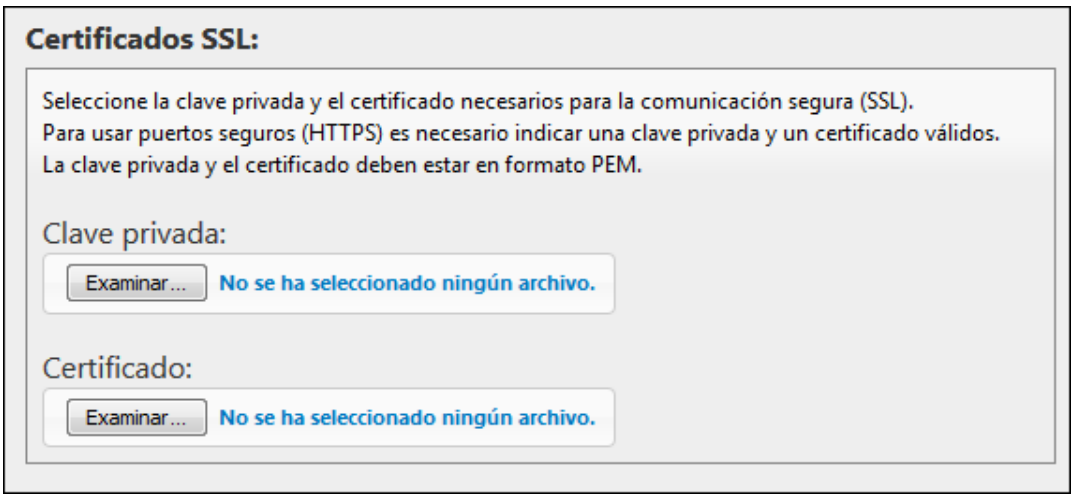


El puerto HTTP es el puerto no seguro, mientras que el puerto HTTPS es el puerto seguro. Para usar HTTPS deberá configurar antes el cifrado SSL. Si configura el puerto HTTPS y desea evitar advertencias del explorador web sobre conflictos entre el certificado SSL y la URL, entonces especifique el nombre de host del equipo donde se abrirá la página de configuración de MobileTogether Server.

Puede especificar si el servidor usará una dirección IP concreta o todas las interfaces y direcciones IP. Si se debe usar una sola dirección IP, introdúzcala en el campo del segundo botón de opción.

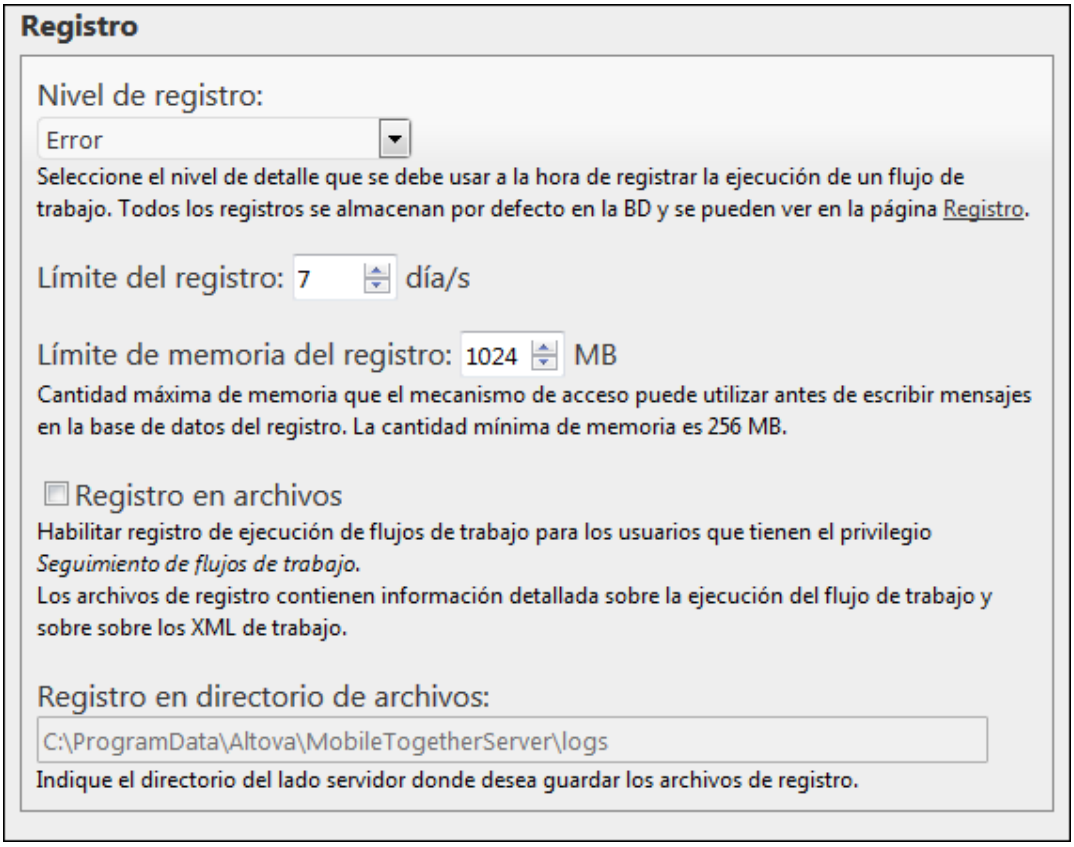
▼ Certificados SSL

Aquí puede indicar qué certificado de clave privada y de clave pública se debe utilizar para la comunicación SSL. Haga clic en el botón **Examinar** correspondiente y seleccione el archivo que desea utilizar. Para más información consulte el apartado Configurar cifrado SSL.



- Registro

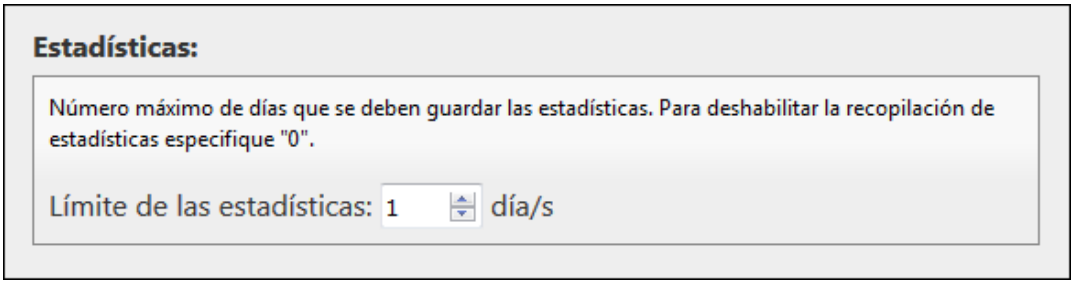
  Los registros de MobileTogether Server contienen informes sobre la actividad de los flujos de trabajo y pueden consultarse en la pestaña **Registro** de la interfaz web. En esta sección del panel puede definir estas opciones de configuración de los registros.



- *Nivel de registro:* aquí puede seleccionar si el registro incluye (i) errores, (ii) errores y advertencias, (ii) errores, advertencias e información (esta última es el nivel de registro más detallado).
- *Límite del registro:* especifica cuánto tiempo se conservan los registros.
- *Límite de memoria del registro:* la escritura de mensajes en la BD del registro tiene menor prioridad que la ejecución de los flujos de trabajo. Por tanto, los mensajes no se escriben en la BD del registro directamente, sino que se guardan en memoria hasta que haya una pausa en la ejecución de flujos de trabajo y se libere tiempo de procesador para escribir los mensajes en la BD. Sin embargo, hay dos excepciones: (i) si no hay tiempo para escribir mensajes en la BD del registro y (i) si la cantidad de memoria utilizada para el registro alcanza el límite de memoria del registro, entonces se descartarán todos los mensajes del registro que están en memoria. En este caso se reemplazan todos los mensajes descartados con un solo mensaje de registro, que indica que la memoria del registro se borró. La opción *Límite de memoria del registro*, por tanto, sirve para crear más espacio en memoria (porque especifica cuándo se deben descartar los mensajes de la memoria) y ayuda a reducir la carga del servidor. De lo contrario, la combinación de la carga de procesamiento y la carga de memoria podría interrumpir el proceso de MobileTogether Server. A la hora de elegir el límite de memoria del registro, tenga en cuenta (i) la cantidad de memoria disponible en el equipo y (ii) el nivel de detalle del registro. El valor mínimo permitido para el límite de memoria del registro es `256 MB`.
- *Registro en archivos:* los usuarios que tengan el privilegio *Seguir flujo de trabajo* podrán guardar registros en un archivo si está marcada la casilla *Registro en archivos*. El directorio donde se guardan los archivos de registro se especifica en la opción *Registro en directorio de archivos*.

▼ Estadísticas

Las estadísticas relacionadas con el uso del servidor se almacenan en una base de datos interna de MobileTogether. Estas estadísticas se pueden consultar en el archivo **`Statistics.mtd`**, que está por defecto en el contenedor **`admin`** de MobileTogether Server (versión 4.0 o superior). La opción **Estadísticas** (*imagen siguiente*) permite especificar el plazo de tiempo durante el que se deben registrar estadísticas. El valor predeterminado es **`0`**, es decir, que no se registran estadísticas.



Debe tener en cuenta que:

- El contenedor **`admin`** se crea automáticamente en las instalaciones nuevas de MobileTogether Server solamente. Si está actualizando su versión de MobileTogether Server, deberá implementar explícitamente el flujo de trabajo

Statistics.mtd en el servidor. Puede implementarlo en cualquier contenedor, pero recomendamos crear un contenedor llamado **admin** e implementarlo ahí.

- Si necesita implementar explícitamente el diseño **statistics.mtd**, está disponible en la carpeta `SolutionFiles` de la carpeta de datos de la aplicación de MobileTogether Server (*ver tabla más abajo*).
- Cuando ejecute la solución, leerá datos de la base de datos de estadísticas internas de MobileTogether Server y le ofrecerá una interfaz desde donde filtrar y seleccionar opciones para ver gráficos de estadísticas de la base de datos.
- La solución muestra cuatro categorías de datos: (i) el número de usuarios que se conectan al servidor, (ii) el número de dispositivos diferentes que se conectan al servidor, (iii) el número de solicitudes enviadas al servidor y (iv) el número de inicios de solución que tienen lugar en el servidor (cada solución se puede iniciar varias veces y cada inicio cuenta). Los datos se pueden filtrar para ver, por ejemplo, estadísticas sobre dispositivos o soluciones concretas. Recuerde que solo se registra la ejecución de la solución y no solicitudes administrativas.
- Para que un usuario pueda leer estadísticas debe tener asignado el privilegio *Lectura de estadísticas*.

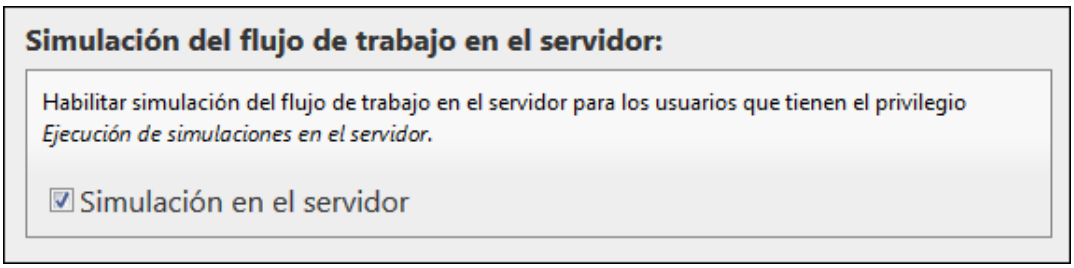
Ubicación de la carpeta de datos de la aplicación MobileTogether Server dependiendo del sistema operativo

Linux	`/var/opt/Altova/MobileTogetherServer`
Mac	`/var/Altova/MobileTogetherServer`
Windows 7, 8, 10	`C:\ProgramData\Altova\MobileTogetherServer`

Para más información sobre cómo configurar y usar la solución **Statistics** consulte el apartado Estadísticas de uso de soluciones.

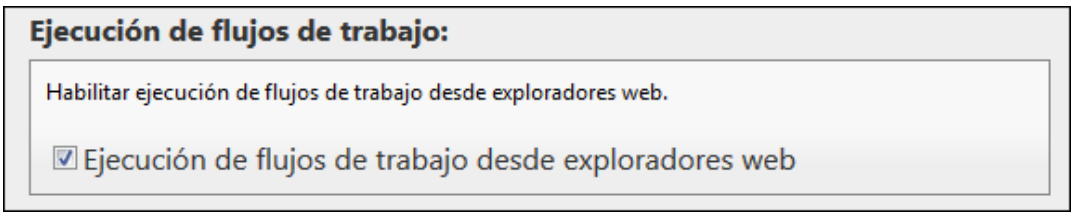
▼ Simulación de flujos de trabajo en el servidor

Si marca esta casilla, los usuarios que tengan el privilegio *Ejecución de simulaciones en el servidor* podrán simular los flujos de trabajo en el servidor.



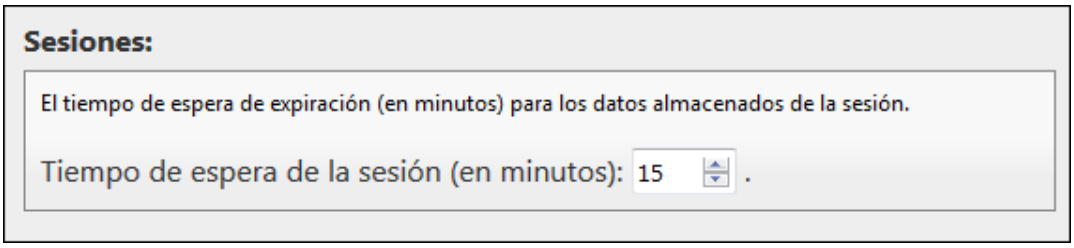
▼ Ejecución de flujos de trabajo

Si marca esta casilla, la ejecución de flujos de trabajo podrá llevarse a cabo desde exploradores web.



- Sesiones

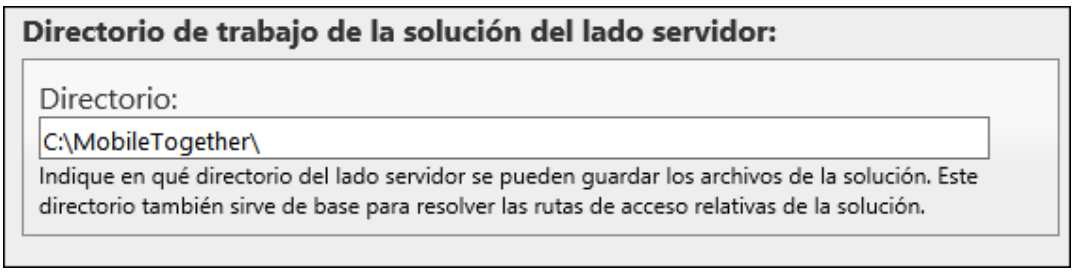
  Establece el tiempo de espera (en minutos) antes de que sea necesario volver a iniciar sesión. Este tiempo de espera afecta tanto al administrador como a los clientes que accedan a MobileTogether Server.



- Directorio de trabajo de la solución del lado servidor

  Cuando las soluciones se ejecutan en el servidor, esta opción sirve para configurar:

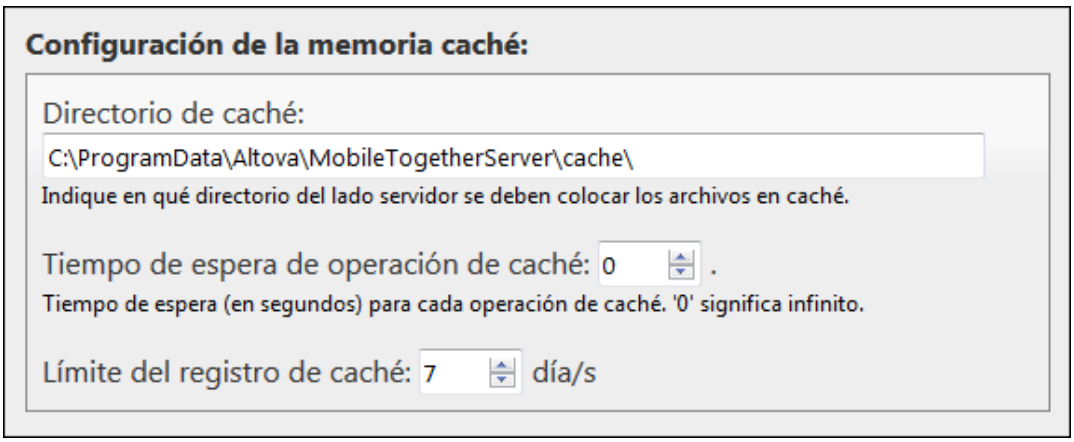
  - El URI base de todas las rutas de acceso relativas del diseño. Las rutas de acceso de todos los archivos del diseño que no estén implementados en el servidor se resolverán como rutas de acceso relativas al directorio que especifique en esta opción. Por ejemplo, si un archivo del diseño tiene la ruta de acceso relativa `MTSData\Test.xml` y no está implementado, entonces debe estar situado en `<Directorio-Trabajo-Configurado-En-Servidor>MTSData\Test.xml`. (Por el contrario, si el archivo está implementado en el servidor, el diseño se sirve de mecanismos internos para acceder a los archivos.)
  - Si en el diseño se utiliza una ruta de acceso absoluta para indicar la ubicación del archivo, esta ruta de acceso debe apuntar a una ubicación dentro de un directorio que sea un subdirectorio del directorio de trabajo especificado en esta opción. Por ejemplo, si el archivo tiene la ruta de acceso absoluta `C:\MTSData\Test.xml`, solamente se podrá acceder al archivo si el directorio de trabajo es `C:\` o `C:\MTSData`.



En otras palabras, esta opción limita el acceso de lectura/escritura a archivos locales durante la ejecución de soluciones. MobileTogether Server solamente tendrá acceso a archivos ubicados dentro del directorio de trabajo o de sus subdirectorios para ejecutar soluciones.

- Configuración de la memoria caché

  En esta sección puede configurar (i) el directorio donde se guardan los archivos de la memoria caché, (ii) el tiempo de espera para cada operación de caché y (iii) cuántos días se mantienen los elementos del registro de caché. Para más información consulte el apartado dedicado a la pestaña **Memoria caché** de la interfaz web.



- Inicio de sesión de Active Directory

  Si habilita esta opción, los usuarios podrán iniciar sesión en el servidor con el nombre de usuario y la contraseña de su dominio. Si marca la casilla *Permitir inicio de sesión a cualquier usuario del dominio,* todos los usuarios del dominio podrán iniciar sesión. Si no marca esta casilla, podrá especificar qué usuarios del dominio pueden iniciar sesión con ayuda de la característica Importar usuarios del dominio. Después podrá asignar roles o privilegios de la forma habitual a los usuarios del dominio que tengan permiso para iniciar sesión.

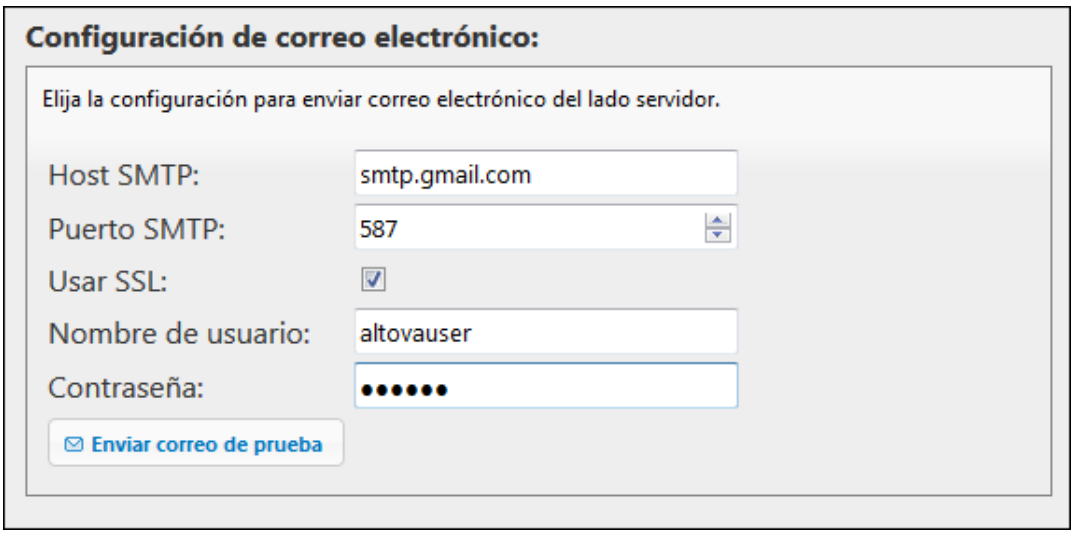
  Tras habilitar el inicio de sesión de Active Directory, introduzca qué dominios desea permitir. Después abra la pestaña **Usuarios y roles | Usuarios** e importe los usuarios pertinentes como usuarios de MobileTogether Server. Estos usuarios podrán utilizar sus datos de inicio

de sesión del dominio para acceder a MobileTogether Server.

- *Permitir inicio de sesión a cualquier usuario del dominio:* todos los usuarios del dominio pueden acceder a MobileTogether Server. Si no marca esta casilla, será necesario importar cada usuario del dominio como usuario de MobileTogether Server. Esto se hace con el botón **Importar usuarios del dominio** de la pestaña **Usuarios y roles | Usuarios**.
- *Sufijos de dominio:* escriba qué dominios se incluyen, separados por comas.

▼ Configuración de correo electrónico

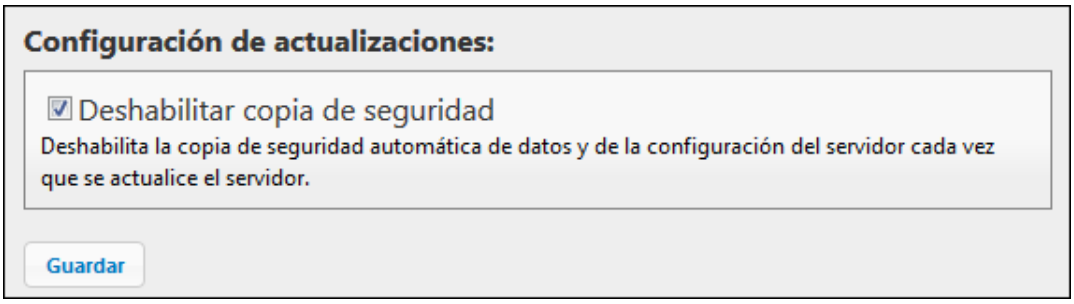
Estas opciones de configuración permiten a los usuarios finales enviar correos electrónicos a través del servidor. Por lo general, la solución ofrecerá un evento que desencadena una acción Enviar correo electrónico que se definió para enviar el correo desde el servidor. Para poder enviar el correo el servidor necesita acceder al servidor SMTP del proveedor del servicio de correo electrónico (que suele ser el ISP).



- *Host y puerto SMTP:* el nombre de host y el puerto SMTP del servidor SMTP de su ISP. Su proveedor de servicios Internet puede darle esta información.
- *Nombre de usuario y contraseña:* nombre de usuario y contraseña de una cuenta de correo electrónico registrada con el proveedor de servicio de correo electrónico.

▼ Configuración de actualizaciones

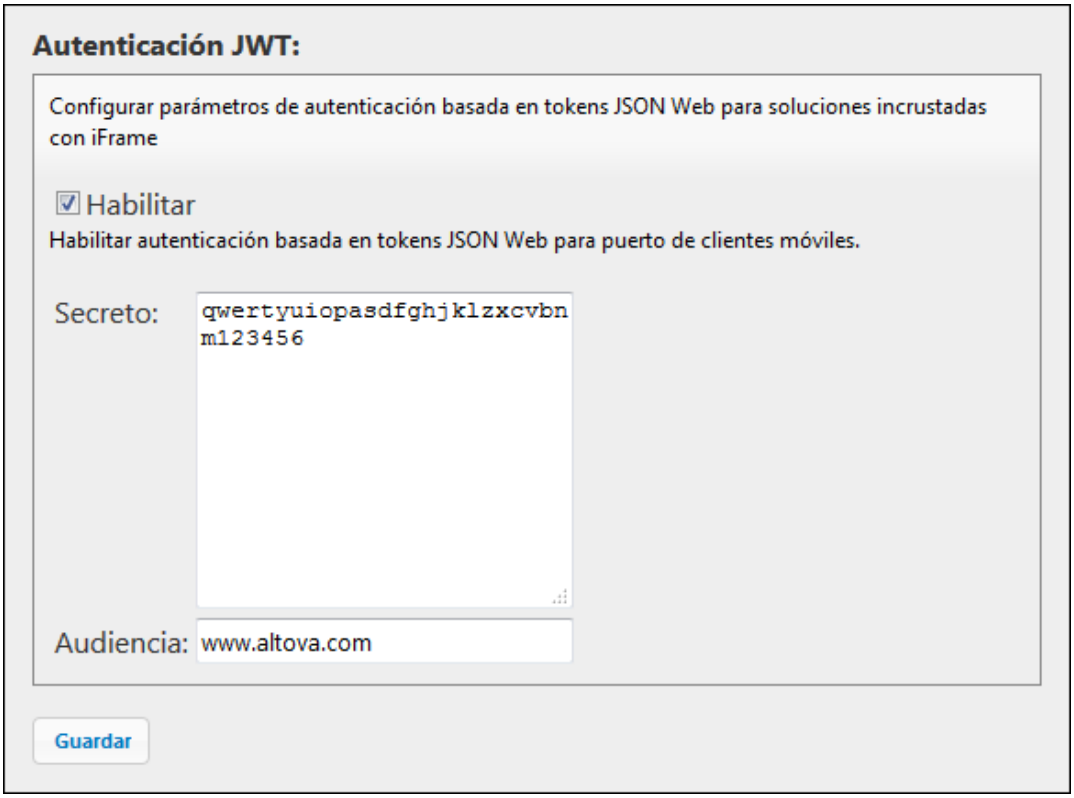
Esta opción de configuración afecta a un procedimiento relacionado con la actualización de la versión de MobileTogether Server. Cada vez que se instala una versión nueva de MobileTogether Server, el procedimiento predeterminado es crear una carpeta de seguridad con todos los archivos y carpetas importantes del servidor. Cuando se desinstala una versión existente de MobileTogether Server, estos archivos y carpetas se conservan en el sistema. Más adelante, cuando se instale una versión nueva de MobileTogether Server, estos datos se copiarán en una carpeta de seguridad que se crea en la carpeta de aplicación MobileTogether Server.



Con esta opción podrá deshabilitar la creación automática de copias de seguridad para la próxima ocasión que instale una versión nueva de MobileTogether Server. De todas maneras, recuerde que puede crear una carpeta de seguridad de forma manual si así lo desea. Para más información consulte el apartado Copias de seguridad y restaurar datos.

Autenticación JWT

Este grupo de opciones de configuración (*imagen siguiente*) habilita la autenticación basada en tokens JSON Web (JWT) de soluciones incrustadas en páginas web. Si una solución está incrustada en una página y la autenticación JWT está habilitada en el servidor, la solución se cargará en la página web donde está incrustada sin necesidad de que el usuario inicie sesión en MobileTogether Server. Consulte la documentación de MobileTogether Designer para obtener más información sobre soluciones incrustadas en páginas web.



Tras habilitar la autenticación JWT debe definir dos valores:

- *Secreto:* si usó una clave simétrica (secreto compartido) para crear los tokens JSON Web, introduzca aquí la clave secreta compartida. Si usó cifrado asimétrico (cifrado de clave pública/privada), introduzca aquí la clave pública. Con esta información el servidor podrá verificar los tokens JSON Web que se envían con la primera solicitud `GET` desde la solución incrustada.
- *Audiencia:* introduzca la misma cadena que introdujo para la notificación *Audiencia* cuando creó los tokens JSON Web (consulte la documentación de MobileTogether Designer para obtener más información).

LicenseServer

MobileTogether Server debe estar registrado con un servidor Altova LicenseServer de la red. Esta opción de configuración sirve para indicar con qué LicenseServer se debe establecer la conexión y para registrar MobileTogether Server con LicenseServer. Consulte el apartado Instalación y configuración de MobileTogether Server para obtener más información.

- Haga clic en el botón **Buscar** para buscar servidores LicenseServer en su red. Los servidores LicenseServer que se detecten se enumeran en la lista desplegable del cuadro combinado. Seleccione el servidor al que desea conectarse en esta lista.
- Haga clic en el botón **Dirección** para introducir la dirección del servidor.

Una vez ubicado el servidor LicenseServer, se habilita el botón Registrarse con LicenseServer. Haga clic en este botón para registrar MobileTogether Server con LicenseServer. Haga clic en **Adquirir licencia** para abrir la interfaz web de LicenseServer y asignar una licencia a MobileTogether Server.

Índice

U

W