Agilent OpenLAB Data Store Administration

Guide for Administrators

Agilent Technologies
Notices

© Agilent Technologies, Inc. 2014

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Agilent Technologies, Inc. as governed by United States and international copyright laws.

Manual Part Number
M8620-90115

Edition
September 2014
Printed in USA

Agilent Technologies, Inc.
3501 Stevens Creek Blvd.
Santa Clara, CA 95051 USA

Microsoft ® is a U.S. registered trademark of Microsoft Corporation.

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Agilent disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Agilent shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Agilent and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Safety Notices

CAUTION

A CAUTION notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

U.S. Government Restricted Rights. Software and technical data rights granted to the federal government include only those rights customarily provided to end user customers. Agilent provides this customary commercial license in Software and technical data pursuant to FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for the Department of Defense, DFARS 252.227-7015 (Technical Data - Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation).
Contents

OpenLAB Data Store System Architecture 5
OpenLAB Data Store Licensing 6
  Licenses 6
  Flexera license manager 6
Security and Data Integrity 7
  Security aspects 7
  Data integrity 7
OpenLAB Control Panel 8
  License Management 8
  System Activity Log 9
  Diagnostics 10
  Administrative Reports 10
  Authentication provider 11
  Security policy 12
  User management 13
OpenLAB Server Utility 16
  Activity Log Export 16
  Backup and restore 17
  Windows Domain 17
  Server Settings 17
FTP Server Protocol 18
  Enable the Data Store server as an FTP server 18
  Connect to the Data Store through an FTP protocol 18
  Disable the Data Store server as an FTP server 19
  Generate a repository SSL Keystore 19
  Generate a Certificate Authority (CA) Key and Certificate 22
  File server properties 23
OpenLAB Data Store System Architecture

OpenLAB Data Store is installed on a Windows Server 2012 R2 or Windows Server 2008 R2 SP1. OpenLAB Data Store includes OpenLAB Shared Services (OLSS) which is automatically installed on the same machine. Changing the server domain after the installation requires direct consultation with Agilent Support.

Client machines that access the Data Store server make use of the following components:

- OpenLAB Data Store web interface - OpenLAB Data Store provides a thin client web based user interface that can be accessed using Microsoft Internet Explorer. The web interface provides access to the Data Store folders and files.

- OpenLAB Control Panel - The OpenLAB Control Panel is the user interface that provides access to administrative functions used for managing OpenLAB Data Store and OpenLAB Shared Services.

Figure 1  OpenLAB Data Store architecture
OpenLAB Data Store Licensing

Licenses

Table 1 lists the License Features in OpenLAB Data Store.

<table>
<thead>
<tr>
<th>Description</th>
<th>License Feature(s) in OpenLAB Data Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenLAB CDS Shared Services Server</td>
<td>1 x AgilentOpenLABSharedServices</td>
</tr>
<tr>
<td>OpenLAB Data Store Server</td>
<td>1 x AgilentOpenLABDataStoreServer</td>
</tr>
</tbody>
</table>

Additional Instrument connectivity licenses (for example, OpenLAB Data Store MS Instrument and OpenLAB Data Store CDS Instrument License) are required for every concurrent instrument that stores data into Data Store.

Flexera license manager

OpenLAB Data Store uses a 3rd party tool called FlexNet Producer Suite from Flexera to manage the licenses. The required Licensing server components are installed by default on the Data Store server.

License Management in OpenLAB Shared Services requires an additional Windows service to be running. This Windows service is called Agilent OpenLAB License Server. This service must be running on the server where you manage your licenses.
Security and Data Integrity

This section explains the built-in security and how it supports the FDA 21 CFR Part 11. It also explains the system security features provided by OpenLAB Shared Services.

Security aspects

In OpenLAB Data Store, security aspects are covered by OpenLAB Shared Services.

The OpenLAB Shared Services functionality related to security includes the following (see “OpenLAB Control Panel” on page 8 for details):

- System Activity Log
- Selection of authentication provider
- Users, Groups and Roles Management
- Security Policy

Data integrity

OpenLAB Data Store stores data in a manner that supports compliance with 21 CFR Part 11. It provides secure data storage with access control and an audit trail. Data files are versioned to ensure data integrity and traceability. In addition, OpenLAB Data Store provides electronic signatures allowing users to sign off on data.
OpenLAB Control Panel

Using the OpenLAB Control Panel, you can access OpenLAB Shared Services control features such as security policy, central configuration. These features are described in more detail in this chapter.

License Management

This service includes the administration of all licenses that are required for your system.

Before adding a license file, you must first purchase the license and generate the license file using SubscribeNet. For more information on generating new license files, refer to the Agilent OpenLAB Data Store Installation Guide.

License Management in OpenLAB Control Panel provides the following functions:

- You can add license files to the license server.
- You can navigate to the license monitor and view the properties of all licenses installed on a given license server.
- You can remove license files from the license server. This may be useful if an invalid license file has been added.
- You can view or change the license server.
- You can view, copy, or save the MAC Address of the license server.
- You can navigate to the Agilent Electronic Software and License Delivery web page to get a license.

For more information on adding license files and viewing the license properties, refer to the OpenLAB Control Panel online help.

The following properties are shown for installed licenses:

- **Feature:** This indicates the type of license used.
- **Version:** If a license is versioned, you can see the version number. For licenses that are not versioned, the version is always shown as 1.0.
• **In Use (Available)**: This indicates the number of licenses that are currently in use and, in brackets, the total number of licenses. With the OpenLAB Data Store licensing strategy, a license is only in use as long as a software instance is running (see “OpenLAB Data Store Licensing” on page 6).

• **Expiration**: If the license is only valid for a certain period of time, the expiration date is displayed.

• In the **Alerts** pane, you are informed if the number of available licenses has gone down to zero for a specific feature, or if you have started a software instance which requires a license that is unavailable.

### System Activity Log

The System Activity Log allows you to centrally access all system activities. It contains information on the various events associated with OpenLAB Shared Services. You can filter the list in order to view only events of a specific type, in a specific time range, created by a specific user, or containing a specific description.

The following types of events are recorded:

- System
- User
- Group
- Security
- Printer
- License

To get more information on an event, expand the line of interest in the activity logbook viewer.

**NOTE**

By default, activity logging is disabled. To enable it in OpenLAB Control Panel, you must have the **Edit activity log properties** privilege. Once enabled, activity logging cannot be disabled again.
Diagnostics

The Diagnostics view allows you to access several reports and tools for diagnostic purposes:

- Ping the OpenLAB Shared Services server.
- Create a report, for the OpenLAB Shared Services server, with information on the operation system, processors, disk drives, processes, network and connections.
- Centrally access and download all the log files, trace files, etc. that are created by the registered modules.

Administrative Reports

In the Administrative Reports view, you can additionally create and export various XML or PDF reports related to the system configuration:

- **Roles and Privileges Report**
  Describes all roles defined on the system, including details of all privileges included in each role.

- **Users and Groups Report**
  This report provides an overview of all users and groups access rights to instruments and projects on the system. Note that users and groups that have not been granted access to instruments or projects are not included in this report.
Authentication provider

Authentication providers are used to prove the identity of users that log in to the system.

During the installation, the OpenLAB Data Store server is automatically activated and configured using internal authentication with a default user, admin, and password, openlab. On first login, the system will require the user to change this password before proceeding. You may now change the authentication mode, if required.

OpenLAB Data Store supports the following Authentication providers:

• **Internal**
  In this mode, the user's credentials are stored in the OpenLAB Shared Services database. You are asked to create an administrator account for OpenLAB Shared Services before setting up other users. This is the only mode in which you can create new users within the system; in all other modes you can only map to users that exist in a different system.

• **Windows Domain**
  You import existing Windows users into OpenLAB Shared Services. The authentication is done by a Windows Domain within the Enterprise. OpenLAB Shared Services only use the identity and password of the mapped users; roles and privileges for OpenLAB Data Store are still configured with OpenLAB Shared Services.
Security policy

With the authentication provider **Internal**, you can set all of the parameters described below in the OpenLAB Control Panel. With Windows Domain authentication you can only set the inactivity time in the OpenLAB Control Panel; all other parameters are defined by the external system. Table 2 describes the security policy settings.

**Table 2  Security Policy settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>If users change their passwords, they must choose a password with at least the given number of characters. The default setting is 5. Only available for authentication provider <strong>Internal</strong>.</td>
</tr>
<tr>
<td>Password expiration period (days)</td>
<td>The default value is 0 days. This period can be reset by the OpenLAB system administrator. When the user tries to log in after this period of time, the system will ask him to change the password. The expiration period starts with the last password change or with the creation of a user with a new default password. Only available for authentication provider <strong>Internal</strong>.</td>
</tr>
<tr>
<td>Maximum unsuccessful login attempts before locking account</td>
<td>If a user tries to log in with invalid user credentials a number of times, the user is locked out of the system for a certain period of time (<strong>Account lock time</strong>, see below). Login is impossible, even with valid user credentials. You can define the number of allowed login attempts. The default setting is 3. Only available for authentication provider <strong>Internal</strong>.</td>
</tr>
<tr>
<td>Account lock time (minutes)</td>
<td>Once a user has exceeded the maximum number of allowed unsuccessful login attempts, this is the amount of time that must pass before he can try again. The default setting is 5 min. Only available for authentication provider <strong>Internal</strong>.</td>
</tr>
<tr>
<td>Inactivity time before locking the application</td>
<td>If the OpenLAB Control Panel is inactive for this amount of time, the user interface will be locked. This setting is also used to set the time-based session lock in ChemStation. The default setting is 10 min. Set the value to zero to never lock.</td>
</tr>
<tr>
<td>Single Sign-On</td>
<td>With Single Sign-On enabled, the user will not see the OpenLAB Control Panel login screen. Only available for authentication provider <strong>Windows Domain</strong>.</td>
</tr>
</tbody>
</table>
User management

OpenLAB Shared Services allow you to assign specific roles to users or user groups. If you manage your users within a Windows domain, you can map those existing users into OpenLAB Shared Services.

Each user can be member of multiple groups. You must assign a specific role to each group. You can also assign roles to single users; however, for the sake of clarity, it is strongly recommended to assign roles only on the group level.

The roles are equipped with numerous specific privileges which define what the users are allowed to view or do in OpenLAB Control Panel and in OpenLAB Data Store. Table 3 describes the user credentials.

**Table 3**  
**User Credentials**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Username to login to the system.</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>Additional information about the user (e.g. department, function etc.)</td>
<td>No</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the user; minimum password length is defined in the Security Policy.</td>
<td>Yes</td>
</tr>
<tr>
<td>Email</td>
<td>Email address of the user.</td>
<td>No</td>
</tr>
<tr>
<td>Full name</td>
<td>The full (long) name of the user.</td>
<td>No</td>
</tr>
<tr>
<td>Contact Information</td>
<td>General contact information (e.g. telephone number, pager etc.)</td>
<td>No</td>
</tr>
<tr>
<td>Account is disabled</td>
<td>Select the check box to disable a user. Disabled users cannot log in any more. Users may be automatically disabled after too many failed login attempts. If a user is disabled, a corresponding message is displayed instead of the check box. After a given time (see <strong>Account lock time</strong> in the <strong>Security Policy</strong> settings), the user is automatically enabled again.</td>
<td>No</td>
</tr>
<tr>
<td>User cannot change password</td>
<td>Flag that indicates whether the user can change his own password. The flag is false by default (that is, users CAN change their passwords).</td>
<td>No</td>
</tr>
<tr>
<td>User must change password at next logon</td>
<td>If set to true, the user has to change his password at the next login. The flag is automatically set to false after the user has changed the password successfully. The flag is true by default for new users.</td>
<td>No</td>
</tr>
<tr>
<td>Password never expires</td>
<td>If set to true, the user never needs to change their password.</td>
<td>No</td>
</tr>
</tbody>
</table>
If you use Windows domain as an external authentication provider you cannot create new users, but must import users that exist in the authentication systems. A search function helps you find specific users in the authentication system. In the OpenLAB Control Panel, you can manage the roles for those external users, but not the actual user credentials such as user name and password. If you want to remove an external user, you unmap the user in the OpenLAB Control Panel. The user continues to exist in the external authentication system.

**Groups**

If you use an external authentication provider, you can either import the names of groups that exist in the external system or create new internal groups. There is no limit on the number of groups that can be mapped or created.

You can assign users to groups in the external system or in OpenLAB Control Panel. If you need additional user assignments that are relevant only for OpenLAB CDS, you create them in OpenLAB Control Panel. Otherwise it is sufficient to only import the groups and assign the required roles to the groups.

If you delete or unmap a group, the users who where members in this group remain unchanged.

**Roles and privileges**

Roles are used to assign privileges to a user or a user group globally. The system contains a list of predefined roles which are installed as part of the system installation (see Table 4). Each role has certain privileges assigned.

---

**Table 3  User Credentials (continued)**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Membership</td>
<td>Assign the user to the relevant groups.</td>
<td></td>
</tr>
<tr>
<td>Role Membership</td>
<td>Assign roles directly to the user.</td>
<td></td>
</tr>
</tbody>
</table>
When you assign privileges to a role, you first select the required role type and then select the privileges related to this role type. Each role can only have privileges of one specific role type; the only exception is the predefined role Everything, which has all privileges of all role types. Users or groups may require multiple roles to perform system functions.

### Table 4 Data Store Predefined roles

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Data Store Approver</th>
<th>Data Store Contributor</th>
<th>Data Store Reader</th>
<th>Archivist</th>
<th>System Administrator</th>
<th>Project Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronically sign files</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Save or modify content</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View content</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View projects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Archive and de-archive content</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify system settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Manage security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
OpenLAB Server Utility

The Agilent OpenLAB Server Utility program is automatically installed with your OpenLAB software to help administrators manage the system.

To open the Utility, select Windows Start > All Programs > Agilent Technologies > OpenLAB > OpenLAB Server Utility.

A user must have Windows administrator rights to access this utility.

Activity Log Export

Activity logs database can become large over time and affect the performance of activity log related operations. Use Activity Log Export to archive the activity log entries to an XML file and purge them from the Activity Log database.

This export can only access logs that are stored on the computer where you are using the Server Utility program.

Export an activity log for a client/server system

1. Access the Server Utility program that is installed on the server.
2. Specify a date range, and click Export.

Export an activity log for a workstation

1. Access the Server Utility program that is installed on the workstation.
2. Select Export from current activity log database.
3. Specify a date range, and click Export.

Export an archived activity log for a workstation

You can create an archived activity log only during an upgrade from a system using SQL CE (primarily associated with a workstation solution) with a database larger than 1 GB.

1. Access the Server Utility program that is installed on the workstation.
2. Select Export from archived activity log database.
3. Browse for and select the archived database.
4. Click Export.
During the export or purge, the OpenLAB Control Panel is disconnected from the server. Agilent recommends that you notify all users before beginning an export.

**Backup and restore**

This feature is not available for OpenLAB Data Store systems. See the Agilent OpenLAB Data Store Maintenance Guide for information on how to back up and restore OpenLAB Data Store.

**Windows Domain**

If windows domain authentication is used to identify your OpenLAB users, OpenLAB must be given access to the server where these credentials are stored.

Use **Windows Domain** to specify or change the credentials that OpenLAB will use to access your windows domain server. This feature can only access credentials that are stored on the computer where you opened the Server Utility program.

To specify or change the **Domain**, **User name**, or **Password** for the windows account that will be used to access your windows domain server, use the **Server Utility** program that is installed on the server.

**Server Settings**

In a client/server configuration, use **Server Settings** to manage server connections for your local system. The list of servers here determines which servers users may choose to connect to when they log into OpenLAB. Administrators can limit users from switching to a non-default server from this tab.

This feature manages server connections for the computer where you are using the **Server Utility** program.

The server connections for each client in a client/server system are managed through each client, therefore to change the server connections for a client, access the **Server Utility** program installed on that client.

In a workstation configuration, there is typically one server connection so this feature is not used.
FTP Server Protocol

Data Store can be used as an FTP server and accessed through any FTP server protocol.

Enable the Data Store server as an FTP server

1. On your server, navigate to \Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\module\ds-alfresco
2. Open the alfresco-global.properties file in any text editor.
3. Change ftp.enabled=false to ftp.enabled=true.
4. Save the file.
5. Restart tomcat service.

Connect to the Data Store through an FTP protocol

1. Access your FTP Client.
2. Within the FTP protocol, use:
   • The Data Store server address as the FTP host name
   • The Data Store server port
   • Your Control Panel username and password
3. Connect according to your FTP protocol.
Disable the Data Store server as an FTP server

1. On your server, navigate to C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\module\ds-alfresco
2. Open the alfresco-global.properties file in any text editor.
3. Change `ftp.enabled=true` to `ftp.enabled=false`.
4. Save the file.
5. Restart the tomcat service.

Generate a repository SSL Keystore

The following procedure creates an RSA public/private key pair for the repository with a certificate signed by the Alfresco Certificate Authority (CA). However, you can use your own Corporate Certificate or a Certificate from Verisign.

You also create a truststore for the repository containing the CA certificate that is used to authenticate connections to specific repository URLs from Solr. This procedure assumes the existence of the Alfresco CA key and certificate to sign the repository certificate. However, for security reasons, these may not available. You can either generate your own CA key and certificate or use a recognized Certificate Authority, such as Verisign. To generate your own CA key and certificate, see “Generate a Certificate Authority (CA) Key and Certificate” on page 22.

**NOTE**

<store password> is the keystore password. The file C:\DSContent\keystore\ssl-keystore-passwords.properties contains passwords for the SSL keystore, whereas the file C:\DSContent\keystore\ssl-truststore-passwords-properties contains passwords for the SSL truststore.
1 Generate the repository public/private key pair in keystore.

   $ keytool -genkey -alias repo -keyalg RSA -keystore
ssl.keystore -storetype JCEKS -storepass <store password>

   Enter keystore password:
   Re-enter new password:
   What is your first and last name?
     [Unknown]: Data Store Repository
   What is the name of your organizational unit?
     [Unknown]:
   What is the name of your organization?
     [Unknown]: Alfresco Software Ltd.
   What is the name of your City or Locality?
     [Unknown]: Maidenhead
   What is the name of your State or Province?
     [Unknown]: UK
   What is the two-letter country code for this unit?
     [Unknown]: GB
   Is CN=Alfresco Repository, OU=Unknown, O=Alfresco
Software Ltd., L=Maidenhead, ST=UK, C=GB correct? [no]: yes
   Enter key password for <repo>
     (RETURN if same as keystore password):

2 Generate a certificate request for the repository key.

   $ keytool -keystore ssl.keystore -alias repo -certreq
-file repo.csr -storetype JCEKS -storepass <store
password>

3 Alfresco CA signs the certificate request and creates a certificate that is
valid for 365 days.

   $ openssl x509 -CA ca.crt -CAkey ca.key -CAcreateserial
-ren -in repo.csr -out repo.crt -days 365 Signature ok
subject=/C=GB/ST=UK/L=Maidenhead/O=Alfresco Software
Ltd./OU=Unknown/CN=Alfresco Repository
Getting CA Private Key

Enter pass phrase for ca.key:

4 Import the Alfresco CA key into the repository keystore.

$ keytool -import -alias AlfrescoCA -file ca.crt
   -keystore ssl.keystore -storetype JCEKS -storepass <store password>

Enter keystore password:

Owner: CN=Alfresco CA, O=Alfresco Software Ltd.,
L=Maidenhead, ST=UK, C=GB
Issuer: CN=Alfresco CA, O=Alfresco Software Ltd., L=Maidenhead, ST=UK, C=GB
Serial number: 805ba6dc8f62f8b8 Valid from: Fri Aug 12
Certificate fingerprints: MD5:
   A3 Signature algorithm name: SHA1withRSA Version: 3
   Extensions: #1: ObjectId: 2.5.29.14 Criticality=false
   SubjectKeyIdentifier [ KeyIdentifier [ 0000: 08 42 40
   DC FE 4A 50 87 05 2B 38 4D 92 70 8E 51 .B@..JP..+8M.p.Q
   0010: 4E 38 71 D6 ] ] #2: ObjectId: 2.5.29.19 Criticality=false
   BasicConstraints:[ CA:true PathLen:2147483647 ] #3:
   ObjectId: 2.5.29.35 Criticality=false
   AuthorityKeyIdentifier [ KeyIdentifier [ 0000: 08 42 40
   DC FE 4A 50 87 05 2B 38 4D 92 70 8E 51 .B@..JP..+8M.p.Q
   0010: 4E 38 71 D6 ] ] [CN=Alfresco CA, O=Alfresco Software Ltd.,
   L=Maidenhead, ST=UK, C=GB] SerialNumber: [ 805ba6dc
   8f62f8b8 ]

Trust this certificate? [no]: yes
Certificate was added to keystore
Import the CA-signed repository certificate into the repository keystore.

```
$ keytool -import -alias repo -file repo.crt -keystore ssl.keystore -storetype JCEKS -storepass <store password>
```

Enter keystore password:
Certificate reply was installed in keystore

Convert the repository keystore to a pkcs12 keystore (for use in browsers, such as IE). Specify the keystore password for pkcs12 keystore as ‘alfresco’. You will need to import this into IE to use https.

```
keytool -importkeystore -srckeystore ssl.keystore -srcstorepass <keystore password> -srcstoretype JCEKS -srcalias repo -srckeypass kT9X6oe68t -destkeystore Browser.p12 -deststoretype pkcs12 -deststorepass alfresco -destalias repo -destkeypass alfresco
```

Create a repository truststore containing the Alfresco CA certificate.

```
keytool -import -alias AlfrescoCA -file ca.crt -keystore ssl.keystore -storetype JCEKS
```

Copy the keystore and truststore to the repository keystore location C:\DSContent\keystore.

Update the SSL properties (properties starting with the prefixes alfresco.encryption.ssl.keystore and alfresco.encryption.ssl.truststore).

---

**Generate a Certificate Authority (CA) Key and Certificate**

Create your CA key and certificate to sign the repository certificate.

1 Generate the CA private key.

```
$ openssl genrsa -des3 -out ca.key 1024 Generating RSA private key, 1024 bit long modulus ............+++++
..++++++ e is 65537 (0x10001)
```

Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
2 Generate the CA self-signed certificate.

```
$ openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields, there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:UK
Locality Name (eg, city) []:Maidenhead
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Alfresco Software Ltd.
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:Alfresco CA
Email Address []:
```

File server properties

Create a Simple Keystore and Truststore

Use keytool to create a simple JKS keystore suitable for use with JSSE. Make a keyEntry (with public/private keys) in the keystore, then make a corresponding trustedCertEntry (public keys only) in a truststore. (For client authentication, a similar process is required for the client's certificates.) Storing trust anchors in PKCS12 is not supported. Users should use JKS for storing trust anchors and PKCS12 for private keys.

For more information on this procedure, please see the keytool documentation for Solaris or Microsoft Windows.
1 Create a new keystore and self-signed certificate with corresponding public/private keys.

% keytool -genkeypair -alias ftp -keyalg RSA -validity 7 -keystore ftp.keystore

Enter keystore password: password

What is your first and last name?
[Unknown]: Duke

What is the name of your organizational unit?
[Unknown]: Java Software

What is the name of your organization?
[Unknown]: Sun Microsystems, Inc.

What is the name of your City or Locality?
[Unknown]: Palo Alto

What is the name of your State or Province?
[Unknown]: CA

What is the two-letter country code for this unit?
[Unknown]: US

Is CN=Duke, OU=Java Software, O="Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US correct?
[no]: yes

Enter key password for <ftp>

(RETURN if same as keystore password): <CR>

This is the keystore that the server will use.

2 Examine the keystore. Note that the entry type is keyEntry, which means that this entry has a private key associated with it (shown in red).

% keytool -list -v -keystore ftp.keystore

Enter keystore password: password

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: ftp
Creation date: Dec 20, 2001
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Duke, OU=Java Software, O="Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US
Serial number: 3c22adc1
Certificate fingerprints:
3 Export and examine the self-signed certificate.
   % keytool -export -alias ftp -keystore ftp.keystore -rfc -file ftp.cer
Enter keystore password: password
Certificate stored in file <ftp.cer>
   % cat ftp.cer
-----BEGIN CERTIFICATE-----
MIICXjCCAccCBDwircEwDQYJKoZIhvcNAQEEBQAwdjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRMwEAYDVQQHEw4xHzAdBgNVBAoTFlN1biBNaWNyb3N5
"Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US
Serial number: 3c22adc1
Certificate fingerprints:
-----END CERTIFICATE-----
MIICXjCCAccCBDwircEwDQYJKoZIhvcNAQEEBQAwdjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRMwEAYDVQQHEw4xHzAdBgNVBAoTFlN1biBNaWNyb3N5
"Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US
Serial number: 3c22adc1
Certificate fingerprints:
-----END CERTIFICATE-----
MIICXjCCAccCBDwircEwDQYJKoZIhvcNAQEEBQAwdjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRMwEAYDVQQHEw4xHzAdBgNVBAoTFlN1biBNaWNyb3N5
"Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US
Serial number: 3c22adc1
Certificate fingerprints:
-----END CERTIFICATE-----
MIICXjCCAccCBDwircEwDQYJKoZIhvcNAQEEBQAwdjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRMwEAYDVQQHEw4xHzAdBgNVBAoTFlN1biBNaWNyb3N5
"Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US
Serial number: 3c22adc1
Certificate fingerprints:
-----END CERTIFICATE-----
MIICXjCCAccCBDwircEwDQYJKoZIhvcNAQEEBQAwdjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRMwEAYDVQQHEw4xHzAdBgNVBAoTFlN1biBNaWNyb3N5
"Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US
Serial number: 3c22adc1
Certificate fingerprints:
-----END CERTIFICATE-----

Alternatively, you could generate a Certificate Signing Request (CSR) with `certreq` and send that to a Certificate Authority (CA) for signing, but that is beyond the scope of this example.

4 Import the certificate into a new truststore.

```bash
% keytool -import -alias ftpcert -file ftp.cer -keystore ftp.truststore
```

Enter keystore password: `trustword`

Owner: CN=Duke, OU=Java Software, O="Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US


Serial number: 3c22adc1


Certificate fingerprints:

```
```

Trust this certificate? [no]: yes
Certificate was added to keystore

Examine the truststore. Note that the entry type is trustedCertEntry, which means that a private key is not available for this entry (shown in red). It also means that this file is not suitable as a KeyManager's keystore.

% keytool -list -v -keystore ftp.truststore
Enter keystore password: trustword

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: ftpcert
Creation date: Dec 20, 2001
Entry type: trustedCertEntry

Owner: CN=Duke, OU=Java Software, O="Sun Microsystems, Inc.", L=Palo Alto, ST=CA, C=US
Serial number: 3c22adc1
Certificate fingerprints:

Copy files ftp.cer, ftp.keystore, and ftp.truststore to C:\DSContent\Keystore.
The following properties have to be added and configured to enable FTPS support. Please edit C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\module\ds-alfresco\alfresco-global.properties and the following properties.

- **ftp.keyStore**: Specifies the absolute path to the keystore filename for FTPS support (for example, C:\\DSContent\\keystore\\ftp.keystore)
- **ftp.trustStore**: Specifies the absolute path to the truststore filename for FTPS support (for example, C:\\DSContent\\keystore\\ftp.truststore)
- **ftp.keyStorePassphrase**: Specifies the passphrase for the keystore files. These correspond to the password specified in the sections above.
- **ftp.trustStorePassphrase**: Specifies the passphrase for the truststore files. These correspond to the trustword specified in the sections above.
- **ftp.requireSecureSession**: Specifies whether only secure FTPS sessions will be allowed to log in to the FTP server. To force all connections to use FTPS, set ftp.requireSecureSession=true.

If IPv6 is enabled on your system, Alfresco automatically uses IPv6.

The **ftp.keyStore**, **ftp.trustStore**, **ftp.keyStorePassphrase**, and **ftp.trustStorePassphrase** values must all be specified to enable FTPS support. These files are under C:\DSContent\keystore.

Only explicit FTP over SSL/TLS mode is supported. Encrypted data sessions are not supported.