Enterprise 3.4.2

Alfresco Enterprise 3.4.2 Administrator

Contents

Copyright

Preface

The purpose of this guide is to provide guidance on installing, configuring, maintaining, and administering an Alfresco production environment.

This guide contains the following sections:

- **Installing Alfresco** describes how to install Alfresco and components
- **Upgrading Alfresco** describes how to upgrade Alfresco and components
- **Administering Alfresco** describes how to configure, maintain, and manage the system
- **Troubleshooting** describes how to analyze and troubleshoot various scenarios
- **Reference** provides additional information on topics discussed in this guide

Audience

This guide is intended to assist administrators to install, upgrade, configure, and manage an Alfresco production environment.

No specialist knowledge is assumed to install and configure Alfresco; however, the information provided in this guide assumes that you are familiar with the environment on which you are installing. Some administrative tasks also require knowledge of your environment and configuration processes.

Typographic conventions used in this guide

The following conventions are used in this guide to indicate types of information.

Convention	Type of information
bold	Identifies user interface elements and items to select, such as menu options, command buttons, and items in a list.
`monospace`	Identifies file and path names, input text, standard output, code, text the user types, and so on.
italics	Emphasizes importance and used for variable expressions, such as parameters. For example: `kill -9` *<process_id>*
CAPITALS	Refers to specific keys on the keyboard. For example: SHIFT, CTRL, or ALT
KEY+KEY	Refers to key combinations when you must press and hold down the first key, and then press another key. For example: CTRL+P or ALT+F4
✏	Refers to a note that provides supplemental information related to a topic.
❗	Refers to a note that provides important information to remember.
⚠	Refers to a note that warns about the danger of doing or not doing something.
💡	Refers to a note that provides helpful information or a faster way of doing something.

Resources

The resources in the following table provide additional information related to using Alfresco.

The guides referred to in this table are available in PDF format from Alfresco Network.

Resource	Description
Getting Started with Alfresco Share Collaboration	Introduction to using Alfresco Share for collaborative content management.
Getting Started with Explorer DM for Alfresco	Introduction to using Alfresco DM Explorer features.
Getting Started with WCM for Alfresco	Introduction to using WCM features.
Getting Started with Alfresco Records Management	Introduction to using the Records Management module.
Share End User Help	How to use the Alfresco Share user interface.
Explorer End User Help	How to use the Alfresco Explorer user interface.
MS Office Add-in End User Help	How to use the MS Office Add-in.
Managing Alfresco Content from within Microsoft Office	How to use the Alfresco Explorer user interface.
Installing and Configuring Alfresco ECM	Installing Alfresco and related components, and configuring the core and extended services.
Administering an Alfresco ECM Production Environment	Administration guide for installing, configuring, and managing an Alfresco production environment.
http://network.alfresco.com	Alfresco Enterprise Network provides real-time access to Alfresco Support, developers, technicians, and staff. It works in conjunction with Alfresco Enterprise backbone services to automate real-time, seamless integration with Alfresco Enterprise server installations, and it provides reporting for Alfresco subscription customers.
Knowledge Base	Additional information on specific Enterprise features and applications in white papers, Frequently Asked Questions (FAQ), and articles.
http://wiki.alfresco.com	Alfresco wiki, community-contributed information on all aspects of the Alfresco environment.
http://www.alfresco.com	Alfresco web site for all information about Alfresco, including links to various resources, such as webinars and forums.

Installing

This section provides information for installing Alfresco and Alfresco components.

Depending on your system, you can install Alfresco using one of the following methods:

- Using an installation wizard, which contains the required software and components you need
- Using a standard WAR file to deploy on an existing application server

Alfresco Simple Installs

This section includes instructions that describe the quickest way to install Alfresco using the installation wizards.

Installing Alfresco on Linux

The setup wizard for Linux installs all the software and components that you require for running Alfresco. This setup wizard installs Alfresco and additional software, including a Tomcat application server, PostgreSQL database, JDK, OpenOffice, SWFTools, and ImageMagick.

1. Download one of the following installation files:

   `alfresco-enterprise-3.4.2-installer-linux-x64.bin`

   This Alfresco setup wizard is for 64-bit systems.
2. Execute the downloaded file.

   The setup wizard starts.
3. In the **Setup - Alfresco Enterprise** window, click **Next**.
4. In the **Installation type** window, choose how you want to use the setup wizard.

   There are two types of installation in the setup wizard:

Options	Description
Easy	Easy type installs Alfresco using the default options and configuration. This install type requires only two fields: install location and and admin password. Choose this route to install Alfresco with the default environment. If you have previously installed Alfresco and the server is running, when you run this installation wizard again, you may be prompted to enter alternative port numbers for the components and services that you install, for example, for the Tomcat application server, FTP port, and the RMI port.
Advanced	Advanced type installs Alfresco but lets you configure the server ports and service properties. You can also choose which additional components to install.

   To complete the **Easy** setup wizard:

   a. Select **Easy**, and then click **Next**.

   b. On the **Installation folder** window, click **Next** to accept the default location.
   c. On the **Admin Password** window, enter a password for the Administrator user (`admin`).
   d. Repeat the password, and then click **Next**.
   e. Click **Next** through the remaining windows in the setup wizard.
   f. Click **Finish** to complete the installation.

      Go to step 14 for information starting and stopping Alfresco.

   To complete the **Advanced** setup wizard, follow the remaining steps in this task, select **Advanced** and then click **Next**.

5. In the **Select Components** window, select the components that you want to install. Deselect the components that you do not want to install.

   You can select from the following components:

   - Java
   - PostgreSQL
   - SharePoint
   - Records Management
   - Web Quick Start
   - Web Project Management (AVM)
   - Quickr Connector Support
   - OpenOffice

   You cannot deselect the Alfresco component because it is installed by default.

6. When you have finished selecting the components, click **Next**.
7. In the **Installation folder** window, click **Next** to accept the default location.

   For example, the default location is `/opt/alfresco`.

   Alternatively, click the icon to choose another location.
8. The **Database Server Parameters** window prompts you to enter a port number for your database.
9. In the **Tomcat Port Configuration** window, enter the following Tomcat configuration parameters:
   a. Web Server Domain

      For example, the default is 127.0.0.1.
   b. Tomcat port

      For example, the default is 8080.
   c. Tomcat Shutdown port

      For example, the default is 8005.
   d. Tomcat SSL Port

      For example, the default is 8443.
   e. Tomcat AJP Port

      For example, the default is 8009.
10. In the **Alfresco FTP Port** window, enter a port number for the Alfresco FTP server.
11. In the **Alfresco RMI Port** window, enter a port number for the RMI service.

12. In the **Admin Password** window, type a password. Repeat the password, and then click **Next**.

    This sets the password for the Alfresco Administrator user account (`admin`).
13. (Optional) If you are installing SharePoint Protocol Support, the **Alfresco SharePoint Port** window displays. Enter a port number, and then click **Next**.
14. (Optional) If you are installing the Quickr Connector Support component, the **Quickr Content Services** window displays. Enter the host and port details for your Quickr server, and then click **Next**.

    For example, the default is localhost and port number 6060. These settings are added to the Quickr configuration file.
15. (Optional) If you are installing the OpenOffice component, the **OpenOffice Server Port** window displays. Enter a port number on which the OpenOffice server will listen.
16. On the **Service Startup Configuration** window, you are presented with two options for starting up the Alfresco services.

Options	Description
Manual	Sets the services to be started manually.
Auto	Sets the services to start up automatically when you start your machine.

    Select the services start up option, and then click **Next**.
17. In the **Ready to Install** window, click **Next**.

    The **Installing** window displays, showing the progress of the installation.
18. In the **Completing the Alfresco Enterprise Setup Wizard** window, click **Finish**.

    By default, when you click **Finish**, the Readme file displays. Click **OK**.

    The Alfresco server starts and Alfresco Share launches in your default browser. If you do not want to view the Readme file, deselect the checkbox. Also, if you do not want to start Alfresco at this point, deselect the **Launch Alfresco Enterprise Share now?** checkbox.
19. Log on to Alfresco Share as the `admin` user. Enter the password that you specified in the **Admin Password** window.

    The Alfresco server is launched automatically as a service called `alfresco`. This service comprises the following individual services:

    - `postgresql`
    - `tomcat`

    If you did not automatically launch Alfresco at the end of the setup wizard, to start Alfresco, you need to start all the services.
20. Manually start the Alfresco server:

    ```
    service alfresco start
    ```

    To start only the `tomcat` service:

    ```
    service alfresco start tomcat
    ```
21. To fully stop Alfresco, you must stop all the services:

    ```
    service alfresco stop
    ```

Installing Alfresco on Windows

The setup wizard for Microsoft Windows installs all the software and components that you require for running Alfresco. This setup wizard installs Alfresco and additional software, including a Tomcat application server, PostgreSQL database, JDK, OpenOffice, SWFTools, and ImageMagick.

1. Download one of the following installation files:

   `alfresco-enterprise-3.4.2-installer-win-x32.exe`

   `alfresco-enterprise-3.4.2-installer-win-x64.exe`

   There are two versions of the Alfresco installation wizard: one for 32-bit systems, and the other for 64-bit systems. The 32-bit installation wizard is not suitable for use on 64-bit environments.
2. Double-click the downloaded file.
3. In the **Setup - Alfresco Enterprise** window, click **Next**.
4. In the **Installation type** window, choose how you want to use the setup wizard.

   There are two types of installation in the setup wizard:

Options	Description
Easy	Easy type installs Alfresco using the default options and configuration. This install type requires only two fields: install location and and admin password. Choose this route to install Alfresco with the default environment. ✎ If you have previously installed Alfresco and the server is running, when you run this installation wizard again, you may be prompted to enter alternative port numbers for the components and services that you install, for example, for the Tomcat application server, FTP port, and the RMI port.
Advanced	Advanced type installs Alfresco but lets you configure the server ports and service properties. You can also choose which additional components to install.

   To complete the **Easy** setup wizard:

   a. Select **Easy**, and then click **Next**.
   b. On the **Installation folder** window, click **Next** to accept the default location.
   c. On the **Admin Password** window, enter a password for the Administrator user (`admin`).
   d. Repeat the password, and then click **Next**.
   e. Click **Next** through the remaining windows in the setup wizard.
   f. Click **Finish** to complete the installation.

      Go to step 14 for information starting and stopping Alfresco.

   To complete the **Advanced** setup wizard, follow the remaining steps in this task, select **Advanced** and then click **Next**.

5. In the **Select Components** window, select the components that you want to install. Deselect the components that you do not want to install.

   You can select from the following components:

   - Java
   - PostgreSQL
   - SharePoint
   - Records Management
   - Web Quick Start
   - Web Project Management (AVM)
   - Quickr Connector Support
   - OpenOffice

   You cannot deselect the Alfresco component because it is installed by default.
6. When you have finished selecting the components, click **Next**.
7. In the **Installation folder** window, click **Next** to accept the default location.

   For example, the default location is `C:\Alfresco`.

   Alternatively, click the icon to choose another location.
8. The **Database Server Parameters** window prompts you to enter a port number for your database.
9. In the **Tomcat Port Configuration** window, enter the following Tomcat configuration parameters:
   a. Web Server Domain

      For example, the default is 127.0.0.1.

   b. Tomcat port

      For example, the default is 8080.

   c. Tomcat Shutdown port

      For example, the default is 8005.

   d. Tomcat SSL Port

      For example, the default is 8443.

   e. Tomcat AJP Port

      For example, the default is 8009.
10. In the **Alfresco FTP Port** window, enter a port number for the Alfresco FTP server.
11. In the **Alfresco RMI Port** window, enter a port number for the RMI service.
12. In the **Admin Password** window, enter a password. Repeat the password, and then click **Next**.

    This sets the password for the Alfresco Administrator user account (`admin`).
13. (Optional) If you are installing SharePoint Protocol Support, the **Alfresco SharePoint Port** window displays. Enter a port number, and then click **Next**.
14. (Optional) If you are installing the Quickr Connector Support component, the **Quickr Content Services** window displays. Enter the host and port details for your Quickr server, and then click **Next**.

    For example, the default is localhost and port number 6060. These settings are added to the Quickr configuration file.

15. (Optional) If you are installing the OpenOffice component, the **OpenOffice Server Port** window displays. Enter a port number on which the OpenOffice server will listen.
16. On the **Service Startup Configuration** window, you are presented with two options for starting up the Alfresco services.

Options	Description
Manual	Sets the services to be started manually.
Auto	Sets the services to start up automatically when you start your machine.

    Select the services start up option, and then click **Next**.
17. In the **Ready to Install** window, click **Next**.

    The **Installing** window displays, showing the progress of the installation.
18. In the **Completing the Alfresco Enterprise Setup Wizard** window, click **Finish**.

    By default, when you click **Finish**, the Readme file displays. Click **OK**.

    The Alfresco server starts and Alfresco Share launches in your default browser. If you do not want to view the Readme file, deselect the checkbox. Also, if you do not want to start Alfresco at this point, deselect the **Launch Alfresco Enterprise Share now?** checkbox.
19. Log on to Alfresco Share as the `admin` user. Enter the password that you specified in the **Admin Password** window.

    The Alfresco server is launched automatically as a Windows service. To manage the server, open the Control Panel **Services** window. The services that will be running for an Alfresco install using the default options are:

    - `alfrescoPostgreSQL`
    - `alfrescoTomcat`

    If you did not automatically launch Alfresco at the end of the installation wizard, to start Alfresco, you need to start all the services. Use the `servicerun start` script in the installation directory or select **All Programs > Alfresco Enterprise > Alfresco Enterprise Service > Start Alfresco Enterprise Service**.
20. To fully stop Alfresco, you must stop all the services. Use the scripts in the installation directory to start or stop the services: `servicerun start` and `servicerun stop`.

Installing Alfresco

This section provides information for installing Alfresco.

Depending on your system, you can install Alfresco using one of the following methods:

- Using an installation wizard, which contains the required software and components you need
- Using a standard WAR file to deploy on an existing application server

System paths

The following standard conventions describe common system paths:

- Explicit Windows paths use back slashes

  `C:\Adirectory`

- Explicit Linux paths use forward slashes

  `/srv/adirectory`
- Back slashes also indicate the same path can apply in both Windows or Linux environments

  `\adirectory\`

Alfresco installation location

The Alfresco installation directory is referenced throughout this guide as `<installLocation>`.

`<classpathRoot>` directory (Windows)

The `<classpathRoot>` denotes a directory whose contents are automatically added to the start of your application server's classpath. The location of this directory varies depending on your application server. For example:

- (Tomcat) `C:\Alfresco\tomcat\shared\classes`
- (JBoss) `C:\jboss\server\default\conf`
- (WebLogic) `C:\bea\user_projects\domains\alf_domain`

  The path can be anywhere on the WebLogic classpath.

`<classpathRoot>` directory (Linux)

The `<classpathRoot>` denotes a directory whose contents are automatically added to the start of your application server's classpath. The location of this directory varies depending on your application server. For example:

- (Tomcat) `tomcat/shared/classes/`
- (JBoss) `/jboss/server/default/conf`
- (WebLogic) `<bea>/user_projects/domains/alf_domain`

  The path can be anywhere on the WebLogic classpath.

`alfresco-global.properties` file

The `alfresco-global.properties` file is where you store all the configuration settings for your environment. The file is in Java properties format, so backslashes must be escaped. The file should be placed in `<classpathRoot>`. When you install Alfresco using the installer, an `alfresco-global.properties` file is created, which contains the settings that you specified in the wizard. A `alfresco-global.properties.sample` file is supplied with the installer and also with the WAR bundle. This `.sample` file contains examples of common settings that you can copy into your `alfresco-global.properties` file.

`<extension>` directory

The `<extension>` directory is where you store Spring configuration files that extend and override the system configuration. This directory can be found at `<classpathRoot>\alfresco\extension`.

`<web-extension>`

The <web-extension> directory is where you store Spring configurations that extend and override the system Share configuration. This directory can be found at `<classpathRoot>\alfresco\extension`.

`<configRoot>`

The `<configRoot>` directory is where the default configuration files are stored. For example, for Tomcat, `<configRoot>` is `<TOMCAT_HOME>\webapps\alfresco\WEB-INF`.

`<configRootShare>`

The `<configRootShare>` directory is where the default configuration files for Share are stored. For example, for Tomcat, `<configRootShare>` is `<TOMCAT_HOME>\webapps\share\WEB-INF`.

Production environment checklist

This section provides a check list for validating the architecture on which Alfresco will run and also for validating the production environment prior to installing Alfresco.

Validating the architecture

This section describes the steps required to validate the architecture to ensure that it meets the prerequisites for an Alfresco installation.

1. Check the supported stacks list.

   Validate that your environment is on the supported stacks list on http://www.alfresco.com.
2. Validate and optimize the hardware (I/O subsystems and CPU) settings.
   a. Optimize the following I/O, in this order of priority:

      - I/O to the relational database that Alfresco is configured to use.
      - I/O to the disk subsystem on which the Lucene indexes are stored.
      - I/O to the disk subsystem on which the content is stored.

      I/O is one of the main factors that influence Alfresco performance. In each case, the goal is to minimize the latency (response time) between Alfresco and the storage system, while also maximizing bandwidth. Low latency is particularly important for database I/O, and one rudimentary test of this is to ping the database server from the Alfresco server. Round trip times greater than 1ms indicate a suboptimal network topology or configuration that will adversely impact Alfresco performance. “Jitter” (highly variable round trip times) is also of concern, as that will increase the variability of Alfresco’s performance. The standard deviation for round trip times should be less than 0.1ms.
   b. Ensure that your system has a clock speed of greater than 2.5Ghz.

      For production use, this clock speed will ensure reasonable response times to the end user. Alfresco Enterprise 3.x and later versions have been tested on 64-bit CPU architectures, primarily because it allows the JVM to use more memory (RAM) that the earlier 32-bit CPU architecture.

      CPU clock speed is of particular concern for the Sun UltraSPARC architecture, as some current UltraSPARC based servers ship with CPUs that have clock speeds as low as 900Mhz, well below what is required for adequate Alfresco performance. If you intend to use Sun servers for hosting Alfresco, ensure that all CPUs have a clock speed of at least 2.5Ghz.

      This implies that:

      - An X or M class Sun server is required, with careful CPU selection to ensure 2.5Ghz (or better) clock speed.
      - T class servers should not be used, as they do not support CPUs faster than approximately 2Ghz. Alfresco is unable to provide specific

guidance on Sun server classes, models, or configurations, so you should talk with your Sun reseller to confirm that minimum CPU clock speed recommendations will be met.

3. Validate the database.

   Alfresco does not provide technical support for maintaining or tuning your relational database. Ensure that your project has access to a certified database administrator (DBA) to support your Alfresco installation.

   Regular maintenance and tuning of the Alfresco database is necessary. Specifically, all of the database servers that Alfresco supports require at the very least that some form of index statistics maintenance be performed at frequent, regular intervals to maintian optimal Alfresco performance.

   Index maintenance can have a severe impact on Alfresco performance while in progress, hence it needs to be discussed with your project team and scheduled appropriately.

4. Validate the Operating System.
   a. Ensure that your chosen OS has been officially certified for use with Alfresco (refer to the Supported Stacks list for details).
   b. Alfresco recommends that a 64-bit OS is used. See the Supported Stacks list for information on the exceptions.

5. Validate and tune the JVM.

   Ensure that your chosen JDK-enabled Java Virtual Machine has been officially certified for use with Alfresco (refer to the Supported Stacks list for details).

   For information on configuring and tuning the JVM, refer to Tuning the JVM on page 140.

   Alfresco requires an official Sun JDK. Other JVMs (including OpenJDK, Harmony, gcj, JRockit, IBM, HP, and so on) are not supported. Alfresco recommends using a 64-bit Sun JVM if the underlying platform (operating system and hardware) is 64-bit capable.

Validating the environment

The following environment-specific items must be validated prior to installing Alfresco.

An Environment Validation tool is also available that can validate most of the following requirements. This tool is available from the Alfresco Support Portal in **Online Resources > Knowledge base** http://support.alfresco.com.

1. Validate that the host name of the server can be resolved in DNS.

   This is required if Alfresco is going to be configured in a cluster.

2. Validate that the user Alfresco will run as can open sufficient file descriptors (4096 or more).

3. Validate that the ports on which Alfresco listens are available:

   The ports listed in the following table are the defaults. If you are planning to reconfigure Alfresco to use different ports, or wish to enable additional protocols (such as HTTPS, SMTP, IMAP or NFS), update this list with those port numbers.

Protocol	Port number	Notes
FTP	TCP 21	On Unix-like operating systems that offer so-called “privileged ports”, Alfresco will normally be unable to bind to this port, unless it is run as the root user (which is not recommended). In this case, even if this port is available, Alfresco will still fail to bind to it, however for FTP services, this is a non-fatal error. The Alfresco FTP functionality will be disabled in the repository.
SMTP	TCP 25	SMTP is not enabled by default.
SMB/NetBT:	UDP 137,138	
SMB/NetBT:	TCP 139,445	On Unix-like operating systems that offer so#called “privileged ports”, Alfresco will normally be unable to bind to this port, unless it is run as the root user (which is not recommended). In this case, even if this port is available, Alfresco will still fail to bind to it, however for CIFS services, this is a non-fatal error. The Alfresco CIFS functionality will be disabled in the repository.
IMAP	TCP 143	IMAP is not enabled by default.
SharePoint Protocol	TCP 7070	This port is only required if you install support for the SharePoint Protocol.
Tomcat Administration	TCP 8005	
HTTP	TCP 8080	
RMI	TCP 50500	

4. Validate that the installed JVM is Sun version 1.6.
5. Validate that the directory in which the JVM is installed does not contain spaces.
6. Validate that the directory in which Alfresco is installed does not contain spaces.
7. Validate that the directory Alfresco will use for the repository (typically called `alf_data`) is both readable and writeable by the operating system user that the Alfresco process will run as.
8. Validate that you can connect to the database as the Alfresco database user, from the Alfresco server.

   Ensure that you install the database vendor's client tools on the Alfresco server.
9. Validate that the character encoding for the Alfresco database is UTF-8.
10. (MySQL only) Validate that the storage engine for the Alfresco database is InnoDB.
11. Validate that the following third-party software is installed and the correct versions:

   a. OpenOffice v3.1 or newer
   b. ImageMagick v6.2 or newer
12. (RHEL and Solaris only) Validate that OpenOffice is able to run in headless mode.

Installation files

There are a number of different installation files available to you, each of which you can choose depending on what is already installed on your system.

The installation wizards install all the components you need for running Alfresco and ensure that you have all the recommended software installed and that configurations are set. When you install Alfresco using the installation wizards, it runs within an instance of the Tomcat application server.

If you wish to install Alfresco within an existing Tomcat or another application server, use the Alfresco WAR file. If you use the WAR file to install Alfresco, you must install the required additional components manually.

The following tables help you to determine what files to download and install.

Alfresco installation wizards

The installation wizards include the full Alfresco install with DM, Explorer, Share, WCM, JDK, OpenOffice, and SharePoint Protocol Support functionality, Records Management, Web Editor, Web Quick Start, and Quickr Connector Support. Use this file if no Alfresco component is installed on your system.

Description	File name
Installation wizard for **Windows**	`alfresco-enterprise-3.4.2-installer-win-x32.exe` (32 bit) `alfresco-enterprise-3.4.2-installer-win-x64.exe` (64 bit) There are two versions of the Alfresco installation wizard for Windows: one for 32-bit systems, and the other for 64-bit systems. The 32-bit installation wizard is not suitable for use on 64-bit environments.
Installation wizard for **Linux**	`alfresco-enterprise-3.4.2-installer-linux-x64.bin` (64 bit) The Alfresco installation wizard for Linux systems is for for 64-bit systems. It is not suitable for use on 32-bit environments. The Linux executable files are graphical installers, but you can also run these files to install Alfresco using text mode. Text mode is a keyboard-based installation method. Run the command with the `--mode text` option.

Alfresco WAR

Description	File name
Alfresco WAR files for manual install into existing application servers or for upgrades to existing Alfresco installations. Includes sample extension files, such as `alfresco-global.properties`. This file also contains Module Management tool and JCR benchmarking tool.	`alfresco-enterprise-3.4.2.zip`

SharePoint Protocol Support

Description	File name
Microsoft SharePoint Protocol Support functionality, which includes the `vti-module.amp` file	`alfresco-enterprise-spp-3.4.2.zip`

Alfresco WCM

Description	File name
Web Quick Start installation files	`alfresco-enterprise-wcmqs-3.4.2.zip`
Alfresco Web Editor installation files	`alfresco-enterprise-webeditor-3.4.2.zip`
WCM installation file for adding WCM functionality (AVM) to an Alfresco Enterprise install, which includes example forms and web pages	`alfresco-enterprise-avm-3.4.2.zip`
Deployment receiver installation file for Windows	`alfresco-enterprise-deployment-3.4.2-win.exe`
Deployment receiver installation file for All platforms	`alfresco-enterprise-deployment-3.4.2-linux.bin`
Forms developer kit	`alfresco-enterprise-fdk-3.4.2.zip`

Microsoft Office Add-ins

Description	File name
Microsoft Office 2003 add-ins zip, which includes the individual add-in zips for Microsoft Excel, PowerPoint, and Word.	`alfresco-enterprise-office-addins-3.4.2.zip`
Add-in for Microsoft Excel 2003	`alfresco-enterprise-excel2003-addin-3.4.2.zip`
Add-in for Microsoft PowerPoint 2003	`alfresco-enterprise-powerpoint2003-addin-3.4.2.zip`
Add-in for Microsoft Word 2003	`alfresco-enterprise-word2003-addin-3.4.2.zip`

Alfresco Records Management

Description	File name
Records Management zip, which includes the required core and Share AMPs	`alfresco-enterprise-dod5015-3.4.2.zip`
Records Management AMP file for core functionality	`alfresco-enterprise-dod5015-3.4.2.amp`

Description	File name
Records Management AMP file for Share functionality	`alfresco-enterprise-dod5015-share-3.4.2.amp`

Alfresco SDK AND APIs

Description	File name
Alfresco Software Development Kit, including the source files (zipped)	`alfresco-enterprise-sdk-3.4.2.zip`

Alfresco Web Service client

Description	File name
WSDL-based API providing standard remote access to the Alfresco repository	`alfresco-web-service-client-3.4.2.zip`

Downloading Enterprise installation files

This section describes the location of the Enterprise installation files that are available for download.

1. Browse to the Alfresco Support Portal at http://support.alfresco.com.
2. At the Login prompt, enter your user name and password.
3. Click **Online Resources**.
4. Click **Downloads**.
5. Browse for the required file from the Alfresco version. Click **More...** for the full list of files available for download.
6. Select the installation file.
7. Click **OK** to download the file to your system.

Refer to the relevant section in this guide for installation instructions.

Supported stacks

The supported stacks are the combinations of operating systems, databases, and application servers that are tested and certified for Alfresco. For the latest list, please refer to the **Supported Stacks** page on the Alfresco Support Portal at http://support.alfresco.com.

Installing Alfresco on Tomcat

For more complex Alfresco installations or if you wish to use an existing Tomcat application server, you can use the Web Archive (WAR) bundle to install Alfresco on any platform. For this type of installation, you must ensure that the required software is installed on the machine.

Use this method of installing Alfresco if you already have installed a JDK, a supported database, an application server, and the additional Alfresco components.

Software requirements

The following table lists the required software that must be on your system before you manually install Alfresco.

Component	Recommendation
Java SE Development Kit (JDK)	The Sun Microsystems JDK 6 is required. The `JAVA_HOME` environment variable must be set to the location of the JDK installation.
Application server	Alfresco runs within an application server. By default, Alfresco runs within Tomcat. For information on installing Alfresco with other supported application servers, see Installing Alfresco on JBoss on page 31, Installing Alfresco on WebLogic on page 35, or Installing Alfresco on WebSphere on page 38.
Database	Alfresco comes preconfigured with the PostgreSQL database. If you intend to use Alfresco in a production environment, you can use one of the supported databases. For the latest information on supported databases, refer to the Alfresco website. For information on configuring the database settings, refer to Configuring databases on page 114.
OpenOffice.org	Alfresco uses OpenOffice for transforming documents from one format to another, for example, a text file to a PDF file. If you do not install OpenOffice, you will not have access to the transformation functionality. Use the latest (stable) version of OpenOffice.org.
ImageMagick	Alfresco uses ImageMagick to manipulate images for previewing.
Flash Player	Alfresco Share requires Flash Player Version 10.x to upload multiple files and view Flash previews. If you do not install Flash, you see the upload screen for single files. Use the latest (stable) version of Flash Player for your platform.
SWF Tools	Alfresco Share uses the pdf2swf utility for previewing PDF files. If you do not install SWF Tools, you will not see PDF previews, but image previews will still be available.

Installing Tomcat application server

This section describes how to install an instance of Tomcat 6.0.26 manually and modify it to use the correct directory structure and files for Alfresco.

These steps describe the installation directory for Tomcat as `<TOMCAT-HOME>`.

These instructions recommend that you name the required directories as `shared/classes` and `shared/lib` because these are the path names used within full Alfresco installations. You can substitute alternative names for these directories.

1. Download Tomcat version 6.0.26 from http://tomcat.apache.org.
2. Install Tomcat following the instructions included in the release.
3. Create the directories required for an Alfresco installation:
   a. Create the `shared/classes` directory.
   b. Create the `shared/lib` directory.
4. Open the `<TOMCAT-HOME>/conf/catalina.properties` file.
5. Change the value of the `shared.loader=` property to the following:

   ```
   shared.loader=${catalina.base}/shared/classes,${catalina.base}/shared/
   lib/*.jar
   ```

   If you have used alternative names for the directories, you must specify these names in the `shared.loader` property.
6. Copy the JDBC drivers for the database you are using to:

`lib/`

7. Edit the `<TOMCAT_HOME>/conf/server.xml` file.
8. Set the character encoding to UTF-8 on the Tomcat connector.

   By default, Tomcat uses ISO-8859-1 character encoding when decoding URLs that are received from a browser. This may cause problems when creating, uploading, and renaming files with international characters.

   Locate the `Connector` section, and then add the `URIEncoding="UTF-8"` property.

   ```
   <Connector port="80" protocol="HTTP/1.1" URIEncoding="UTF-8"
                  connectionTimeout="20000"
                  redirectPort="8443" />
   ```
9. Save the `server.xml` file.

Configuration settings for using MySQL with Alfresco

This section describes how to configure your MySQL instance to work with Alfresco. The following table represents the specific settings in the MySQL configuration wizard that enable MySQL to work effectively with Alfresco.

Configuration wizard dialog	Setting for Alfresco
Server Type	Choose **Dedicated MySQL Server Machine**. The option selected determines the memory allocation.
Database usage	Choose **Transactional Database Only**. This creates a database that uses InnoDB as its storage engine.
InnoDB Tablespace	Accept the default drive and path.
Concurrent Connections	Select **Decision Support (DSS) OLAP**. This sets the approximate number of concurrent connections to the server.
Networking and Strict Mode Options	Accept the default networking options (**Enable TCP/IP Networking**, **Port Number 3306**), and the default server SQL mode (**Enable Strict Mode**).
Character Set	Select **Best Support for Multilingualism**. This sets the default character set to be UTF-8 (set in `character-set-server`).
Security Options	Select **Modify Security Settings**. Type the root password `admin`, then retype the password.

For MySQL 5.5 installations, you also need to modify the `my.ini` and `my.cnf` configuration files.

Installing the Alfresco WAR

A WAR file is a JAR file used to distribute a collection of files (JavaServer Pages, servlets, Java classes, XML files, tag libraries, and static Web pages) that together constitute a web application.

Use this method of installing if you already have installed a JDK, a supported database, an application server, and the additional Alfresco components.

The Alfresco WAR file is a bundle file containing the required WAR files, in addition to the additional commands, configuration files, and licenses for a manual installation.

1. Browse to the Alfresco Enterprise download area.
2. Download the following file:

   `alfresco-enterprise-3.4.2.zip`

3. Specify a location for the download.
4. Extract the WAR file.

   The WAR bundle extracts into the following directory structure:

   ```
   bin
   licenses
   web-server
   ```

   The WAR bundle also contains the following file:

   ```
   README.txt
   ```

   The following files are contained within the suggested subdirectories for within the Tomcat application server.

   `/bin`

File name	Description
`alfresco-bm.jar`	The JCR Benchmarking toolkit.
`alfresco-mmt.jar`	The Alfresco Module Management Tool (MMT).
`apply_amps.bat`	Windows batch file for Tomcat application server installs, used to apply all AMP files in the `<installLocation>` directory.
`apply_amps.sh`	Linux script file for Tomcat application server installs, used to apply all AMP files in the `<installLocation>` directory.
`clean_tomcat.bat`	Windows batch file for cleaning out temporary application server files from previous installations.
`clean_tomcat.sh`	Linux script for cleaning out temporary application server files from previous installations.
`Win32NetBIOS.dll`	Required for CIFS.
`Win32NetBIOSx64.dll`	Required for CIFS on 64-bit Windows.
`Win32Utils.dll`	Required for CIFS.
`Win32Utilsx64.dll`	Required for CIFS on 64-bit Windows.

   The `/licenses` directory contains the following structure:

   ```
   3rd-party
   ```

   This directory contains the third-party license files.

   The web-server directory contains the following structure:

   ```
   conf
   lib
   shared
   webapps
   ```

   `/conf`

File name	Description
`catalina.properties`	Used to define property settings for Tomcat.
`context.xml`	Used to define Context element settings for Tomcat for controlling certain behaviors for the application and the JNDI settings.
`server.xml`	Used to define server configuration elements for Tomcat.

   `/lib`

File name	Description
`postgresql-9.0-801.jdbc4`	PostgreSQL database JDBC connector file.

`/shared`

File name	Description
`/classes/alfresco-global.properties.sample`	The global properties file, which is used for Alfresco configuration properties.
`/classes/alfresco`	Contains the Alfresco directory structure for the configuration override files, including the `extension` and `web-extension` directories.

`/webapps`

File name	Description
`alfresco.war`	The Alfresco WAR file.
`share.war`	The Alfresco Share WAR file.

5. Move the `alfresco.war` file and `share.war` files to the appropriate location for your application server.

   For example, for Tomcat, move the `.war` files to the `<TOMCAT_HOME>/webapps` directory.
6. Edit the `/shared/classes.alfresco-global.properties.sample` file with your configuration settings.
7. Save the file without the `.sample` extension.
8. Move the `alfresco-global.properties` file to `<classpathRoot>`.

   For example, `<TOMCAT_HOME>/shared/classes`.

If you deployed previous versions of Alfresco, you must remove any temporary files created by your application server. Use the `clean_tomcat.bat` or `clean_tomcat.sh` command.

Deploying Share into a separate Tomcat instance

This task provides information for running Share in a separate Tomcat instance. These instructions are for Windows deployments, but Linux-based deployments can use the same methods.

1. Install a new Tomcat instance.
2. Modify the `/conf/server.xml` file for the new Tomcat instance as follows:
   a. Change the port number in the line (for example, to 8006):
   ```
   <Server port="8005" shutdown="SHUTDOWN">
   ```
   b. Change the port number in the section (for example, to 8180):
   ```
   <!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
   <Connector port="8080" ....
   ```
3. Move the `share.war` file from the original Tomcat `\webapps` directory to the new Tomcat `/webapps` directory.
4. (Optional) Configure the original Alfresco Tomcat deployment.
5. Start the original Tomcat. You can use Alfresco supplied batch files.
6. Ensure that a copy of the `commons-el.jar` file is in the Share Tomcat `lib` directory.
7. If you are running the Share Tomcat on a separate machine, you must modify the override file in the Share Tomcat `web-extension` directory, as follows:

   a. Open the `share-config-custom.xml` file.
   b. Change any instance of the server and port to the correct name or IP address of the Alfresco server.

      `http://`*`yourserver`*`:8080`
   c. Save the file without the `.sample` extension.
8. Start the new Share Tomcat. You can use copies of the Alfresco supplied batch files, or your own methods.

Configuring Alfresco as a Windows service

This section describes how to configure Alfresco as a Windows service in a standard Tomcat installation. To configure Alfresco to run as a Windows service, you need to set up the application server (Tomcat) to run as a Windows service.

Before you start, Alfresco and JDK 6 must be installed on your system.

1. Open a command prompt.
2. To install Alfresco as a Windows service, enter the following commands:

   It is important to use the full path. The commands in this task assume an Alfresco installation at `c:\alfresco`.

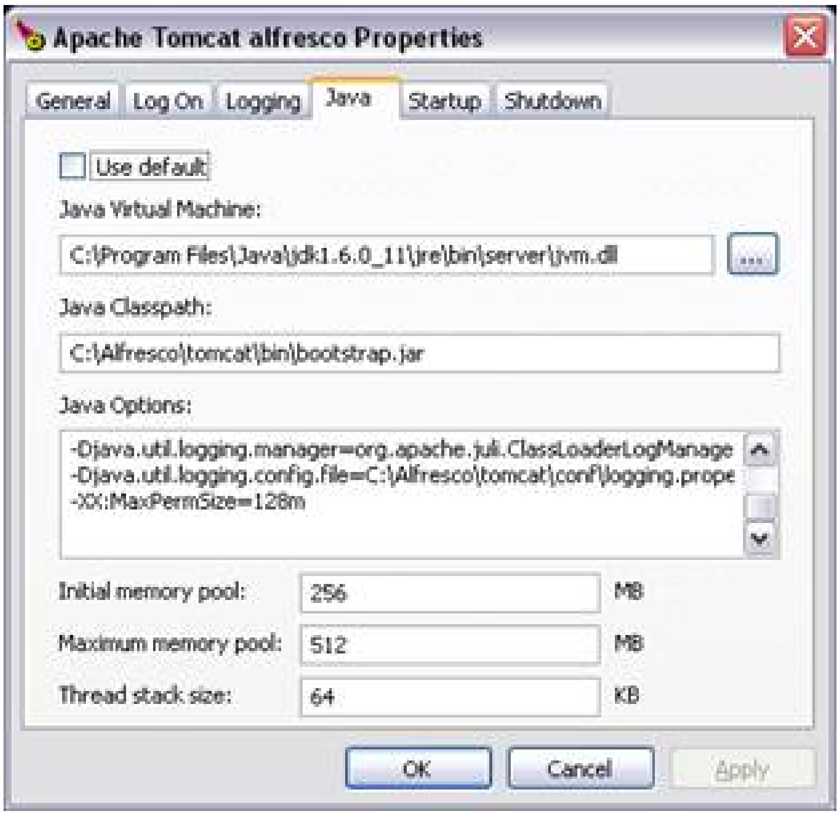
   For Tomcat 6:

```
cd c:\alfresco\tomcat\bin
service.bat install alfresco
tomcat6 //IS//Tomcat6 --DisplayName="Alfresco Server" \
--Install="C:\Program Files\Tomcat\bin\tomcat6.exe" --Jvm=auto \
--StartMode=jvm --StopMode=jvm \
--StartClass=org.apache.catalina.startup.Bootstrap --StartParams=start \
--StopClass=org.apache.catalina.startup.Bootstrap --StopParams=stop
```

3. To edit your service settings, enter the following commands:

   For Tomcat 6:

```
cd c:\alfresco\tomcat\bin
tomcat6w.exe //ES//alfresco
```



Use default

Java Virtual Machine:

C:\Program Files\Java\jdk1.6.0_11\jre\bin\server\jvm.dll

Java Classpath:

C:\Alfresco\tomcat\bin\bootstrap.jar

Java Options:

```
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManage
-Djava.util.logging.config.file=C:\Alfresco\tomcat\conf\logging.prope
-XX:MaxPermSize=128m
```

Initial memory pool: 256 MB

Maximum memory pool: 512 MB

Thread stack size: 64 KB

4. Locate the service named **Alfresco Server** in the Services panel.
5. Start the **Alfresco Server** service.

You can uninstall the service using the following commands:

```
cd c:\alfresco\tomcat\bin
service.bat uninstall alfresco
```

Installing Alfresco on JBoss

You can install and deploy the Alfresco WAR on the JBoss application server.

These instructions provide command line examples for Linux, but can be adapted to Windows.

1. Browse to the Enterprise download area.
2. Download the following file to your local machine:

   `alfresco-enterprise-3.4.2.zip`
3. Extract the file to a temporary directory.

   For example, use a temporary directory called `~/alfrescodist`.

   The commands that you would enter are:

   ```
   mkdir ~/alfrescodist
   tar -C ~/alfrescodist -xzvf ~/alfresco-enterprise-war-3.3.2.tar.gz
   ```
4. Create an alfresco directory under the JBoss configuration directory.

   For example, `/opt/jboss/jboss-5.1.0.GA/server/default/conf/alfresco`.
5. Copy the distribution extension folder to the new directory.

   The commands that you would enter are:

   ```
   mkdir /opt/jboss/jboss-5.1.0.GA/server/default/conf/alfresco
   cp -r ~/alfrescodist/extensions/extension /opt/jboss/jboss-5.1.0.GA/
   server/default/conf/alfresco
   ```
6. Copy the `alfresco-global.properties` sample file to the JBoss configuration directory.

For example, `/opt/jboss/jboss-5.1.0.GA/server/default/conf`.

The command that you would enter is:

```
cp ~/alfrescodist/extensions/extension/alfresco-global.properties /opt/
jboss/jboss-5.1.0.GA/server/default/conf
```

7. Edit the parameters in the `alfresco-global.properties` file to suit your environment.
8. Copy the Alfresco war files to the JBoss deploy directory.

   `For example, /opt/jboss/jboss-5.1.0.GA/server/default/deploy.`

   The commands that you would enter are:

   ```
   cp ~/alfrescodist/alfresco.war /opt/jboss/jboss-5.1.0.GA/server/default/
   deploy
   cp ~/alfrescodist/share.war /opt/jboss/jboss-5.1.0.GA/server/default/
   deploy
   ```

Configuring JBoss for Alfresco

This section describes how to configure an Alfresco installation on JBoss.

1. Configure the database. This example assumes you are using a MySQL database.
   a. Create a new empty database schema instance called `alfresco` in MySQL -

      Use the example files in `~/alfrescodist/extra/databases/mysql` to perform this with the correct user permissions.
   b. Download the MySQL JDBC driver file from the MySQL website.
   c. Extract the MySQL JDBC driver `.jar` file and copy to `/opt/jboss/jboss-5.1.0.GA/server/default/lib`.
   d. Create a datasource that defines the connection details for your MySQL database by copying `/opt/jboss/jboss-5.1.0.GA/docs/examples/jca/mysql-ds.xml` to `/opt/jboss/jboss-5.1.0.GA/server/default/deploy` and editing with the parameters appropriate for your database.

      The `jndi-name` must be changed to `alfresco-datasource` to match up with the `alfresco.war`.

      For example:

      ```
      <local-tx-datasource>
         <jndi-name>alfresco-datasource</jndi-name>
         <connection-url>jdbc:mysql://localhost:3306/alfresco</connection-
      url>?useUnicode=yes&characterEncoding=UTF-8
         <driver-class>org.gjt.mm.mysql.Driver</driver-class>
         <user-name>alfresco</user-name>
         <password>alfresco</password>
         <exception-sorter-class-
      name>org.jboss.resource.adapter.jdbc.vendor.MySQLExceptionSorter</
      exception-sorter-class-name>
         <metadata>
            <type-mapping>mySQL</type-mapping>
         </metadata>
       </local-tx-datasource>
      ```
2. Configure UTF-8 support.
   a. Edit the following files:

      - `/opt/jboss/jboss-5.1.0.GA/server/default/deploy/jbossweb.sar/server.xml`
      - `/opt/jboss/jboss-5.1.0.GA/server/all/deploy/jbossweb.sar/server.xml`

b. Add `URIEncoding="UTF-8"` to the following section:

```
<Connector port="8080" address="${jboss.bind.address}"
        maxThreads="250" maxHttpHeaderSize="8192" />
```

For example:

```
<Connector port="8080" URIEncoding="UTF-8"
 address="${jboss.bind.address}"
        maxThreads="250" maxHttpHeaderSize="8192" />
```

or

```
<Connector protocol="HTTP/1.1" port="8080" URIEncoding="UTF-8"
 address="${jboss.bind.address}"
        connectionTimeout="20000" redirectPort="8443" />
```

3. Configure logging.

   a. Edit the /opt/jboss/jboss-5.1.0.GA/server/default/conf/jboss-log4j.xml file to reduce the huge debug log output.

   For example:

```
<root>
     <priority value="INFO" />
     <appender-ref ref="CONSOLE"/>
     <appender-ref ref="FILE"/>
  </root>
```

   b. (Optional) The logging configuration that is set reduces the debug output but there will still be a lot of output sent to the console. To reduce it further, adding the following to the `/opt/jboss/jboss-5.1.0.GA/server/default/conf/jboss-log4j.xml` file:

```
 <category name="org.jboss.logging.Log4jService$URLWatchTimerTask">
     <priority value="INFO"/>
  </category>
  <category name="org.jboss.system.server.Server">
     <priority value="INFO"/>
  </category>
  <category name="org.jboss">
     <priority value="WARN"/>
  </category>
  <category name="net">
     <priority value="WARN"/>
  </category>
  <category name="org.alfresco">
     <priority value="WARN"/>
  </category>
  <category name="org.alfresco.repo.policy">
     <priority value="WARN"/>
  </category>
  <category name="org.springframework">
     <priority value="WARN"/>
  </category>
  <category name="org.hibernate">
     <priority value="WARN"/>
  </category>
  <category name="org.hibernate.cache.ReadWriteCache">
     <priority value="ERROR"/>
  </category>
  <category name="org.hibernate.cache.EhCacheProvider">
     <priority value="ERROR"/>
  </category>
  <category
 name="org.hibernate.engine.StatefulPersistenceContext.ProxyWarnLog">
     <priority value="ERROR"/>
  </category>
  <category name="org.apache.myfaces">
     <priority value="ERROR"/>
  </category>
  <category name="org.jbpm.jpdl.xml.JpdlXmlReader">
     <priority value="ERROR"/>
  </category>
```

4. Configure Hibernate.

   a. Edit the `/opt/jboss/jboss-5.1.0.GA/server/default/deployers/ejb3.deployer/META-INF/jpa-deployers-jboss-beans.xml` file so that a value of `cglib` is specified for the `hibernate.bytecode.provider` key.

      For example:

```
<entry>
  <key>hibernate.bytecode.provider</key>
  <value>cglib</value>
</entry>
```

5. Configure the JVM options.

   a. Ensure that the /opt/jboss/jboss-5.1.0.GA/bin/run.sh file specifies appropriate JVM memory settings in JAVA_OPTS.

      For example, the following are minimums:

```
-Xms128m -Xmx512m -XX:MaxPermSize=256m
```

   b. Enable JMX monitoring and automatic discovery of Alfresco by the Hyperic plugin by ensuring that JAVA_OPTS contains the following arguments:

```
-Dcom.sun.management.jmxremote -Dalfresco.home=.
```

   c. Open the `/opt/jboss/jboss-5.1.0.GA/server/default/deployers/jbossweb.deployer/META-INF/war-deployers-jboss-beans.xml` file, and then edit the `filteredPackages` property of the `WarClassLoaderDeployer` bean. Add the following filtered packages.

```
<bean name="WarClassLoaderDeployer"
 class="org.jboss.web.tomcat.service.deployers.WarClassLoaderDeployer">
     <property name="relativeOrder">-1</property>
     <property
 name="filteredPackages">javax.activation,javax.servlet,javax.servlet.jsp,
javax.servlet.jsp.jstl,javax.servlet.jsp.jstl.core,javax.servlet.jsp.jstl.fmt,
javax.servlet.jsp.jstl.sql,javax.servlet.jsp.jstl.tlv,javax.xml,
javax.xml.bind,javax.xml.bind.annotation,javax.xml.bind.annotation.adapters,
javax.xml.bind.attachment,javax.xml.bind.helpers,javax.xml.bind.util,javax.xml
javax.xml.crypto.dom,javax.xml.crypto.dsig,javax.xml.crypto.dsig.dom,javax.xml
javax.xml.crypto.dsig.spec,javax.xml.datatype,javax.xml.messaging,
javax.xml.namespace,javax.xml.parsers,javax.xml.rpc,javax.xml.rpc.encoding,
javax.xml.rpc.handler,javax.xml.rpc.handler.soap,javax.xml.rpc.holders,
javax.xml.rpc.server,javax.xml.rpc.soap,javax.xml.soap,javax.xml.stream,
javax.xml.stream.events,javax.xml.stream.util,javax.xml.transform,
javax.xml.transform.dom,javax.xml.transform.sax,javax.xml.transform.stream,
javax.xml.validation,javax.xml.ws,javax.xml.ws.handler,javax.xml.ws.handler.so
javax.xml.ws.http,javax.xml.ws.soap,javax.xml.ws.spi,javax.xml.ws.wsaddressing
javax.xml.xpath,org.apache.commons.logging,org.apache.commons.logging.impl,
org.apache.xerces,org.apache.xerces.dom,org.apache.xerces.dom.events,
org.apache.xerces.dom3,org.apache.xerces.dom3.as,org.apache.xerces.impl,
org.apache.xerces.impl.dtd,org.apache.xerces.impl.dtd.models,org.apache.xerces
org.apache.xerces.impl.dv.dtd,org.apache.xerces.impl.dv.util,
org.apache.xerces.impl.dv.xs,org.apache.xerces.impl.io,org.apache.xerces.impl.
org.apache.xerces.impl.validation,org.apache.xerces.impl.xpath,
org.apache.xerces.impl.xpath.regex,org.apache.xerces.impl.xs,
org.apache.xerces.impl.xs.identity,org.apache.xerces.impl.xs.models,
org.apache.xerces.impl.xs.opti,org.apache.xerces.impl.xs.traversers,
org.apache.xerces.impl.xs.util,org.apache.xerces.jaxp,
org.apache.xerces.jaxp.datatype,org.apache.xerces.jaxp.validation,
org.apache.xerces.parsers,org.apache.xerces.util,org.apache.xerces.xinclude,
org.apache.xerces.xni,org.apache.xerces.xni.grammars,
org.apache.xerces.xni.parser,org.apache.xerces.xpointer,
org.apache.xerces.xs,org.apache.xerces.xs.datatypes,org.apache.xml,
org.apache.xml.resolver,org.apache.xml.resolver.apps,org.apache.xml.resolver.e
org.apache.xml.resolver.etc.catalog.dtd,org.apache.xml.resolver.etc.catalog.rn
org.apache.xml.resolver.etc.catalog.xsd,org.apache.xml.resolver.etc.xcatalog.d
org.apache.xml.resolver.helpers,org.apache.xml.resolver.readers,
org.apache.xml.resolver.tools,org.apache.xml.security,
org.apache.xml.security.algorithms,org.apache.xml.security.algorithms.implemen
org.apache.xml.security.c14n,org.apache.xml.security.c14n.helper,
org.apache.xml.security.c14n.implementations,org.apache.xml.security.encryptio
org.apache.xml.security.exceptions,org.apache.xml.security.keys,
org.apache.xml.security.keys.content,org.apache.xml.security.keys.content.keyv
org.apache.xml.security.keys.content.x509,org.apache.xml.security.keys.keyreso
org.apache.xml.security.keys.keyresolver.implementations,
org.apache.xml.security.keys.storage,org.apache.xml.security.keys.storage.impl
org.apache.xml.security.resource,org.apache.xml.security.resource.schema,
org.apache.xml.security.signature,org.apache.xml.security.transforms,
org.apache.xml.security.transforms.implementations,
org.apache.xml.security.transforms.params,org.apache.xml.security.utils,
org.apache.xml.security.utils.resolver,org.apache.xml.security.utils.resolver.
org.apache.xml.serialize,org.apache.xmlcommons,org.xml,org.xml.sax,org.xml.sax
org.xml.sax.helpers,org.w3c.css,org.w3c.css.sac,org.w3c.css.sac.helpers,
org.w3c.dom,org.w3c.dom.bootstrap,org.w3c.dom.css,org.w3c.dom.events,
org.w3c.dom.html,org.w3c.dom.ls,org.w3c.dom.ranges,org.w3c.dom.smil,
org.w3c.dom.stylesheets,org.w3c.dom.svg,org.w3c.dom.traversal,
org.w3c.dom.views,org.w3c.dom.xpath</property>
  </bean>
```

This avoids collisions between the JVM bootstrap classes and those embedded in the war.

6. Execute the `/opt/jboss/jboss-5.1.0.GA/bin/run.sh` file.

   By default JBoss will only listen on the `localhost` network adapter, rather than the adapter with a real IP address connected to the outside world. To override this, start JBoss with the `-b addr` option, specifying the IP address of the network adapter you want to listen on or `0.0.0.0` to listen on all adapters. For example:

   ```
   run.sh -b 0.0.0.0
   ```

   The following warning message will appear in the log but can be ignored, since Alfresco disables the faces RI with a special parameter in web.xml:

   [STDOUT] 16:59:43,814 ERROR [shared_impl.config.MyfacesConfig] Both MyFaces and the RI are on your classpath. Please make sure to use only one of the two JSF-implementations.

7. Start the Alfresco server.

Installing Alfresco on WebLogic

This section describes how to install Alfresco as an Enterprise ARchive format (EAR) into Oracle WebLogic 10.3.

Certain components of Alfresco require access to the EAR file contents as files. These instructions require expanding the `.ear` into exploded format, as described in the WebLogic documentation. The Alfresco WebLogic deployment solution makes use of a Filter Classloader, configured in the `weblogic-application.xml` file, to ensure that the unmodified contents of the Alfresco web module will run in WebLogic.

Before you start:

- Install OpenOffice and ensure that the `ooo.exe` property is set in the the `alfresco-global.properties` file
- Create an `alfresco` database and user with appropriate permissions
- Install WebLogic 10.3 without creating any domains or servers

1. Browse to the Enterprise download area.
2. Download the `alfresco-enterprise-3.4.2.ear` file.
3. Obtain the license (`.lic` file).
4. Create a directory in the WebLogic user's home directory to host the exploded EAR file and copy the `alfresco-enterprise-3.4.2.ear` file to that directory.
5. Run the following commands in the new directory to explode the EAR file:
    a. `mkdir alfresco`
    b. `cd alfresco`
    c. `jar xvf ../alfresco-enterprise-3.4.2.ear`
    d. `mv alfresco.war alfresco.war.tmp`
    e. `mv share.war share.war.tmp`
    f. `mkdir alfresco.war`
    g. `mkdir share.war`
    h. `cd alfresco.war`
    i. `jar xvf ../alfresco.war.tmp`
    j. `cd ../share.war`
    k. `jar xvf ../share.war.tmp`
6. Open the WebLogic Configuration Wizard.

    For example, on Unix, use the following command to create a new domain, `alf_domain`:

    ```
    <Weblogic_HOME>/common/bin/config.sh
    ```
7. Create a directory for the license file.

    For example, in Linux, use the following command:

    ```
    mkdir -p <Weblogic_HOME>/user_projects/domains/alf_domain/alfresco/
    extension/license
    ```
8. Move the license `.lic` file into the `license` directory.
9. In the `<Weblogic_HOME>/user_projects/domains/alf_domain` directory, create the `alfresco-global.properties` file.

    Modify the file in the same way you would for global properties configuration.
10. In the `alfresco-global.properties` file, add the following line:

    ```
    db.pool.statements.enable=false
    ```

    This property setting is required to make the DBCP connection pool work on WebLogic.
11. Move the database JDBC driver `.jar` to the `<Weblogic_HOME>/user_projects/domains/alf_domain/lib` directory.
12. Edit the `<Weblogic Home>/user_projects/domains/alf_domain/config/config.xml` file and add the following before the end of the `</security-configuration>` section:

    ```
    <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-
    credentials>
    ```
13. Open the `<Weblogic Home>/user_projects/domains/alf_domain/bin/setDomainEnv.sh` file, and then edit all of the lines prefixed with `MEM_MAX_PERM_SIZE` to increase the PermGen space.

    ```
    MEM_MAX_PERM_SIZE="-XX:MaxPermSize=256m"
    MEM_MAX_PERM_SIZE_64BIT="-XX:MaxPermSize=512m"
    MEM_MAX_PERM_SIZE_32BIT="-XX:MaxPermSize=256m"
    ```

You may see different combinations of these lines, depending on whether you have installed on a 64 or 32-bit platform.

This setting may need to be increased further, depending on the number of deployed applications.

14. Set the heap size parameter appropriately. The following setting is a recommendation:

    ```
    WLS_MEM_ARGS="-Xmx2048m"
    ```
15. For Weblogic 10.3.2.0, the following extra edit is required to ensure that `alf_domain` is in the global classpath.

    ```
    PRE_CLASSPATH=$WL_HOME/user_projects/domains/alf_domain
    ```
16. Open the `<Weblogic Home>/wlserver_10.3/common/nodemanager/nodemanager.properties` file, and then edit the settings so that the PermGen settings are passed on to the Alfresco server by the node manager.

    ```
    StartScriptEnabled=true
    ```
17. Start the domain admin server.

    For example:

    ```
    <Weblogic_HOME>/user_projects/domains/alf_domain/startWebLogic.sh
    ```
18. Open a web browser and log in to the admin server (for example, at `http://localhost:7001/console`). The default user name and password is `weblogic`.
19. To enable automatic control of your Alfresco server:
    a. Create a machine with the details of the machine running the domain. This will allow the node manager to control servers on that machine.
    b. Create a server called `AlfrescoServer`, within the new machine.

       Note that you have to choose a unique port number. A good port number to choose is 8080 because it is preconfigured in Share. You can leave the host name blank if you want it to listen on all network adapters.
    c. Ensure that the node manager is running (for example, `<Weblogic_HOME>/wlserver_10.3/server/bin/startNodeManager.sh`).

       You will be able to use the admin server **Change Center** panel to start and stop the Alfresco server.

    Refer to the WebLogic documentation to find out how to create a machine and new server within the machine.
20. In the left pane of the Administration Console, click **Deployments**.
21. In the right pane, click **Install**.
22. Using the **Install Application Assistant**, locate the directory of your exploded EAR file (containing the `alfresco.war` and `share.war` directories).
23. Locate the file or directory to install, and then click **Next**.
24. Check **Install this deployment as an application** radio button, and then click **Next**.
25. Click **Finish**.
26. Click **Activate Changes**.
27. Using the **Change Center** panel, restart `AlfrescoServer`.
28. Log in to Alfresco:

    - Alfresco Share at `http://localhost:8080/share`
    - Alfresco Explorer at `http://localhost:8080/alfresco`

If the Alfresco finds a JDBC data source with JNDI path (`java:comp/env/jdbc/dataSource`), it will use that rather than the embedded data source. To set that up in WebLogic you need to define a new global data source, for example, `AlfrescoDataSource`. See the WebLogic documentation for more information. Then, map `AlfrescoDataSource` in to Alfresco by adding the `WEB-INF/weblogic.xml` file into `alfresco.war` containing the following:

```
<! DOCTYPE weblogic-web-app PUBLIC "-//BEA Systems, Inc.//DTD Web
Application 8.1//EN"

"http://www.bea.com/servers/wls810/dtd/weblogic810-web-jar.dtd" >
< weblogic-web-app >
< reference-descriptor >
< resource-description >
< res-ref-name > jdbc /dataSource </ res-ref-name >
< jndi-name > AlfrescoDataSource </ jndi-name >
</ resource-description >
</ reference-descriptor >
</ weblogic-web-app >
```

Installing Alfresco on WebSphere

This section describes how to install Alfresco on WebSphere 7.0.3. These instructions are valid for installing on Windows 2008

Ensure that your WebSphere 7.0.3 installation is updated with all available service packs, including WASSDK (embedded JDK) patches. This is because the Alfresco optimized I/O code requires the very latest patches available from IBM and will not function on an unpatched WebSphere 7 installation.

1. Create a Myfaces v1.1 shared library.

   Because neither of the versions of JSF that ship with WebSphere 7 are compatible with Alfresco, you must define a new isolated shared library in WebSphere that contains a compatible implementation. This is documented in the Configuring JavaServer Faces implementation section of the WebSphere 7 manual. The Alfresco Enterprise `.ear` file embeds an appropriate shared library definition in `META-INF/ibmconfig`, so it is only necessary to prepare WebSphere, as described in this section.

   Obtain the `myfaces1_1-websphere-shared-lib.zip` Enterprise distributable from Alfresco and extract it to the root WebSphere installation directory. This creates a `myfaces1_1` directory containing all the `.jars` required by the `myfaces1_1` shared library on WebSphere. For example, on Windows:

   ```
   cd /d "C:\Program Files\IBM\WebSphere\AppServer"
   java\bin\jar xvf myfaces1_1-websphere-shared-lib.zip
   ```

2. Enable Xalan as the standard JAXP Transformer.

   Copy the file `$WAS_INSTALL_ROOT/java/jre/lib/jaxp.properties.sample` (for example, `C:\Program Files\IBM\WebSphere\AppServer\java\jre\lib\jaxp.properties.sample`) to `$WAS_INSTALL_ROOT/java/jre/lib/jaxp.properties`.

   Edit the `jaxp.properties` file and change the following line: `#javax.xml.transform.TransformerFactory=com.ibm.xtq.xslt.jaxp.compiler.Transformer` to read:

   ```
   javax.xml.transform.TransformerFactory=org.apache.xalan.
   ```

   ```
   processor.TransformerFactoryImpl
   ```

   Also, add the following line:

   ```
   javax.xml.parsers.DocumentBuilderFactory=org.apache.xerces.
   ```

   ```
   jaxp.DocumentBuilderFactoryImpl
   ```

3. Configure Share to point to the WebSphere default HTTP port 9080 (or another number that you wish to specify).

   a. Obtain the `share-config-custom.xml.sample` file and copy it to `$WAS_INSTALL_ROOT/lib/alfresco/web-extension/share-config-custom.xml` (For example, `C:\Program Files\IBM\WebSphere\AppServer\lib\alfresco\web-extension\share-config-custom.xml`).

   b. Uncomment this section by removing the begin comment `<--` and end comment `-->` lines surrounding this section.

```
  <config evaluator="string-compare" condition="Remote">
      <remote>
         <endpoint>
            <id>alfresco-noauth</id>
            <name>Alfresco - unauthenticated access</name>
            <description>Access to Alfresco Repository WebScripts that
 do not require authentication</description>
            <connector-id>alfresco</connector-id>
            <endpoint-url>http://localhost:8080/alfresco/s</endpoint-
url>
            <identity>none</identity>
         </endpoint>

         <endpoint>
            <id>alfresco</id>
            <name>Alfresco - user access</name>
            <description>Access to Alfresco Repository WebScripts that
 require user authentication</description>
            <connector-id>alfresco</connector-id>
            <endpoint-url>http://localhost:8080/alfresco/s</endpoint-
url>
            <identity>user</identity>
         </endpoint>

         <endpoint>
            <id>alfresco-feed</id>
            <name>Alfresco Feed</name>
            <description>Alfresco Feed - supports basic HTTP
 authentication via the EndPointProxyServlet</description>
            <connector-id>http</connector-id>
            <endpoint-url>http://localhost:8080/alfresco/s</endpoint-
url>
            <basic-auth>true</basic-auth>
            <identity>user</identity>
         </endpoint>
      </remote>
   </config>
```

   c. Edit the file, replacing all instances of 8080 with 9080 (or the port number that you specify) and all instances of `yourserver` with localhost (or a different host running Alfresco).

   d. In certain environments, an HTTP request originating from Flash cannot be authenticated using an existing session. For these cases, it is useful to disable the Flash-based uploader for Share Document Libraries.

      To disable the Flash uploader, add the following lines to the Document Library config section:

```
<!-- Document Library config section -->
   <config evaluator="string-compare" condition="DocumentLibrary"
 replace="true">
      <!--
         File upload configuration
      -->
      <file-upload>
         <adobe-flash-enabled>false</adobe-flash-enabled>
```

```
        </file-upload>
    </config>
```

   e. Save the file.

4. Install a license.

   If you have been issued with a `.lic` license file for this version of Alfresco, copy it to a `$WAS_INSTALL_ROOT/lib/alfresco/extension/license` directory (for example, `C:\Program Files\IBM\WebSphere\AppServer\lib\alfresco\extension\license\mylicense.lic`).

5. (Optional) Enable WCM.

   You need the WCM bootstrap context on the class path. Obtain the `wcm-bootstrap-context.xml` file and copy it to the `$WAS_INSTALL_ROOT/lib/alfresco/extension` directory (for example, `C:\Program Files\IBM\WebSphere\AppServer\lib\alfresco\extension`).

6. Define the environment information using the extension classpath mechanism and the `alfresco-global.properties` file.

   a. Download either the `alfresco-enterprise-sample-extensions.tar.gz` file or `alfresco-enterprise-sample-extensions.zip` file and extract it to an empty directory .

   b. From the empty directory, copy the `alfresco-global.properties` file to `$WAS_INSTALL_ROOT/lib (for example, C:\Program Files\IBM\WebSphere\AppServer\lib\alfresco-global.properties).`

   c. Disable the `mbean` server lookup by adding the following line `mbean.server.locateExistingServerIfPossible=false`.

7. Define the database connection information using WebSphere.

   This section makes use of Websphere's built-in connection pooling features with a MySQL database. If you are using another database type or prefer to use the DBCP connection pool built in to Alfresco, jump to the next step.

   a. Log on to the WebSphere Administrative console, typically at http://localhost:9060/ibm/console/.

   b. Expand **Guided Activities** in the top left panel and select **Connecting to a database**.

      Follow each of the steps, supplying the parameters appropriate for your database to define a data source with JNDI name `jdbc/alfresco`.

   c. In the **Configure credentials for secure database access** step, provide the user ID and password to your database account and give it the alias `alfresco`.

   d. In the **Configure a JDBC provider** step, follow the instructions to create a new JDBC provider using the following properties:

      Name
         MySQL JDBC Provider

      Description
         MySQL JDBC Provider

      Class path
         `${MYSQL_JDBC_DRIVER_PATH}/mysql-connector-java-5.0.3-bin.jar`

      Implementation class name
         `com.mysql.jdbc.jdbc2.optional.MysqlConnectionPoolDataSource`

   e. In the **Configure WebSphere variables** step, define a `MYSQL_JDBC_DRIVER_PATH` variable holding the absolute path to the directory containing the MySQL JDBC driver.

f. In the **Configure a data source** step, click the MySQL JDBC Provider and then the **Data sources** link. Select **New** to create a new data source with the following parameters:

   Name
   `alfresco-datasource`

   JNDI name
   `jdbc/alfresco`

g. Select **Use this data source in container managed persistence (CMP)**.

h. Ensure that the generic data store helper (`com.ibm.websphere.rsadapter.GenericDataStoreHelper`) is selected.

i. Select **alfresco** as the component-managed authentication alias.

j. Click **OK** to save the data source.

k. Add the following custom properties:

   databaseName
   `alfresco?autoReconnect=true`

   port
   3306

   serverName
   `localhost`

8. Define the database connection information using Alfresco.

   This step is an alternative method to the previous step for defining the database connection information using WebSphere.

   a. Copy your JDBC driver jar to `${WAS_INSTALL_ROOT}/lib` (for example, `C:\Program Files\IBM\WebSphere\AppServer\lib`).

   b. Uncomment and edit the lines appropriate for your database type in the `alfresco-global.properties` file you set up.

9. Install the EAR file.

   a. Download the `alfresco-enterprise-3.4.2.ear` file.

      This embeds Alfresco Explorer and Share, plus the necessary WebSphere configuration to use the `myfaces1_1` shared library with parent-last loading order.

   b. Log on to the WebSphere Administrative console.

      For example, http://localhost:9060/ibm/console/.

   c. Navigate to **Applications > New Application > New Enterprise Application**.

   d. Browse to `alfresco-enterprise-3.4.2.ear` on the local file system, and then click **Next**.

   e. Select **Detailed - Show all installation options and parameters**, and then click **Next**.

      If you followed the steps to define the database connection information using WebSphere, this maps to the datasource you set up earlier. Otherwise, Alfresco will fall back to the database connection configuration in the `alfresco-global.properties` file. If you want to force Alfresco not to use a WebSphere datasource, enter any invalid path, such as `jdbc/dummy`.

   f. Jump to the **Map resource references to resources** step, which is highlighted with a (**+**).

g. Under **Target Resource JNDI Name**, type `jdbc/alfresco` (the data source you set up earlier), and then click **Next**.

h. Jump to the **Map environment entries for Web modules** step.

i. For `properties/dir.root`, specify an absolute file system path where you would like Alfresco file data to be stored.

   For example, `C:\alf_data`.

j. Leave the Hibernate properties blank, unless you want to override the default behaviour, where they will be auto-detected.

k. Click **Next** and **Finish**.

l. Save your profile changes to the master repository.

m. Restart the WebSphere server.

   Alfresco starts with the WebSphere server.

10. Remove the SQL warning messages from log file.

    WebSphere shows warnings in the log file, similar to the following:

```
[12/7/10 17:24:42:206 EET] 0000003a JDBCException W
 org.hibernate.util.JDBCExceptionReporter logWarnings SQL Warning: 4474,
 SQLState: 01000
[12/7/10 17:24:42:208 EET] 0000003a JDBCException W
 org.hibernate.util.JDBCExceptionReporter logWarnings [jcc][t4][10217]
[10310][4.8.87]
Connection read-only mode is not enforceable after the connection has
 been established.
To enforce a read only connection, set the read-only data source or
 connection property. ERRORCODE=4474, SQLSTATE=01000
```

    The current driver implementation will display these warnings, however, they have no impact on the operation of Alfresco. You can either choose to ignore these warnings, or you can configure the logging to stop them displaying.

    a. Open WebSphere Administrative console.

    b. Navigate to **Troubleshooting > Logs** and **trace- Server - Change Log Detail Levels**.

    c. Search for the `org.hibernate.util.*` component.

    d. Set `org.hibernate.util.JDBCExceptionReporter` class logger - Messages and Trace Levels to `severe` or `fatal`.

11. Log in to Alfresco:

    - Alfresco Share at `http://localhost:9080/share`
    - Alfresco Explorer at `http://localhost:9080/alfresco`

Installing a new license

The Alfresco license file must be installed before you can use Alfresco.

You must have installed Alfresco before you can install the license. This is because you use a license directory within the installed product.

1. Copy the license file to your machine.

   The license file has a file extension of `.lic`.

2. Ensure that the Alfresco server is not running.

3. From your Alfresco installation directory, browse to the `<extension>` directory, for example for Tomcat on Windows, this is:

`C:\Alfresco\tomcat\shared\classes\alfresco\extension`

4. Create the `license` directory.
5. Move the `.lic` file into the `license` directory.

You have installed the Alfresco license file.

When you run Alfresco, the server detects the existence of the `.lic` file and installs your license. If the license is valid, Alfresco renames the file to `<license-name>.lic.INSTALLED` and you can begin to use the terms of your license immediately.

Installing Alfresco components

This section describes how to install components that integrate with Alfresco. Some of these components can be installed any time before or after installing Alfresco.

Installing OpenOffice

Within Alfresco, you can transform a document from one format to another, for example, a text file to a PDF file. To have access to these transformation facilities in Alfresco, you must install OpenOffice. This is optional, and can be done any time after Alfresco is installed.

1. Browse to the OpenOffice.org download site: http://download.openoffice.org
2. Download the latest (stable) version of OpenOffice for your platform.
3. When prompted, specify a download destination.
4. Browse to the location of your downloaded file, and install the application.

   A wizard guides you through the installation.
5. Accept the license agreement, and then click **Next**.
6. Enter Customer information as appropriate, and then click **Next**.
7. Select the set up type and **Custom**, and then click **Next**.
8. Change the installation directory to:
   - (Windows) `c:\Alfresco\OpenOffice`
   - (Linux) `/opt/alfresco/OpenOffice`
9. Optionally, select the files for which you want OpenOffice to be the default application, and then click **Next**.
10. Start one of the OpenOffice programs for the initial registration, and then close the program.
11. Modify the `ooo.exe=` property in the `<classpathRoot>/alfresco-global.properties` file to point to the OpenOffice binary `soffice.exe`.

    For Windows, set the path using the `\\` separator or use the forward slash `/` Unix path separator. For example: `c:\\Alfresco\\OpenOffice\\soffice.exe` or `c:/Alfresco/OpenOffice/soffice.exe`.

    For Solaris, ensure that the `<configRoot>/classes/alfresco/subsystems/OOoDirect/default/openoffice-transform-context.xml` file can start OpenOffice. Remove the quotes from the connection string values:

    ```
      <value>-
    accept=socket,host=localhost,port=8100;urp;StarOffice.ServiceManager</
    value>
      <value>-env:UserInstallation=file:///${ooo.user}</value>
    ```
12. If the Alfresco server is running, stop and restart the server.

You can configure the OpenOffice transformation settings using one of the OpenOffice subsystems.

Refer to Configuring OpenOffice on page 122.

Installing ImageMagick

To enable image manipulation in Alfresco, you must install and configure ImageMagick. Alfresco uses ImageMagick to manipulate images for previewing.

1. Verify if ImageMagick is already installed on your system.

   You can run the `convert` command, which is part of ImageMagick and usually located in `/usr/bin`.
2. If ImageMagick is not on your system, browse to the ImageMagick download site and install the appropriate package for your platform.
3. Modify the `img.root=` and `img.exe=` properties in the `<classpathRoot>/alfresco-global.properties` file to point to the ImageMagick root directory.

   For example, for Windows:

   a. Set the `img.root=` property to `img.root=C:/Alfresco/ImageMagick`.

   b. Set the img.exe= property to `img.exe=C:/Alfresco/ImageMagick/bin/convert.exe`.

   For Linux:

   a. Set the `img.root=` property to `img.root=/ImageMagick`.

   b. Set the img.exe= property to `img.exe=/ImageMagick/bin/convert.exe`.

   Ensure that you do not include a slash (`/`) at the end of the path. For example, `/ImageMagick/`

Installing Flash Player

This is optional and may be installed after you have installed Alfresco. Alfresco Share uses the Flash Player for viewing Flash previews and also when you use the multi-file upload facility.

1. Browse to the Adobe website: http://www.adobe.com.
2. Download the latest (stable) version of Flash Player for your platform.
3. Browse to the location of your downloaded file and install the application.

   A wizard guides you through the installation.
4. When the installation is complete, click **Close**.

Installing SWF Tools

Alfresco Share uses the pdf2swf utility of the SWF Tools for previewing PDF files. The pdf2swf utility generates one frame per page of fully formatted text inside a Flash movie. To install the pdf2swf utility, you must install the complete SWF Tools.

Installing SWF Tools on Windows

This section describes the steps used to install the SWF Tools.

1. Browse to the SWF Tools website.
2. Download the latest (stable) version of the SWF Tools for your platform. The Windows version is designated with the suffix `.exe`.

Download a version post 0.8.1 from 2007-02-28 because it does not support some functionalities Alfresco needs to render the preview.

3. Browse to the location of your downloaded file and and install the application.

   A wizard guides you through the installation.
4. Accept the license agreement and click **Next**.
5. Select the installation directory.
6. Select whether you want to install the SWF Tools for all users or only for the current user.
7. Click **Next** to begin the install process.

   By default, the options to **Create start menu** and **Create desktop shortcut** are selected.
8. Click **Finish**.
9. Modify the `swf.exe=` property in the `alfresco-global.properties` file to point to the SWF Tools root directory, for example: `swf.exe=C:/Alfresco/bin/pdf2swf`

   Ensure that you do not include a slash (`/`) at the end of the path. For example, `/usr/bin/`

The SWF Tools are installed. For the most up-to-date instructions on installing the SWF Tools, refer to the SWF Tools website.

Installing SWF Tools on Linux

This section describes the steps used to install the SWF Tools. Alfresco Share uses the features provided in the development snapshots of the tools. For Linux, there is no binary version, so you need to compile a development snapshot.

(Linux) Before you compile, ensure that the following packages are installed on your machine:

- `zlib-devel`
- `libjpeg-devel`
- `giflib-devel`
- `freetype-devel`
- `gcc`
- `gcc-c++`

You can download and install all of these packages using the following command:

```
yum install zlib-devel libjpeg-devel giflib-devel freetype-devel gcc gcc-c++
```

1. Browse to the SWF Tools website.
2. Download the latest version of the SWF Tools for your platform. The Unix version is designated with the suffix .tar.gz.

   Download a version post 0.8.1 from 2007-02-28 because it does not support some functionalities Alfresco needs to render the preview. The following version has been tested and verified by Alfresco as being fully functional: `http://www.swftools.org/swftools-2008-10-08-0802.tar.gz` (you may have to copy this URL and paste it into a download manager).
3. Unpack the tar.gz file.

   The install file contains detailed instructions on how to compile and install the SWF Tools.
4. Change to the directory containing the source code.
5. Type the following command to configure the package for your system:

   `./configure`

   If you see a message on Red Hat Linux that states your operating system is unknown, then use the following setting: `./configure–build=x86_64-pc-linux-gnu`

   If you have an issue on Solaris with the lame libs, you can disable the making of portions of SWF Tools that use lame by using the following setting: `./configure -disable-lame`

6. Type the following command to compile the package:

   `make`

   Optionally, you can run the `make check` command to run any self-tests that come with the package.
7. Type the following command to install the programs, data files, and documentation:

   `make install`

   By default, the files are installed to the `/usr/local/bin` directory.
8. Modify the `swf.exe=` property in the `alfreso-global.properties` file to point to the SWF Tools root directory, for example: `swf.exe=/usr/bin/pdf2swf`

   Ensure that you do not include a slash (`/`) at the end of the path. For example, `/usr/bin/`

The SWF Tools are installed. For the most up-to-date instructions on installing the SWF Tools, refer to the SWF Tools website.

Installing TinyMCE language packs

Translations in Alfresco use the language pack supplied in the default install. This default includes English, Catalan, Croatian, Czech, Danish, German, Spanish, Greek, Finnish, French, Italian, Japanese, Dutch, Polish, Portuguese, Portuguese (Brazilian), Russian, Swedish, Turkish, Simplified Chinese. The language used switches according to the browser locale.

If you have a translation that is not supplied with Alfresco, then you must add the appropriate TinyMCE language pack for the translation to work correctly.

If you installed Alfresco using one of the installation wizards, the default language packs are already installed.

1. Browse to the TinyMCE website: http://tinymce.moxiecode.com/download_i18n.php
2. Download the required TinyMCE language pack.
3. Unpack the language file:
   - For Share, unpack to: `<TOMCAT_HOME>/webapps/share/modules/editors/tiny_mce`
   - For Explorer, unpack to: `<TOMCAT_HOME>/webapps/alfresco/scripts/tiny_mce`
4. Ensure that the browser cache is cleared or refresh the page.

Installing an Alfresco Module Package

An Alfresco Module Package (AMP) is a bundle of code, content model, content, and the directory structure that is used to distribute additional functionality for Alfresco. Use the Module Management Tool (MMT) to install and manage AMP files. This section describes how to install an AMP in an Alfresco WAR using the MMT.

The MMT is included in the Alfresco installers, and it is also available as a separate JAR file from the Alfresco WAR file bundle (`alfresco-enterprise-3.4.2.zip`).

For Tomcat, alternatively, run the `apply_amps` command in the Alfresco `\bin` directory, which applies all the AMP files that are located in the `amps` and `amps_share` directories.

1. Browse to the `/bin` directory:
   - (Windows) `C:\Alfresco\bin`
   - (Linux) `/opt/alfresco/bin`
2. Run the following command:

   ```
   java -jar alfresco-mmt.jar install <AMPFileLocation> <WARFileLocation>
   [options]
   ```

   Where:

Option	Description
`<AMPFileLocation>`	The location of the AMP file that you want to install.
`<WARFileLocation>`	The location of the WAR file for your Alfresco installation.
`-verbose`	Install command [options]. Enables detailed output containing what is being updated and to where it is being copied.
`-directory`	Install command [options]. Indicates that the AMP file location specified is a directory. All AMP files found in the directory and its sub directories are installed.
`-force`	Install command [options]. Forces installation of AMP regardless of currently installed module version.
`-preview`	Install command [options]. Previews installation of AMP without modifying WAR file. It reports the modifications that will occur on the WAR without making any physical changes, for example, the changes that will update existing files. It is good practice to use this option before installing the AMP.
`-nobackup`	Indicates that the WAR will not be backed up before the AMP is installed.

   This command installs the files found in the AMP into the Alfresco WAR. If the module represented by the AMP is already installed and the installing AMP is of a higher release version, then the files for the older version are removed from the WAR and replaced with the newer files.

   The following commands show examples of how to install the `example-amp.amp`, and assumes that the AMP file is in the same directory as the WAR file:

   ```
   java -jar alfresco-mmt.jar install example-amp.amp alfresco.war -preview
   ```

   Review the modification to check the changes that will update any existing files.

   The following example will install the AMP file:

   ```
   java -jar alfresco-mmt.jar install example-amp.amp alfresco.war -verbose
   ```

   The modified Alfresco WAR can then be redeployed back into your application server.

   On restarting the application server, the console will show that the custom class was initialized during startup.

3. Verify that the AMP is installed using the MMT `list` command. For example:

   ```
   java -jar alfresco-mmt.jar list <WARFileLocation>
   ```

   This command provides a detailed listing of all the modules currently installed in the WAR file specified.

When the repository is next started, the installed module configuration will be detected, and the repository will be bootstrapped to include the new module functionality and data.

It is not recommended that you overwrite an existing file in an AMP, however it is sometimes necessary. The MMT makes a backup copy of the updated file and stores it in the WAR. When an update of the module occurs and the old files are removed, this backup will be restored prior to the installation of the new files. Problems may occur if multiple installed modules modify the same existing file. In these cases, a manual restore may be necessary if recovery to an existing state is required.

Some application servers (notably Tomcat) do not always fully clean up their temporary working files, and this can interfere with successful installation of an AMP file. To remedy this situation, it is recommended that you delete (or move) the Tomcat `work` and `temp` directories while Tomcat is shut down.

Installing the Firefox extension

The Firefox extension allows access to the network folder for a space in the Firefox browser.

To access the network folder for a space in the Firefox browser, you must install the Alfresco Firefox extension.

1. Go to the URL: http://sourceforge.net/projects/alfresco.
2. Click **Download** to display the available Alfresco Content Management downloads.
3. Locate **Firefox extension** and click **Download**.
4. Click the link `alfrescoext-0.91.xpi`.
5. In the list of download sites, click **Download** for the site nearest you.
6. Allow permission to install the extension.

Installing and configuring Alfresco WCM

Alfresco Web Content Management (WCM) is the leading open source solution.

Alfresco Web Content Management provides:

- An Open Source, lower cost, and lower risk solution that offers greater control and visibility over current and future costs
- A full ECM suite providing complete control over any content from within a single integrated platform – documents, images, video, audio, etc.
- A complete collaboration environment for creating, approving and publishing content to the web
- A platform built on industry standard technology that is as simple to use as a shared network drive

The Alfresco repository supports two store implementations for WCM:

- Web Quick Start (WQS)
- Alternative Versioning Model (AVM)

Web Quick Start

Web Quick Start is an easy-to-install package that provides developers with a strong starting point for their Alfresco implementations.

Web Quick Start is packaged in four parts:

- An Alfresco Module Package (AMP) that extends the repository to support a generic website model
- An AMP that extends Alfresco Share for editing content for the website, managing the structure of the website, and publishing content using workflow
- A JAR file that contains a Java API for accessing the website data held in the repository
- A web application that, when deployed to a servlet container such as Tomcat, delivers a fictional financial news website. The web appilcation is a Spring MVC application constructed using Spring Surf, and communicating with the Alfresco repository using the Java API. As well as dynamically building the website from data held in the repository, Web Quick Start also provides examples of user generated content whereby content is sent from the web application back to the repository.

About Web Quick Start

Alfresco Web Quick Start is a set of website design templates and sample architecture, built on top of the powerful Alfresco Share content management and collaboration framework. With Quick Start, developers can rapidly build customized, engaging, dynamic web applications with powerful content management features for the business users – without having to start from scratch.

Using standard development tools developers can quickly deploy the comprehensive content management capabilities of Alfresco to build new and innovative web applications. Developed using the Spring framework with Spring Surf, the Web Quick Start allows developers to easily extend Alfresco WCM to add new features to support the demands of the CMO.

Installing Alfresco and Web Quick Start

If you are installing Alfresco and Web Quick Start for the first time, use the Alfresco installation wizard.

When you run the installation wizard, your can choose to install a number of Alfresco components. Web Quick Start is provided by default as a selected component.

Manually installing Web Quick Start

If you have an existing Alfresco installation and prefer to install Web Quick Start manually, you can apply the relevant AMP files to your application. This method is suitable for customized or integrated Alfresco installations.

This procedure describes how to copy the AMP files into their appropriate AMP directories and uses the `apply_amps.bat` or `.sh` file to apply them. Alternatively, use the Module Management Tool (MMT) to apply the AMP file.

1. Download the Web Quick Start zip bundle file:

   `alfresco-enterprise-wcmqs-3.4.2.zip`
2. Locate your Alfresco installation directory.
3. Copy the AMP files into the relevant amps directories for Alfresco and Share:
   a. Copy the `alfresco-enterprise-wcmqs-3.4.2.amp` file to the amps directory.
   b. Copy the `alfresco-enterprise-wcmqs-share-3.4.2.amp` file to the amps-share directory.

4. Apply the AMP files using the `apply_amps` command for the Tomcat application server, or, alternatively, use the Module Management Tool (MMT).
5. Copy the website WAR (`wcmqs.war`) into the `webapps` directory of your existing Alfresco installation.

   For example, on Windows with a Tomcat application server, this is `C:\Alfresco\tomcat\webapps`.
6. Copy the Alfresco Web Editor file (`awe.war`) into the `webapps` directory to replace the existing `awe.war` file.
7. Delete the existing alfresco and share directories.
8. Restart the Alfresco server.

Installing Web Quick Start on an existing Alfresco Enterprise install

If you have an existing Alfresco Enterprise installation, you can use the standalone installation wizard for installing Web Quick Start.

Ensure that Alfresco is not running before you start the WQS installer.

1. Download the Web Quick Start installer.

   (Windows) `alfresco-enterprise-wcmqs-3.3.4-win-installer.exe`

   (Linux) `alfresco-enterprise-wcmqs-3.3.4-linux-installer.bin`

   (Mac) `alfresco-enterprise-wcmqs-3.3.4-osx-installer.app.tar.gz` (the uncompressed file is `alfresco-enterprise-wcmqs-3.3.4-osx-installer`)
2. Run the installation wizard.
3. In the **Setup – Alfresco Enterprise Quick Start** window, click **Next**.
4. In the **Installation Directory** window, enter the directory where Alfresco Enterprise 3.3.4 is installed, and then click **Next**.

   The installer tries to locate the default Alfresco installation directory:

   (Windows) `C:\Alfresco`

   (Linux) `/op/alfresco`

   (Mac) `/Applications/alfresco-3.3.4`

   The installation starts.
5. In the **Completing the Alfresco Enterprise Quick Start Setup Wizard** window, ensure that you deselect the checkbox to automatically launch Share, and then click **Finish**.
6. Delete the existing `alfresco` and `share` directories.
7. Restart the Alfresco server.

Creating the Web Quick Start site

The Web Quick Start site is a default Share Collaboration site with the sample Quick Start data imported. A Share dashlet is provided, from which you can import the sample data.

1. Open Share.
2. Click **Create Site**.

   This creates a new collaboration site.
3. Type a name for the site, for example, **Web Quick Start**.
4. Type a URL name for the site, for example **wcmqs**.
5. Click **OK**. The new site displays in your My Sites dashlet.

6. Open the new site.
7. Click **Customize Dashboard**.
8. Click **Add Dashlets**.
9. Drag the Web Quick Start dashlet to your dashboard layout.
10. Click **OK**.

    The Web Quick Start dashlet displays in the site dashboard.

Importing Web Quick Start demo data

When you initially add the Web Quick Start dashlet into the site dashboard, the dashlet displays a link that enables you to import the Web Quick Start demo data.

1. Click **Import Website Data**.

   Choose the sample content to import: **Government** or **Finance**.

   Both samples are identical in functionality but contain different images and section headings. The samples provide an example of how developers can package and import their own sample site data.

   The system imports the data for the demo website.
2. Refresh the browser running Share.

   The Web Quick Start dashlet now displays a link to the **Web Quick Start Help**.

By default, Web Quick Start is configured to be accessed at `localhost` on port 8080. If these settings are relevant for your installation and the `wcmqs.war` is running in the same container as Alfresco, you will now be able to access the Web Quick Start editorial website on http://localhost:8080/wcmqs.

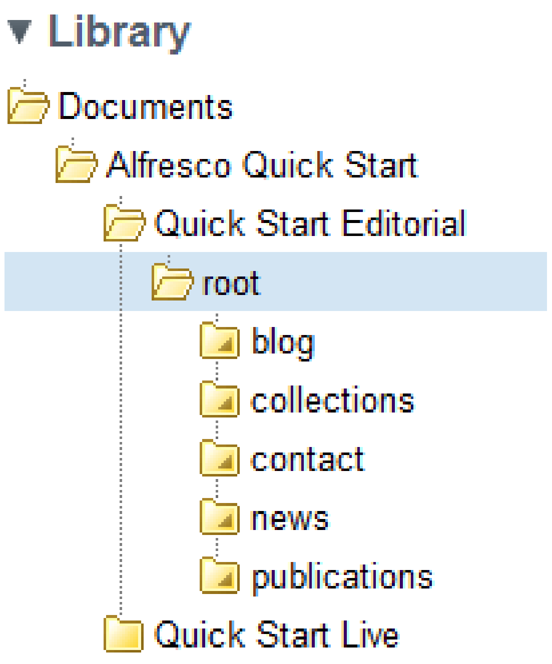
To change the server host name, port, or web application context from the default values, refer to Configuring Web Quick Start on page 51.

Configuring Web Quick Start

After you have imported the Web Quick Start website data, when you have refreshed Share, or the next time you log on, you can access the Web Quick Start site for configuration.

1. Open the Web Quick Start site.
2. Navigate to the Document Library.

   The default site structure will have the following structure:



The site structure contains two folders: `Quick Start Editorial` and `Quick Start Live`. These folders represent a separation between the work in progress content, and the finished, reviewed, editorially complete content that is then published to the “Live” environment.

If your web container is running on port 8080 and the web application is running in the same container as Alfresco, the setup is complete and you should be able to access the web site on http://localhost:8080/wcmqs.

Configuring the web application host name, port, and context

This section describes how to change the host name, port, and context for the Web Quick Start web application.

The Web Quick Start installation assumes that the web application has been deployed to localhost on port 8080, using the context of wcmqs. This means that the editorial website can be accessed at http://localhost:8080/wcmqs. The "live" website can be accessed as default on http://127.0.0.1:8080/wcmqs.

If you are not running the web application on port 8080 or if the web application is deployed to a different container or host, you can configure the site to the required location.

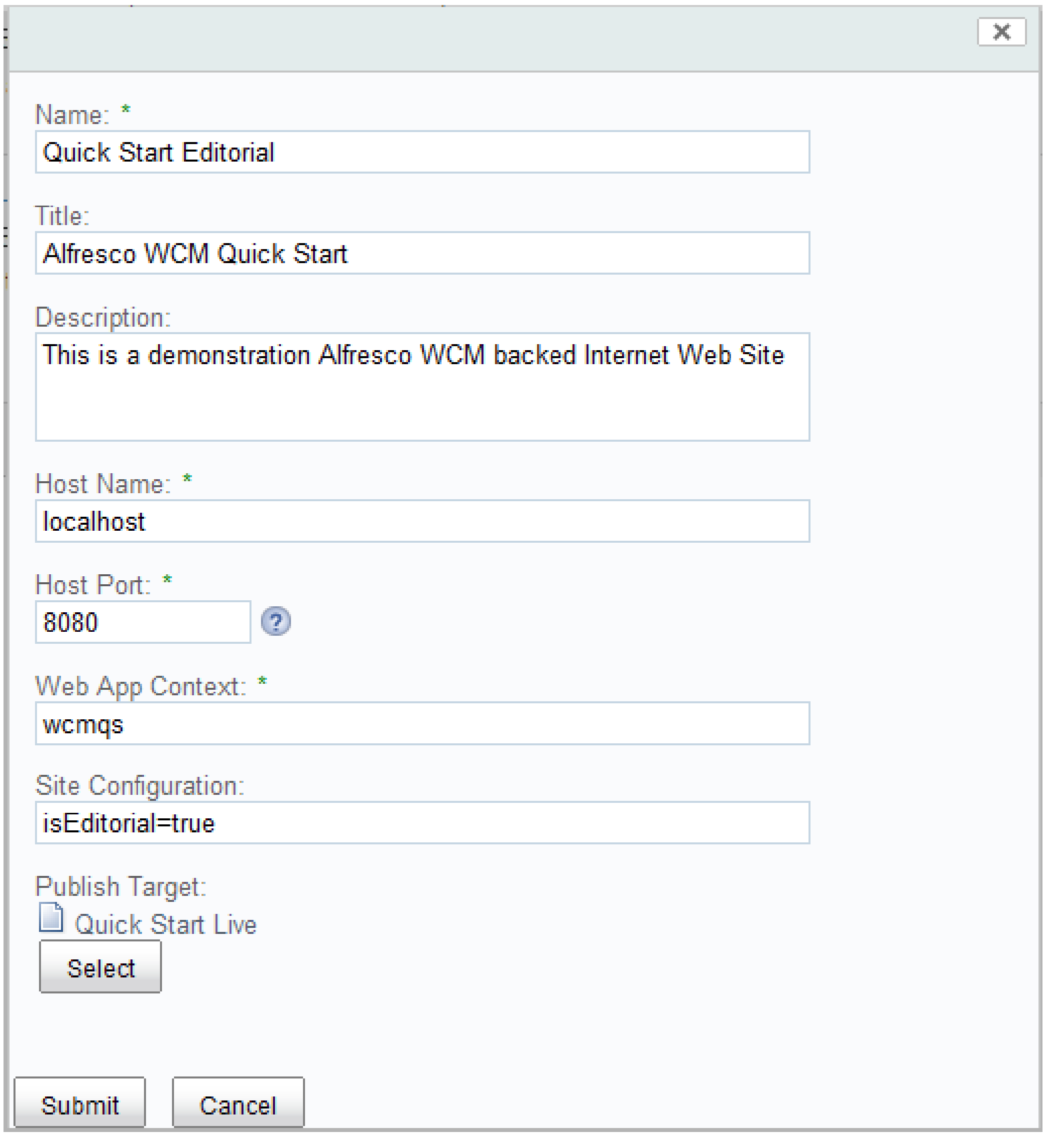
1. In the Web Quick Start site, navigate to the **Document Library**.
2. Click **Edit Metadata** on either the **Quick Start Editorial** folder, or the **Quick Start Live** folder.
3. Configure the **Host Name**, **Port**, and **Web App Context** fields to point to the location your web application (`wcmqs.war`).
4. Click **Submit**.

Disabling AWE on the Live environment

The Web Editor (AWE) is configured to be enabled on the Editorial content, and disabled on the Live. This is controlled by the `isEditorial` flag on the **Quick Start Editorial** metadata. This also (when complete) dictates what can be viewed via the live web application with regards to publishing go live and expiry dates.

This procedure configures the web application to view the “Live” site structure.

1. Edit the metadata properties on the **Quick Start Live** folder.
2. In the **Site Configuration** field, enter the `isEditorial=true` flag.



Name: *	Quick Start Editorial
Title:	Alfresco WCM Quick Start
Description:	This is a demonstration Alfresco WCM backed Internet Web Site
Host Name: *	localhost
Host Port: *	8080
Web App Context: *	wcmqs
Site Configuration:	isEditorial=true
Publish Target:	Quick Start Live

3. Click **Submit**.

The default configuration sets the host address to 127.0.0.1, so if you are running Web Quick Start locally, you can view the editorial environment on http://localhost:8080/wcmqs and the live on http://127.0.0.1:8080/wcmqs.

Alfresco Web Editor

The Alfresco Web Editor is a Spring Surf-based web application that provides in-context editing capabilities for Alfresco repository content. The editor provides a mechanism for non-technical users to make edits to Alfresco content directly within a web page.

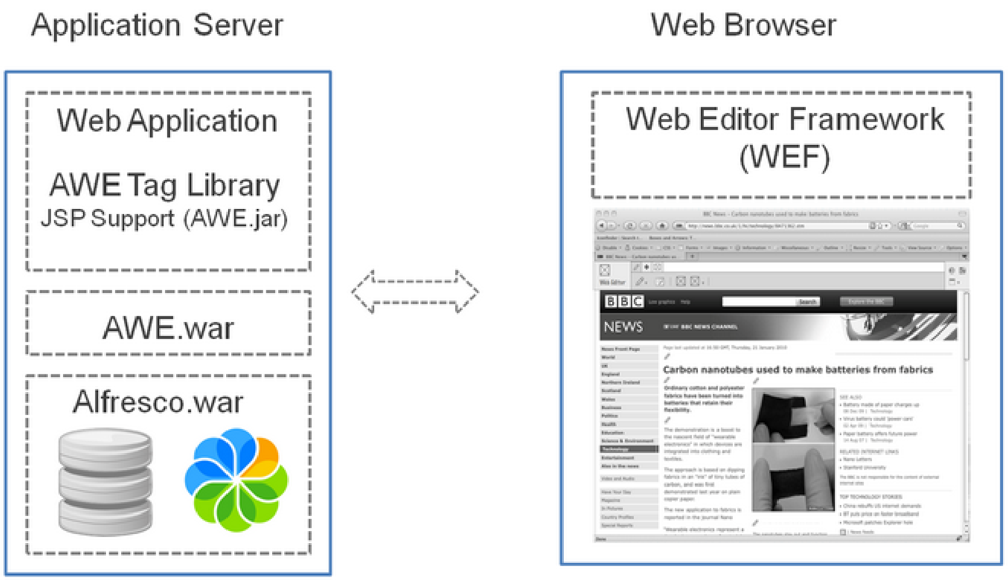
The Alfresco Web Editor uses the Forms Service default template.

The Alfresco Web Editor is packaged as a stand-alone WAR file so that it can be deployed to web applications that are in the sample instance, or remote, to the Alfresco server. When it is deployed, an Alfresco banner displays in your deployed web pages showing the Alfresco Web Editor tab and it identifies the editable content. By default, it assumes that you have JavaScript enabled but it can also run without JavaScript.

Alfresco Web Editor deployment

The simplest way to deploy the Alfresco Web Editor is to use the pre-built WAR (`awe.war`) file and to deploy it in the same application server instance of your web application.

The following diagram shows an example Alfresco Web Editor deployment in the same application server as the Alfresco repository.



The Alfresco Web Editor is a Spring Surf-based application, therefore it is also possible to deploy it in a different application server instance from the Alfresco repository.

The deployment comprises the following components:

AWE.war
The Alfresco Web Editor WAR file.

Web Application
Your own web application.

AWE tag library
Provides the ability to mark areas of the page as editable. The areas marked can represent any property or content from the Alfresco repository.

Web Editor Framework (WEF)
The client-side JavaScript framework on which the Web Editor is built. It is built using YUI and can be extended easily. New tabs and buttons can be packaged and dropped into the framework. This provides the core Alfresco product features, and also provides the ability to build additional custom plugins.

When the Alfresco Web Editor is enabled, the WEF renders the tool bar and basic in-context editing buttons and functionality. If the WEF is deployed as standalone, the default blank tool bar is rendered.

Deploying the Alfresco Web Editor

The Alfresco Web Editor distribution consists of a single zip file named `alfresco-enterprise-webeditor-3.4.2.zip`.

1. Shut down your Alfresco server.
2. Download the `alfresco-enterprise-webeditor-3.4.2.zip` file.
3. Deploy the `awe.war` file into the same application server instance as the Alfresco repository.
4. Copy the `alfresco-webeditor-taglib.jar` file to the `WEB-INF/lib` folder of your application.
5. To include the tag library in your application, add the following tag library declaration to your JSP page:

   `<%@ taglib uri="http://www.alfresco.org/tags/awe" prefix="awe" %>`

   Once the tag library is declared, you can use the startTemplate, endTemplate and markContent tags within your application.
6. Restart your Alfresco server.

Deploying the Alfresco Web Editor to a Spring Surf application

The Alfresco Web Editor distribution also includes all the files required to provide the functionality within an existing Spring Surf application.

1. Copy the following files to your application `WEB-INF/lib` directory:
   a. `yui-2.7.0.jar`
   b. `spring-webeditor-1.0.0.CI-SNAPSHOT.jar`
   c. `alfresco-forms-client.jar`
   d. `alfresco-webeditor-plugin.jar`

   The `yui` and `spring-webeditor` JAR files represent the Web Editor Framework (WEF) upon which the Web Editor is built. The remaining `alfresco-form-client` and `alfresco-webeditor-plugin` JAR files provide the Web Editor functionality.
2. If you plan to use the Web Editor within the application (rather than the application being a host for the Web Editor services) you also must copy the following additional files into the `WEB-INF/lib` directory:
   a. `spring-webeditor-client-jsp-1.0.0.CI-SNAPSHOT.jar`
   b. `alfresco-webeditor-taglib.jar`
3. If you use the additional files, define a servlet filter in your application's `web.xml` file.

   If you do not provide the filter, the tags will be ignored. The following filter configuration is required:

```
<filter>
    <filter-name>Alfresco Web Editor Filter</filter-name>
    <description>Enables support for the Alfresco Web Editor</
description>
    <filter-class>org.alfresco.web.awe.filter.WebEditorFilter</filter-
class>
    <init-param>
       <param-name>contextPath</param-name>
       <param-value>/your-context-path</param-value>
    </init-param>
</filter>

<filter-mapping>
   <filter-name>Alfresco Web Editor Filter</filter-name>
   <url-pattern>/*</url-pattern>
</filter-mapping>
```

4. Set the `contextPath` parameter.

   If you do not provided a value for this parameter, a default `contextPath` of `/awe` is presumed.

   No further configuration is required as all the necessary Spring context files and Alfresco configuration files are contained within the JAR files. However, there is no default hook point for custom form configuration but this can be located anywhere within your application.

Configuring Alfresco Web Editor

The following Web Editor components must be configured:

- tag library, that is, the `markContent` tag used to define editable content
- servlet filter
- form configuration

Configuring the tag library

This section describes the tag library configuration.

The tag library comprises the following tags:

- `startTemplate`
- `markContent`
- `endTemplate`

1. The `startTemplate` tag bootstraps the WEF using a script element that executes a web script. Place this tag in the `head` section of your page.

   The `startTemplate` tag has only one optional attribute.

   toolbarLocation
   Controls the initial location of the tool bar. The valid values are: `top`, `left`, and `right`. The default is `top`.

   The following shows an example of how to use the `startTemplate` tag:

   ```
   <awe:startTemplate toolbarLocation="top" />
   ```

2. Use the `markContent` tag to indicate an editable area of the page.

   The tag renders an edit icon that, when clicked, displays a form for editing the corresponding Alfresco content and properties, or both.

   The `markContent` tag has two mandatory attributes and two optional attributes.

   id
   The mandatory identifier attribute specifies the NodeRef of the Alfresco node to be edited.

   title
   The mandatory title attribute defines a descriptive title for the editable area being marked. The title used is used in the quick edit drop down menu of editable items, as the title of the form edit popup/dialog and the alt text and tool tip text of the edit icon.

   formId
   This is an optional attribute that specifies which form will be used when the marked area is edited.

nestedMarker
This is an optional attribute, which defines whether the editable area is nested within another HTML tag that represents the content being edited. If it is set to true, the whole parent element is highlighted when the area is selected in the quick edit drop down menu. If set to "false" only the edit icon is highlighted.

An example use of the markContent tag is shown below.

```
<awe:markContent id="<%=subTextNodeRef%>" formId="description"
 title="Edit Description" nestedMarker="true" />
```

3. The `endTemplate` tag initializes the Web Editor with details of all the marked content areas on the page. It also renders a script element that executes the WEF resources web script, which starts the process of downloading all the assets required to render and display the tool bar and all configured plugins. Place this tag just before the closing body element.

   The `endTemplate` tag does not have any attributes.

   The following shows an example of how to use the `endTemplate` tag:

```
<awe:endTemplate />
```

Configuring the servlet filter

The `startTemplate`, `markContent`, and `endTemplate` tags will only render their output if they detect the presence of the Web Editor servlet filter. The tags can remain in the JSP page in production and have no effect until the servlet filter configuration is added to the `web.xml` file.

1. Add the following servlet filter configuration to the web application's `web.xml` file:

```
<filter>
   <filter-name>Alfresco Web Editor Filter</filter-name>
   <description>Enables support for the Alfresco Web Editor</description>
   <filter-class>org.alfresco.web.awe.filter.WebEditorFilter</filter-
class>
</filter>

<filter-mapping>
   <filter-name>Alfresco Web Editor Filter</filter-name>
   <url-pattern>/*</url-pattern>
</filter-mapping>
```

   This enables the tags.

2. Set the following two optional parameters:

```
<init-param>
   <param-name>contextPath</param-name>
   <param-value>/quickstart</param-value>
</init-param>

<init-param>
   <param-name>debug</param-name>
   <param-value>true</param-value>
</init-param>
```

   These parameters control the `contextPath` that is used when URLs to the Web Editor are generated and the debug mode.

Configuring Web Editor forms

The Alfresco Web Editor uses a form to edit the node referenced by a `markContent` tag. By default, the form displayed will contain the `cm:title`, `cm:description`, and `cm:content` fields. An alternative form can be used by providing the `markContent` tag with a `formId` attribute.

Out of the box, only two other forms are configured: a form with an identifier of `title`, and one with an identifier of `description`. As the identifiers indicate, the forms display a single property: `cm:title` and `cm:description`, respectively. The node type is presumed to be `cm:content`.

If you have custom types or wish to specify other properties, you can use the the forms configuration techniques.

Sample web application using Alfresco Web Editor

A sample customer WAR file is available in the Alfresco Web Editor distribution. It demonstrates how a customer may use Alfresco Web Editor in a very simple JSP-based web application. This sample must not be used in a production environment and is not supported.

A sample customer tag library is provided, which includes two tags. These tags are included as a demonstration sample and should never be used in a production environment.

`content`
: Allows content to be pulled from an Alfresco repository and sends output to a JSP page. The `content` tag requires one mandatory attribute called `nodeRef`

`property`
: Allows properties to be pulled from an Alfresco repository and sends output to a JSP page. The `property` tag requires two mandatory attributes: `nodeRef` and `property`.

The following example show the use of these tags:

```
<customer:content nodeRef="<%=mainTextNodeRef%>" />
<customer:property nodeRef="<%=subTextNodeRef%>" property="cm:description" />
```

The sample customer application consists of several, simple JSP pages that display the content and properties of two nodes from the repository. Update the `/includes/noderefs.jsp` page to provide the NodeRefs of two nodes in your repository.

By default, the sample pulls content from the Alfresco repository located at `http://localhost:8080/alfresco`, using a user name and password of `admin`. These values can be supplied using `context-param` values in the `web.xml` file, for example:

```
<context-param>
     <param-name>org.customer.alfresco.host</param-name>
     <param-value>localhost</param-value>
  </context-param>

  <context-param>
     <param-name>org.customer.alfresco.port</param-name>
     <param-value>8080</param-value>
  </context-param>

  <context-param>
     <param-name>org.customer.alfresco.context</param-name>
     <param-value>alfresco</param-value>
  </context-param>

  <context-param>
     <param-name>org.customer.alfresco.username</param-name>
     <param-value>admin</param-value>
  </context-param>

  <context-param>
     <param-name>org.customer.alfresco.password</param-name>
     <param-value>admin</param-value>
  </context-param>
```

Alternative Versioning Model (AVM)

This section describes the installation, configuration, and deployment procedures for the Alfresco WCM functionality using the Alternative Versioning Model (AVM).

About Alternative Versioning Model (AVM)

The Alfresco repository currently supports two store implementations. The “core”, or Document Management based store used by the Quick Start, and the Alternative Versioning Model (AVM). The AVM is an alternative store implementation designed to support the version control requirements of managing websites and web applications. The AVM consists of a forest of content stores that can be used to manage the development and staging of web content and associated source code. Each AVM store is loosely modeled on Subversion, providing static content control for websites.

Installing AVM

This section describes how to install AVM.

Installing AVM to an existing instance of Alfresco

This task describes how to install AVM to an existing instance of Alfresco.

1. Browse to the Alfresco Enterprise download area.
2. Select the following file:

   `alfresco-enterprise-avm-3.4.2.zip`
3. Download and extract the file into the Alfresco home directory. For example:
   - (Windows) `C:\Alfresco`
   - (Linux) `/opt/alfresco`
4. Browse to the Alfresco home directory, and unzip the downloaded file.

   If your unzip program asks about existing directories, allow this because no existing files will be overwritten.
5. In the root of the Alfresco home directory, copy the file `wcm-bootstrap-context.xml` to the `<extension>` directory.
6. Restart the Alfresco server.

   This ensures that the Alfresco server starts to use the installed components. To restart the Alfresco server, see Starting the Alfresco server on page 101

WCM is installed and configured.

Verifying the AVM installation

Verify the AVM installation after you have installed, configured, and started the Alfresco server.

1. In the Alfresco home directory, open `alfresco.log`.
2. In `alfresco.log`, search for the following text:

   ```
   The Web Forms folder was successfully created: and The Web Projects
   folder was successfully created:
   ```
3. Check that the following additional spaces are in your Alfresco repository:
   - **Web Projects** in **Company Home**
   - **Web Forms** in **Data Dictionary**

AVM has been installed, configured, started, and verified. To use the Website Preview feature, start the Alfresco virtualization server.

Installing the standalone deployment receiver

The standalone deployment receiver allows a web project from AVM to be deployed to a remote file server, typically a web or application server. The published files are then typically published by a web server such as Apache for static content, or an application server, such as Tomcat or JBoss for dynamic content

1. Browse to the Alfresco Enterprise download area.
2. Download one of the following files:
    - (Windows) `alfresco-enterprise-deployment-3.4.2-win.exe`
    - (Linux) `alfresco-enterprise-deployment-3.4.2-linux.bin`
3. Run the installation file.
4. In the **Setup - Alfresco Enterprise Deployment** window, click **Next**.
5. In the **Installation Directory** window, click **Next** to accept the default location for the deployment receiver, or you can choose another location.

    For example, `C:\alfresco\deployment` on Windows or `/opt/alfresco/deployment` on Linux.
6. In the **User Account Details** window, enter a user name and password for the user account that will administer the deployment receiver, and then click **Next**.
7. If you are using RMI as your transport protocol, enter the port numbers for the following:

Deployment	Description
RMI Registry Port Number	The port number for the RMI registry. Choose the default of 44100 to avoid conflict the other services.
RMI Service Port Number	The port number to use for the RMI service. Choose the default of 44101 to avoid conflicts with other services.

8. Click **Next**.
9. In the **Ready to Install** window, click **Next**.
10. In the **Completing the Alfresco Enterprise Deployment Setup Wizard** window, click **Finish**.

The deployment receiver, out of the box, is configured with a single file system deployment target.

Deployment receiver subsystem properties

The following properties can be configured for the WCM deployment receiver subsystem.

wcm-deployment-receiver.poll.delay
Specifies how long to wait before polling. For example, `5000`.

wcm-deployment-receiver.rmi.service.port
Specifies the port number for the RMI service. For example, `44101`.

Configuring AVM

This section describes how to configure AVM.

In AVM, content is managed in sandboxes, which isolate each user's changes, and content can be submitted to a shared (staging) sandbox, and then deployed either to a flat file system or another instance of Alfresco. Content is collected and displayed using forms, and workflow controls the approval and publishing of content.

Configuring the virtualization server

WCM preview allows editorial users to preview the website in-context (with the style, markup, and composition of the website), but using the content from any sandbox in the system. Preview provides a way for contributors and reviewers to view changes as if they had been published to the live site, without publishing those changes.

This is primarily used for two activities:

- To allow content approvers to review a change they have been asked to approve in the context of the website.
- To allow content contributors to view their changes in the context of the website, while they are in the process of making those changes.

The virtualization server is the default WCM preview functionality when WCM is installed. The virtualization server (which is a slightly modified Tomcat server) interprets data in the AVM repository as a set of virtual websites, allowing users to browse these websites prior to deployment. These websites may include both static sites (or example, `.html`, `.gif`, `.png`) and simple Java-based sites (virtualized servlets and JSPs).

Each Web Project is assumed to be a self contained J2EE web application, and each sandbox in the Web Project is automatically "deployed" as a J2EE web application to the virtualization server. The virtualization server lazily "deploys" each sandbox the first time it receives a preview request, and no physical deployment occurs. The virtualization server has been customized to read the web application directly from the Alfresco repository, rather than from the file system.

To ensure the transparent preview of any sandbox in any Web Project in the system, Alfresco uses dynamic host names (in tandem with wildcard DNS) for accessing the virtualization server. From this enhanced host name, the virtualization server is able to determine from which sandbox and Web Project to read content and web application assets. This ensures that the web application itself has no knowledge of any WCM constructs (sandboxes, Web Projects, virtualization server, and so on); it runs as if it is in a native Tomcat server and the virtualization system ensures that assets are read from the correct sandbox for each preview request.

Each virtual view corresponds to a virtual website within its own virtual host. You can see the virtual view in the URL itself. The following URL shows the general format of an Alfresco virtual hyperlink:

```
http://virtual-hostname.www--sandbox.virtualization-domain:port/request-path
```

To configure virtual websites, the `virtualization-domain` and all its subdomains must resolve in DNS to the IP address of the virtualization server (also known as a “wildcard DNS” mapping). There are two ways to achieve this:

- Use the appropriate subdomain of ip.alfrescodemo.net
- Configure a nameserver, and setting up a wildcard domain pointing at your virtualization server's IP address

Using ip.alfrescodemo.net

To set up virtualization for a single machine or a LAN, use the appropriate subdomain of `ip.alfrescodemo.net`.

In this example, `192.168.1.5` is the IP address of the machine hosting the virtualization server. Alfresco has set up a nameserver at ip.alfrescodemo.net that is able to resolve any domain name of the form `AAA-BBB-CCC-DDD.ip.alfrescodemo.net` (or any of its subdomains) as the IP address `AAA.BBB.CCC.DDD`.

For example, if your browser asks for the virtual host name: `alice.mysite.www--sandbox.192-168-1-5.ip.alfrescodemo.net`, the IP address returned will be: `192.168.1.5`. Therefore, ip.alfrescodemo.net provides "wildcard dns" for all valid IPV4 address. By default, the virtualization server is configured to use the virtualization domain `127-0-0-1.ip.alfrescodemo.net`. This returns the IP address `127.0.0.1`. This special IP address always refers to your local machine (hence its name: `localhost`). Therefore, if you use the default virtualization domain `127-0-0-1.ip.alfrescodemo.net`, you will only be able to do in-context preview on the same machine that hosts the virtualization server. To enable everybody on a LAN to use in-context preview, you need to use a network-accessible IP address.

1. Open the `$VIRTUAL_TOMCAT_HOME/conf/alfresco-virtserver.properties` file.

   Where `$VIRTUAL_TOMCAT_HOME` represents the directory in which you installed the virtualization server.
2. Locate the property `alfresco.virtserver.domain=127-0-0-1.ip.alfrescodemo.net.`
3. Edit the property to contain the hyphen-encoded IP address you want.

   For example: `alfresco.virtserver.domain=192-168-1-5.ip.alfrescodemo.net`.

   When specifying `alfresco.virtserver.domain` that uses `ip.alfrescodemo.net`, the IP address for a DNS wildcard domain must be hyphen-encoded. Otherwise, `ip.alfrescodemo.net` will assume an error, and return `127.0.0.1` for all DNS name lookups within your malformed virtualization domain.

   For example:

   Valid: `alfresco.virtserver.domain=192-168-1-5.ip.alfrescodemo.net`

   Malformed: `alfresco.virtserver.domain=192.168.1.5.ip.alfrescodemo.net`

   Alfresco can now generate URLs that address the virtualization server's network-accessible address, such as `192.168.1.5` and not `127.0.0.1`, allowing users on a LAN to use in-context preview.
4. Restart the Tomcat instance that runs Alfresco.
5. Near WCM assets, click the icon resembling an eyeball.

   A list of URLs displays, for example: `http://<hostname>.www--sandbox.192-168-1-5.ip.alfrescodemo.net`

   These links will resolve to your virtualization server, which is on `192.168.1.5`.
6. To view this in isolation, run one of the following commands:

   - `ping alice.mysite.www--sandbox.192-168-1-5.ip.alfrescodemo.net`
   - `ping mysite.www--sandbox.19`

Configuring wildcard DNS on a nameserver

This section describes how to configure a nameserver and set up a wildcard domain pointing at your virtualization server machine's IP address to do the following:

- Virtualize content on a machine or LAN with no access to the Internet (for example: a demo laptop)
- Attain faster speeds on the first DNS lookup of a name than when served locally (IP address answers have a one day TTL)
- Keep everything centralized if you already have BIND, djbdns, Microsoft DNS, or other DNS solution in place
- Be independent from the Alfresco alfrescodemo.net uptime

1. Set the directory where you installed the virtualization server, for example: `$VIRTUAL_TOMCAT_HOME`.

   In this example, the LAN's domain name is `localdomain.lan`, a wildcard DNS record resolves to an IP address such as `192.168.1.5`, and the wildcard DNS names are within `ip.localdomain.lan`.
2. Open the file `$VIRTUAL_TOMCAT_HOME/conf/alfresco-virtserver.properties`.
3. Modify the value of the `alfresco.virtserver.domain` property to resemble the following:

```
alfresco.virtserver.domain=ip.localdomain.lan
```

You cannot use the “hosts” file to create a wildcard DNS domain on Windows or Unix. To create a DNS wildcard that is usable when you are not connected to the Internet, you must install, configure, and maintain a real nameserver.

Enabling links validation

The check links action is used to validate links in the web project and generate a report detailing broken hyperlinks so they can be corrected. By default, links validation is disabled. This section describes how to enable links validation.

1. Open the `alfresco-global.properties` file.
2. Add the following property:

   ```
   linkvalidation.pollInterval=5000
   ```
3. Save your file.
4. Restart the Alfresco server and the virtualization server.

Links validation is enabled and visible in the graphical interface.

Installing Records Management

This section describes the general procedure for installing Records Management.

Ensure that you have Alfresco Enterprise 3.4.2 installed on your machine.

1. Download and apply the Records Management AMP files to your existing Alfresco installation.
2. Restart the Alfresco server.
3. Log in to Share to add the Records Management dashlet.
4. Create the Records Management site.

Applying the Records Management AMP files

To install Records Management, you need to apply the AMP files to an existing Alfresco installation.

The installation procedure uses the following Records Management AMP files:

`alfresco-enterprise-dod5015-share-3.4.2.amp`	This AMP file contains the additional Records Management functionality that is applied to an existing Alfresco Share user interface. The functionality should be applied to the `tomcat/webapps/share` directory.
`alfresco-enterprise-dod5015-3.4.2.amp`	This AMP contains the additional Records Management functionality that is applied to an existing Alfresco installation.

The following procedure applies the Records Management AMP files to an existing Alfresco Enterprise 3.4.2 running in a Tomcat application server. If you are using an application server other than Tomcat, use the Module Management Tool (MMT) to install the AMP files. If you are using the MMT, you must apply the `alfresco-enterprise-dod5015-share-3.4.2.amp` to the `share.war` file.

1. Move the `alfresco-enterprise-dod5015-3.4.2.amp` file to the `amps` directory.
2. Move the `alfresco-enterprise-dod5015-share-3.4.2.amp` file to the `amps_share` directory.

3. Stop the Alfresco server.
4. Run the `apply_amps` command, which is in the root Alfresco directory.

   This command applies all the AMP files that are located in the `amps` and `amps_share` directories.

   For Linux, edit the `CATALINA_HOME` variable, as needed.
5. Start the Alfresco server.
6. Start Alfresco Share by browsing to:

   `http://<your-server-name>:8080/share`

Adding the Records Management dashlet

When you have installed the Records Management module and started your server, you need to add the Records Management dashlet into your personal dashboard.

This dashlet allows you to create the pre-defined Share site for Records Management functionality.

1. Log in to Alfresco Share.
2. Click **Customize Dashboard**.
3. Click **Add Dashlets**.
4. Locate the **Records Management config** dashlet in the **Add Dashlets** list.
5. Drag the **Records Management config** dashlet to the desired column.
6. Click **OK**.

The Records Management dashlet displays in the selected column in your Records Management site dashboard.

The Records Management dashlet provides actions that allow you to:

- Create the Records Management site
- Access the Records Management site once it is created
- Load sample test data for an example of how to structure a File Plan
- Access the management console

Creating the Records Management site

This task assumes that you have added the Records Management dashlet into your dashboard.

1. On the Records Management dashlet, click **Create Records Management Site**.

   A message displays to confirm that the site had been created.
2. Refresh the Share dashboard, either:
   - Refresh the browser, or
   - Logout of Share, and then logon again using the same user name and password.

The Records Management site now displays in the **My Sites** dashlet.

Installing and configuring Alfresco Kofax Release script

This section provides details on installing, configuring, and using the Alfresco Kofax Release script.

Integrating Kofax and Alfresco provides complete content management support including the capture, management, and publishing of content. Kofax Capture captures content from various sources, typically through scanning and OCR. The captured information is then released to Alfresco to be managed in an ad-hoc manner or using pre-defined business processes.

The Kofax architecture provides a plug-in architecture for deploying a Kofax Release script that is responsible for mapping and transferring the information captured by Kofax to the destination application or database.

The Alfresco Kofax Release script comprises a Release script plug-in that is installed within the Kofax Capture application and a set of Alfresco web scripts installed on the Alfresco server.

The Alfresco Kofax Release script provides the following capabilities:

- Alfresco server connection (connection URL, user name, password)
- Destination folder in which to store the captured documents (folders may be automatically created based on index field values)
- Mapping of Kofax Capture indexing information and files to Alfresco properties
    - Support for Alfresco types, sub-types, and aspects, and their associated properties
    - Mapping of Kofax Image (TIFF), Text (OCR), or PDF files to Alfresco content properties
- Automatic versioning, overwrite, and error handling for existing documents

System requirements and prerequisites

This section describes the system requirements for the Alfresco Kofax Release script.

The Alfresco Kofax Release script has the following prerequisites:

- Alfresco Version 3.1 or higher
- Kofax Capture 8.x

You need to have a working knowledge of Kofax Capture and Alfresco.

Installation and advanced configuration requires experience with Alfresco Module Packages (AMPs) and defining Alfresco models. For more information Kofax, refer to the Kofax Capture documentation.

Installing Kofax Release script

Installing the Alfresco Kofax Release script is a two-part process.

The installation process involves the following steps:

1. Installation of the Alfresco Kofax Release script Alfresco Module Package (AMP) file using the Alfresco Module Management Tool.
2. Installation of the Alfresco Kofax Release script binaries in your Kofax Capture installation.

Installing the Alfresco Kofax Release script AMP

The following describes how to install the Alfresco Kofax Release script AMP file (`alfresco-kofax.amp`) on your Alfresco server.

1. Shut down your Alfresco server.
2. Move or copy the `alfresco-kofax.amp` file to the `amps` directory in your Alfresco installation.
    - (Windows) `c:\Alfresco\amps`
    - (Linux) `/opt/alfresco/amps`

3. From the command line, browse to the Alfresco `bin` directory.
    - (Windows) `c:\Alfresco\bin`
    - (Linux) `/opt/alfresco/bin`
4. Install the Alfresco Kofax AMP using the Module Management Tool.
    - (Windows) `java -jar alfresco-mmt.jar install c:\Alfresco\bin\amps\alfresco-kofax.amp c:\Alfresco\tomcat\webapps\alfresco.war`
    - (Linux) `java -jar alfresco-mmt.jar install /opt/alfresco/amps/alfresco-kofax.amp /opt/alfresco/tomcat/webapps/alfresco.war`

    Alternatively for Tomcat, you can run the `apply_amps.bat` command in the root Alfresco directory to install the `alfresco-kofax.amp`. This batch file applies all the AMPs that are located in the amps directory.
5. Remove your existing expanded Alfresco web application directory to allow updates to be picked up when the server restarts.
    - (Windows) `c:\Alfresco\tomcat\webapps\alfresco.war`
    - (Linux) `/opt/alfresco/tomcat/webapps/alfresco`

Installing the Alfresco Kofax Capture Release script binaries

The following steps describe how to install the binaries required to set up and configure the Kofax Release script in your Kofax Capture installation.

You must have Windows administrator privileges to install Kofax Capture Release script binaries. If you do not have administrator rights, you may encounter errors and the script may fail to install.

1. Unzip the `alfresco-kofax-client-binaries-3.4.2.zip` file to your Kofax Capture `bin` directory.

    For example, (Windows) `c:\Program Files\Kofax\Capture\bin`
2. Start the Kofax Capture Administration Module.
3. In the Kofax Administration module, click **Tools > Release Script Manager**.
4. From the **Release Script Manager** dialog box, click **Add** and then browse to the directory of the unzipped files.
5. Select `Alfresco.Kofax.Release.inf`, and click **Open**.
6. Click **OK** to register the release script.
7. Close the open dialog boxes to complete the process.

Configuring the Alfresco Kofax Release script

This section provides instructions on setting up the Alfresco Kofax Release script. These instructions assume you are familiar with Kofax Capture and have created a Kofax Capture batch class. For information on setting up batch classes in Kofax Capture, refer to the Kofax Capture documentation.

In Kofax Capture, release scripts are associated with document classes. The script is configured to define where and how the documents will be released, including:

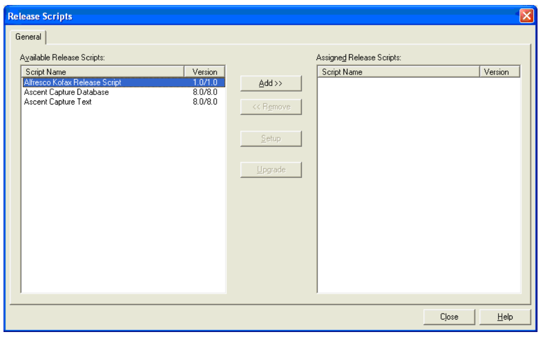
- URL to connect to your Alfresco server
- Alfresco user name and password used to create the documents in Alfresco
- Location in the Alfresco repository where documents will be released
- Options for handing existing documents, such as Overwrite, Version, Release to Default Folder, or Report an Error

- Alfresco document type
- Mapping between the Alfresco properties (including those based on type and configured aspects), and the Kofax indexing fields to be populated by the release script

Associating the Alfresco Kofax Release script with a document class

Once you have set up a batch class with an associated document class in Kofax Capture, you can associate a Release script with the batches document class. As part of this process, you are prompted to enter the connection details for your Alfresco server.

1. Start the Kofax Capture Administration Module.
2. Select the **Batch class** tab from the **Definitions** panel, and right-click the applicable document class. (Expand the Batch class item to select associated document classes.)
3. From the **Context** menu, select **Release Scripts**.



Available Release Scripts:

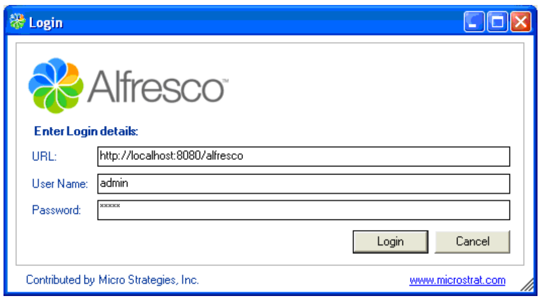
Script Name	Version
Alfresco Kofax Release Script	1.0/1.0
Ascent Capture Database	8.0/8.0
Ascent Capture Text	8.0/8.0

Assigned Release Scripts:

Script Name	Version

The **Release Scripts** dialog box displays, listing all available release scripts. Available release scripts are those that are registered with Kofax Capture.

4. From the **Release Scripts** dialog box, select the Alfresco Kofax Release Script, and click **Add**.



Enter Login details:

URL: http://localhost:8080/alfresco

User Name: admin

Password: *****

Contributed by Micro Strategies, Inc. www.microstrat.com

The **Login** dialog box displays.

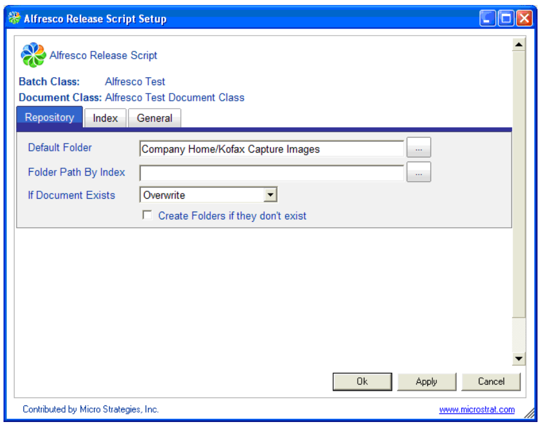
5. Enter your Alfresco server URL, user name, and password.
6. Click **Login**.

Alfresco Kofax Release script configuration tabs

The Kofax Release script is configured using three main tabs. The following sections describe each of these and the options available.

Repository tab

The **Repository** tab is used to configure where documents are stored in the Alfresco repository and how existing documents are handled.



Alfresco Release Script Setup

Alfresco Release Script

Batch Class: Alfresco Test
Document Class: Alfresco Test Document Class

Default Folder: Company Home/Kofax Capture Images
Folder Path By Index:
If Document Exists: Overwrite
Create Folders if they don't exist

Contributed by Micro Strategies, Inc. www.microstrat.com

The Repository tab has the following options:

Default Folder
Defines the root Alfresco space in which documents will be created.

The user that connects to Alfresco must have permission to create documents in this space.

Folder Path by Index
Allows the folder path to be dynamically generated based on indexing values. Substitute Alfresco property name(s) to be used as part of the folder path.

For example, the following will store all documents with the same `Invoice Date` property in folders according to the invoice date:

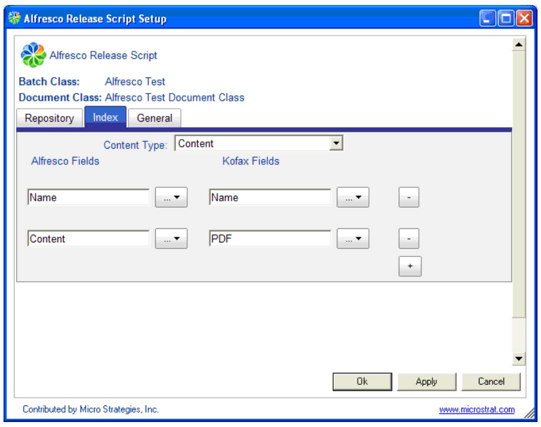
```
Company Home/Invoices/[Invoice Date]
```

If Document Exists
A document already exists if a document of the same name already exists in the folder in which the document is being released. The following defines how the Release script will handle existing documents.

- **Overwrite**: Replaces the document with the one being currently released.
- **Version**: Creates a new version of the document.
- **Release To Default Folder**: If the folder path specified in the **Folder Path By Index** field has an existing document with the same name, the document will be put into the location specified in the **Default Folder** field.
- **Throw Error**: The release fails with the error `Duplicate child name not allowed`.
- **Create Folders if they don't exist**: If selected, this will automatically create folders that do not exist as defined by the previous **Folder Path by Index** settings. If this is not selected, and the folder path(s) do not exist, an error will occur and the document will fail.

Index tab

The **Index** tab defines the Alfresco document type used for released documents, and the mappings between Kofax index fields and Alfresco properties.



Alfresco Release Script Setup

Alfresco Release Script

Batch Class: Alfresco Test

Document Class: Alfresco Test Document Class

Repository | Index | General

Content Type: Content

Alfresco Fields	Kofax Fields
Name	Name
Content	PDF

Ok Apply Cancel

Contributed by Micro Strategies, Inc. www.microstrat.com

Each row defines the mapping between an Alfresco property and a Kofax indexing field. The **Content Type** and **Alfresco Fields** values available can be controlled through configuration.

Content Type
: The Alfresco content type that will be used for documents created by the Release script. It can be a custom content type or content.

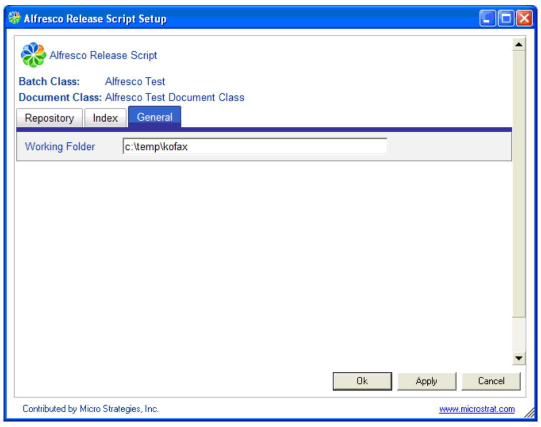
Alfresco Fields
: Use the drop-down list to pick Alfresco properties based on the available types and aspects that will be populated with Kofax Capture index data.

Kofax Fields
: Use the drop-down list to pick the Kofax Capture field to map to the Alfresco property. The **Text Constant** field can provide a fixed text value for the field.

You must define an Alfresco **Name** field and an Alfresco **Content** field, as shown in the previous figure. The **Content** field is used to store the image file, such as Image (TIF), PDF, or Text (OCR).

General tab

The **General** tab defines the working folder used by Kofax Capture for temporary file storage during the release process.



Alfresco Release Script Setup

Alfresco Release Script

Batch Class: Alfresco Test

Document Class: Alfresco Test Document Class

Repository | Index | General

Working Folder: c:\temp\kofax

Ok Apply Cancel

Contributed by Micro Strategies, Inc. www.microstrat.com

Working Folder
: Set this to a folder where the user running the script has write access on the local Kofax Capture machine.

Publishing a batch class

After you select all your batch class settings, you must publish your batch class before you can use it.

The publishing process checks the integrity of the settings in your batch class and makes the batch class available for use. If problems are found with any of the settings, error and warning messages will display, along with the recommended actions for fixing the problems.

If you edit your batch class, you must publish your batch class again before your changes can be used. Your changes will not be applied to batches created before the new publication date.

1. Start the Kofax Capture Administration module to display the main screen.
2. Select the **Batch class** tab from the **Definitions** panel, and right-click the applicable batch class.
3. From the **Context** menu, select **Publish**.
4. From the **Publish** window, select your batch class and click **Publish**.

   Kofax Capture will check all of your batch class settings and display the results in the **Results** box.

   If no problems are detected, the message "Publishing successful" displays. If problems are detected, warning/error messages will display along with recommended actions to resolve the problems. Perform the recommended actions, and then try to publish the batch class again.
5. Run some sample batches through the system to test the operation of the release script.

After successfully publishing, you can create batches based on your batch class. As your batches flow through your Kofax Capture system, they will be routed from module to module. The modules that are used to process a batch, and the order that processing occurs, are specified as part of the batch class definition for the batch.

Refer to the Kofax Capture Help for more information about batch classes.

Releasing batches

The Kofax Capture Release module will process batches based on the settings of the associated batch classes. This module is responsible for releasing documents, as well as index data using the attributes defined during release setup.

The Kofax Capture Release module usually runs as an unattended module on a Windows workstation, periodically polling the module for available batches. It may be configured to run during off-hours to avoid any impact to the throughput of Kofax Capture and/or the network system.

1. Start the Kofax Capture Release module by selecting **Start > Programs > Kofax Capture > Release**.

   All batches queued for release will be processed after initiation of the module.

   Once your batch is released, it will be removed from Kofax Capture. If any documents or pages are rejected, the batch will be routed to the Kofax Capture Quality Control module.
2. To exit the Kofax Capture Release module, select **Batch > Exit** from the module menu bar.

Refer to the Kofax Capture Help for more information about releasing batches.

Advanced configuration: custom types, aspects, and properties

By default, the Release Setup web script (`\service\kofax\releasesetup`) displays all types, aspects, and their associated properties available in your Alfresco repository.

The Release script can be configured to limit this list to only show only those values that are applicable to your use case. A web script configuration file is used to define the items to be displayed.

The Release script configuration file uses a structure similar to that used by the model definitions themselves. Add the types and/or aspects and the relevant properties to the `releasescript.get.config.xml` file to define the options you want available. See the sample configuration provided for examples.

For information on defining your own model for types and aspects, refer to the Alfresco Wiki page **Data Dictionary Guide**.

1. Locate the `releasesetup.get.config.xml.sample` file. For Tomcat this will be located at:

   ```
   tomcat\WEBINF\classes\alfresco\templates\webscripts\com\microstrat\kofax
   \releasesetup.get.config.xml.sample
   ```

   This is the default location used by the Tomcat application server. The location of the file may vary depending on the application server used by your Alfresco installation.
2. Rename `releasesetup.get.config.xml.sample` to `releasesetup.get.config.xml`.
3. Reload your web script using the Web Script Index page as follows:
   a. Go to `http://YOURHOST:8080/alfresco/service/index`.
   b. Click **Refresh Web Scripts**.
4. Open the Release Script **Index** tab.

   This will now only allow selection of types, aspects, and properties as defined in the configuration file.

If an aspect exists with properties and these properties are to be mapped from Kofax to Alfresco, then all properties for this aspect must be populated in the batch process. If certain properties are omitted from the mapping within the release script set up, then when documents are released, the unmapped properties are overwritten with empty strings.

For example, you have an aspect with properties assigned to the default content model and have a document with this aspect assigned. When using Kofax integration, when the document exists `version` option is set, all aspect properties must be mapped and populated in the batch process, otherwise all unmapped properties are overwritten with empty strings (blanked out). This is because in the document exists case, the `version` option uses checkout/check in functionality, which means that the aspect as a whole is repopulated with empty strings if they are unmapped.

The workarounds are:

- Map all properties in the batch process
- Split out your aspects so that unmapped properties are part of different aspects

Removing the Alfresco Kofax Release script

The following steps describe how to remove the Alfresco Kofax Release script from your Kofax installation.

1. Start the Kofax Capture Administration module.
2. Remove the Alfresco Kofax Release script from any document classes using the script:
   a. Right-click the applicable document class. (Expand the batch class item to select associated document classes.)
   b. From the **Context** menu, select **Release Scripts**.
   c. From the **Release Scripts** dialog box, select the Alfresco Kofax Release Script from the list of **Assigned Release Scripts**, and click **Remove**.

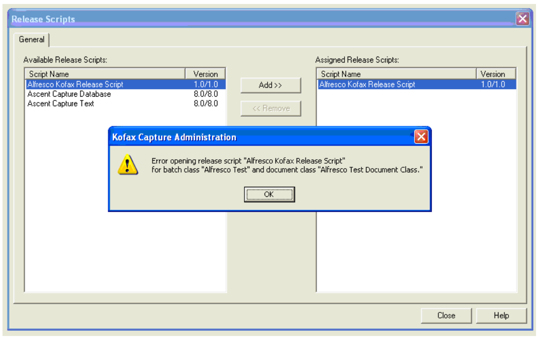
3. Repeat step 2 for all document classes using the Alfresco Kofax Release script.
4. In the Kofax Administration module, click **Tools > Release Script Manager**.
5. Select **Alfresco Kofax Release Script**, and click **Remove**.
6. To remove the installation files, manually delete the following files from your Kofax Capture `bin` directory.
   - `Alfresco.Kofax.Release.Core.dll`
   - `Alfresco.Kofax.Release.Core.Logging.xml`
   - `Alfresco.Kofax.Release.Core.xml`
   - `Alfresco.Kofax.Release.inf`
   - `Alfresco.Kofax.Release.WebScripts.dll`
   - `Antlr.runtime.dll`
   - `Common.Logging.dll`
   - `Jayrock.Json.dll`
   - `log4net.dll`
   - `Spring.Core.dll`

Troubleshooting the Kofax Release script

This section describes how to troubleshoot the Kofax Release script.

Error adding the Alfresco Kofax Release script to a document class

If you see an error message “Error opening release script “Alfresco Kofax Release Script" when adding the script to a document class, it may be an indication that you have not copied the binaries to your Kofax Capture `bin` directory.



Available Release Scripts:

Script Name	Version
Alfresco Kofax Release Script	1.0/1.0
Ascent Capture Database	8.0/8.0
Ascent Capture Text	8.0/8.0

Assigned Release Scripts:

Script Name	Version
Alfresco Kofax Release Script	1.0/1.0

```
Error opening release script "Alfresco Kofax Release Script"
for batch class "Alfresco Test" and document class "Alfresco Test Document Class."
```

Ensure that the following files are in the `bin` directory:

- `Alfresco.Kofax.Release.Core.dll`
- `Alfresco.Kofax.Release.Core.Logging.xml`
- `Alfresco.Kofax.Release.Core.xml`
- `Alfresco.Kofax.Release.inf`
- `Alfresco.Kofax.Release.WebScripts.dll`
- `Antlr.runtime.dll`
- `Common.Logging.dll`
- `Jayrock.Json.dll`
- `log4net.dll`
- `Spring.Core.dll`

Release Error: [Release Script Returned -1. Your release script may need to be re-installed.]

This is a generic Kofax error. The most likely cause is that an invalid working folder has been specified when setting up the release.

Ensure that you have entered a valid folder path in the **Working Folder** field on the **General** tab.

Other causes of this error include missing dependencies in the installation. Check that you have installed all the required files the `bin` directory.

Installing and configuring IBM Lotus Quickr integration

This section provides information on integrating Alfresco with the IBM Lotus software suite of products (Lotus Quickr, Lotus Connections, and Lotus Notes).

Installing the Lotus Quickr AMP

This section describes how to install and configure the AMP that integrates Lotus Quickr with Alfresco.

To integrate Lotus Quickr with Alfresco, you must have already installed Alfresco Enterprise and Lotus Quickr 8.1.1. To use Quickr Connectors with Alfresco, you must also have the following:

- Lotus Notes 8.5
- Microsoft Office 2003 or Microsoft Office 2007
- Windows XP

1. Download the `alfresco-enterprise-quickr-3.4.2.amp` file from the Alfresco Enterprise download area.
2. Unzip the file.
3. Stop the Alfresco server.
4. Copy the `alfresco-enterprise-quickr-3.4.2.amp` file to the `amps` directory.
5. Apply the `alfresco-enterprise-quickr-3.4.2.amp` file into the `alfresco.war` file using the Module Management Tool (MMT).

   Alternatively, for Tomcat, run the `apply_amps` command, which is in the root Alfresco directory. This batch file applies all the AMP files that are located in the `amps` directory.
6. Start your Alfresco server to deploy the newly installed AMP.
7. Move and rename the following files:
   a. `<configRoot>\classes\alfresco\module\ org.alfresco.module.quickr \context\custom-lotus-ws-context.xml.sample` to `<configRoot>\classes \alfresco\extension\custom-lotus-ws-context.xml`
   b. `<configRoot>\classes\alfresco\module\org.alfresco.module.quickr \context\custom-lotus.properties.sample` to `<configRoot>\classes \alfresco\extension\custom-lotus.properties`
8. Open the `custom-lotus.properties` file, and then edit the following settings:

Setting	Description
`lotus.ws.version`	Add the version of Quickr Protocol implemented by Alfresco. The default is 8.0.1. You do not need to change this version for the Technical Preview version of Alfresco AMP file.

Setting	Description
`lotus.server.host`	Add the server host name where Alfresco is installed. For example, `localhost`.
`lotus.server.port`	Add the port number for Quickr to talk with Alfresco. For example, the default is 6060.
`lotus.share.document.url`	`http://${lotus.server.host}:8080/share/page/site/{0}/document-details?nodeRef={1}`
`lotus.share.folder.url`	`http://${lotus.server.host}:8080/share/page/site/{0}/documentlibrary\#path\={1}`
`lotus.share.site.url`	`http://${lotus.server.host}:8080/share/page/site/{0}/dashboard`

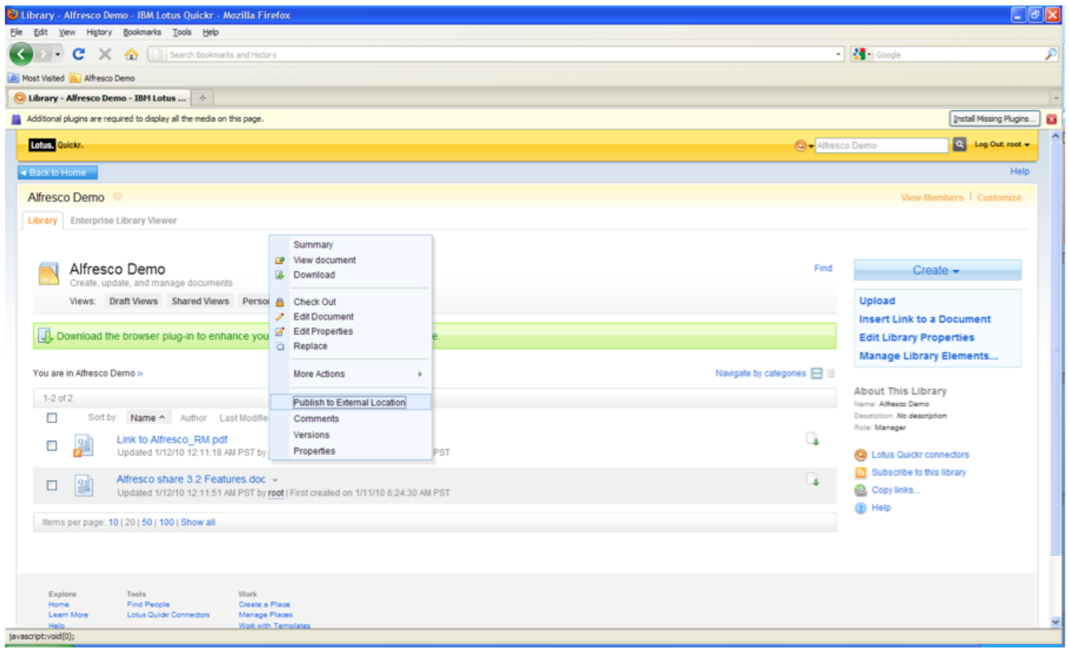
9. Start the Alfresco server.

   Lotus Quickr can now communicate with Alfresco as an ECM server.

Publishing content from Quickr to Alfresco

You can publish documents to Alfresco from the Lotus Quickr Library.

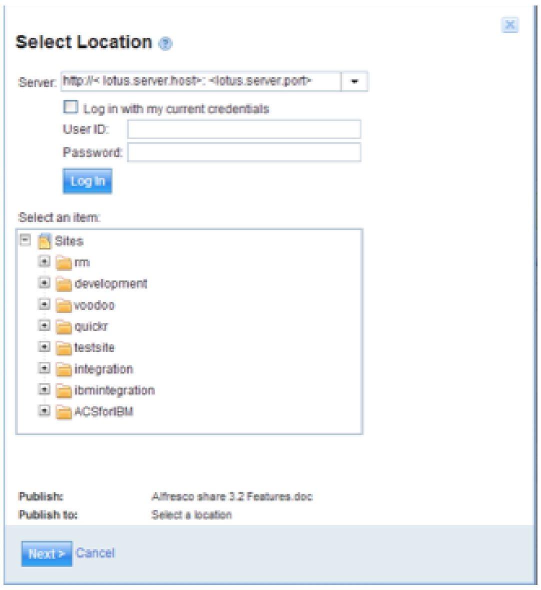
1. In Lotus Quickr, right-click on a document, and then select **Publish to External Location**.


Library - Alfresco Demo - IBM Lotus Quickr - Mozilla Firefox
Alfresco Demo
Library
Enterprise Library Viewer
Summary
View document
Download
Check Out
Edit Document
Edit Properties
Replace
More Actions
Publish to External Location
Comments
Versions
Properties
Create
Upload
Insert Link to a Document
Edit Library Properties
Manage Library Elements...
Link to Alfresco_RM.pdf
Alfresco share 3.2 Features.doc

   You see the location of Alfresco sites.

2. During the publish process, enter the server details and the Alfresco Share login credentials.

   For example, the server details are `http://< lotus.server.host>:<lotus.server.port>` as configured.


Select Location

Server: http://< lotus.server.host>: <lotus.server.port>

☐ Log in with my current credentials

User ID:

Password:

Select an item:

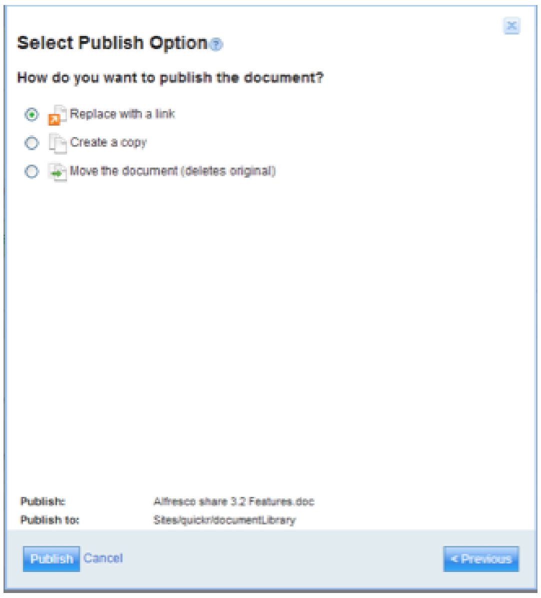
- Sites
  - rm
  - development
  - voodoo
  - quickr
  - testsite
  - integration
  - ibmintegration
  - ACSforIBM

Publish: Alfresco share 3.2 Features.doc

Publish to: Select a location

3. Alfresco supports all the three publishing options that Quickr provides:

   - **Replace with a Link**: the document is removed from Quickr library and added to Alfresco. A link pointing to the document in Alfresco is added to the Quickr Library. Click the link in Quickr to open the document in Alfresco.
   - **Create a Copy**: the document remains in Quickr library, and a copy is added to Alfresco.
   - **Move the Document**: the document is deleted from the Quickr library and is added to Alfresco.


Select Publish Option

How do you want to publish the document?

[✓ Replace with a link]

Create a copy

Move the document (deletes original)

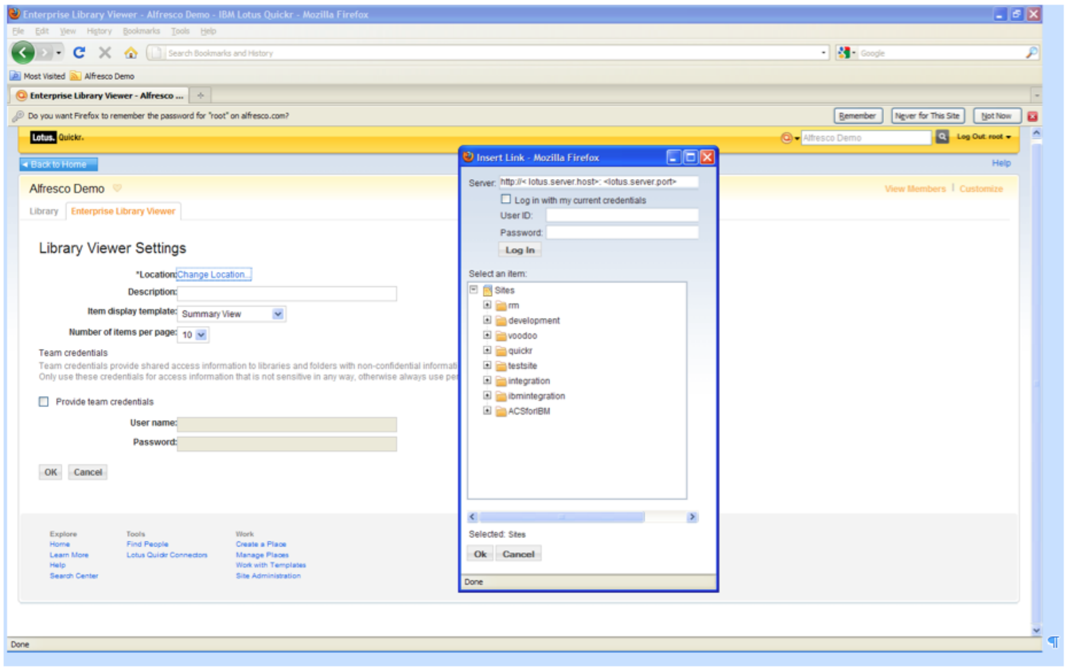
Publish: Alfresco share 3.2 Features.doc

Publish to: Sites/quickr/documentLibrary

Configuring Quickr to browse Alfresco as the Enterprise library

In Quickr, you can use the Enterprise Library Viewer to browse Alfresco as an enterprise library.

1. In Quickr, select the **Enterprise Library Viewer** tab.
2. Browse to Alfresco as an enterprise library.



Enterprise Library Viewer - Alfresco Demo - IBM Lotus Quickr - Mozilla Firefox

Do you want Firefox to remember the password for "root" on alfresco.com?

Alfresco Demo

Library | Enterprise Library Viewer

Library Viewer Settings

*Location: Change Location...
Description:
Item display template: Summary View
Number of items per page: 10

Team credentials
Team credentials provide shared access information to libraries and folders with non-confidential informati
Only use these credentials for access information that is not sensitive in any way, otherwise always use pe

Provide team credentials
User name:
Password:

Insert Link - Mozilla Firefox

Server: http://< lotus.server.host>: <lotus.server.port>
Log in with my current credentials
User ID:
Password:

Select an item:
- Sites
  - rm
  - development
  - voodoo
  - quickr
  - testsite
  - integration
  - ibmintegration
  - ACSforIBM

Selected: Sites

3. To configure the settings, select the **Enterprise Library Viewer** tab, and then select Alfresco as the server location.
4. Browse the sites in Quickr and select content from Alfresco in Quickr.

   The content opens in Alfresco.

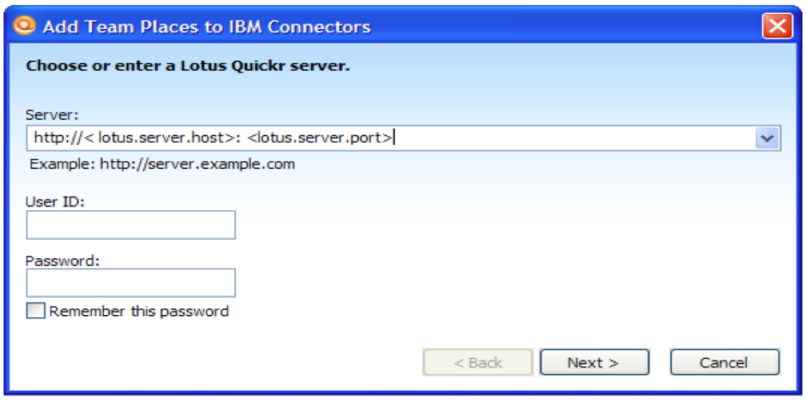
Accessing Alfresco as a Team Place using Quickr connectors

You can also add Alfresco as a Team Place to provide access to Alfresco from the standard Quickr connectors.

This enables you to perform Alfresco content management operations using the following:

- Lotus Notes: Lotus Notes IBM Lotus Notes 8.5
- Microsoft Office 2003 or Microsoft Office 2007
- Microsoft Windows Explorer for Windows XP

1. Access the Connector for which you want to add Alfresco as a Team Place.
2. Add a Team Place, specifying the Alfresco URL (as configured during installation) as the server.



Add Team Places to IBM Connectors

Choose or enter a Lotus Quickr server.

Server:
http://< lotus.server.host>: <lotus.server.port>
Example: http://server.example.com

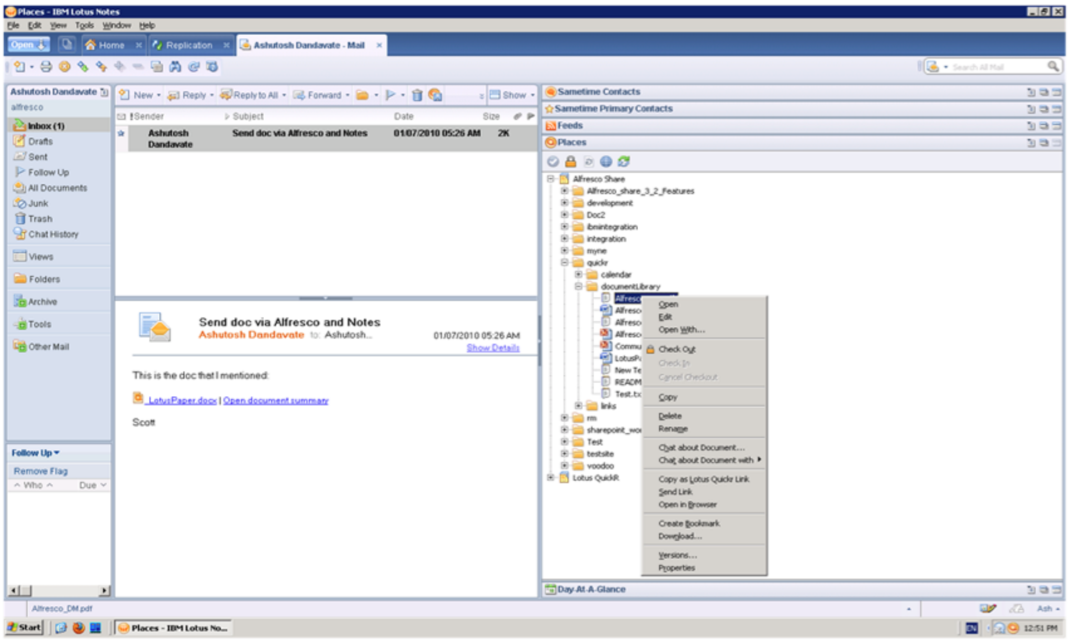
User ID:

Password:

Remember this password

3. From the Team Place, you can perform operations such as check in, check out, versioning, and sending documents as a link using email.

   The following example shows Alfresco Share as Team place in a Lotus Notes client.


Send doc via Alfresco and Notes
Ashutosh Dandavate to Ashutosh... 01/07/2010 05:26 AM

This is the doc that I mentioned

LotusPaper.docx | Open document summary

Scott

Installing and configuring Alfresco XAM Connector

The Alfresco XAM Connector module provides integration between Alfresco and Content Addressable Storage (CAS) systems. XAM is a series of APIs developed to interface with different storage vendor's CAS systems.

CAS systems store and locate files using addresses based on the file’s content, rather than a physical location address. CAS systems are typically used for long-term storage of content that does not require frequent access or where it is stored for regulatory purposes.

When a CAS system stores content, it generates a unique key or hash, which is based on the content. The hash is generated from the content properties, such as the name, date, or content itself. An example hash might be `d8668fbab44d88f8601e625fd88dee84`. This hash is then used as the address of the stored content, and which is then used to retrieve the content. When a request is made to the CAS using this address, it returns the associated content.

The benefits of using CAS systems are:

- Content can be located easily even in large volumes of data
- Content integrity: if stored content has been altered then there is a mismatch between the hash passed as the address and hash computed on the fly
- Avoids redundancy by recognizing that the hash is already present and so does not store it again

The Alfresco XAM Connector module integrates Alfresco with a XAM-enabled Content Access Store (CAS). Currently, this module supports the EMC Centera store.

The module uses a series of properties to control the way that you access the store, and so on. There is also a feature of this module that allows you to set retention policies, such as, preventing content from being deleted for a period of time (for example, retaining invoices for seven years).

The XAM Connector module can be applied to Alfresco Enterprise 3.3.5 or later.

Software prerequisites for XAM Connector module

The Alfresco XAM Connector module supports the EMC Centera.

To use the Alfresco XAM Connector module, you need to ensure that you have the prerequisite software installed on your machine. The software is available from the EMC Community Network.

You will need to register and login to the Community Network before you can access the required software.

Download the following software from these sites:

- Centera VIM and XAM: https://developer-content.emc.com/downloads/centera/download.htm
- Server details and .pea files: https://community.emc.com/docs/DOC-1038
- XAM tools: https://community.emc.com/docs/DOC-2542

Setting up the Centera test environment

These steps describe how to set up the test environment for Centera to integrate with the Alfresco XAM Connector module.

1. Download and extract Centera VIM and XAM into one of the following appropriate directories:

    - (Linux) `/opt/Centera`
    - (Windows) `C:\prog\centera`

    Create a subdirectory structure of the Centera directory to include the following directories:

    ```
    docs
    include
    lib
    lib32
    lib64
    ```

    The following files are also included:

    ```
    Centera_SDK_XAM_VIM_ReferenceGuide.pdf
    Centera_SDK_XAM_Windows_ReleaseNotes.pdf
    ReadMe.txt
    us2_armTest1.pea
    XAM_Arch.pdf
    XAM_C_API.pdf
    XAM_Java_API.pdf
    ```
2. Move the libraries to the relevant `/lib` directory for your system.
    - Choose `/lib32` for 32-bit systems
    - Choose `/lib64` for 64-bit systems
3. Download the Centera `us2_armTest1.pea` file.
4. Move the `us2_armTest1.pea` file to the `/opt/Centera` or `C:\prog\centera` directory.
5. Download and unzip the XAM tools to any location.

The structure of the directory will be similar to the following example (for Windows):

```
13/12/2010  16:03    <DIR>          .
13/12/2010  16:03    <DIR>          ..
09/12/2009  12:44         1,095,932 Centera_SDK_XAM_VIM_ReferenceGuide.pdf
09/12/2009  12:44           350,372 Centera_SDK_XAM_Windows_ReleaseNotes.pdf
13/12/2010  15:54    <DIR>          docs
13/12/2010  15:56    <DIR>          include
13/12/2010  15:56    <DIR>          lib
13/12/2010  15:56    <DIR>          lib32
13/12/2010  15:56    <DIR>          lib64
09/12/2009  12:44             2,344 ReadMe.txt
11/10/2010  12:20               294 us2_armTest1.pea
09/12/2009  12:44         1,402,087 XAM_Arch.pdf
09/12/2009  12:44         1,419,797 XAM_C_API.pdf
09/12/2009  12:44           881,682 XAM_Java_API.pdf
               7 File(s)      5,152,508 bytes
```

```
               7 Dir(s)  91,181,363,200 bytes free
```

The structure of the C:\progs\centera\lib32 directory is similar to the following example:

```
13/12/2010  15:56    <DIR>          .
13/12/2010  15:56    <DIR>          ..
09/12/2009  12:44           839,680 centera_vim.dll
09/12/2009  12:44           831,488 FPCore.dll
09/12/2009  12:44           450,560 fpos32.dll
09/12/2009  12:44         2,011,136 fpparser.dll
09/12/2009  12:44           184,320 FPStreams.dll
09/12/2009  12:44           438,272 FPUtils.dll
09/12/2009  12:44           192,512 FPXML.dll
09/12/2009  12:44           262,144 pai_module.dll
09/12/2009  12:44           401,408 xam.dll
09/12/2009  12:44            64,114 xam.lib
09/12/2009  12:44            53,248 xam_toolkit.dll
09/12/2009  12:44             2,844 xam_toolkit.lib
              12 File(s)      5,731,726 bytes
               2 Dir(s)  91,162,980,352 bytes free
```

The structure of the C:\progs\centera\lib64 directory is similar to the following example:

```
13/12/2010  15:56    <DIR>          .
13/12/2010  15:56    <DIR>          ..
09/12/2009  12:44           940,032 centera_vim.dll
09/12/2009  12:44         1,149,952 FPCore.dll
09/12/2009  12:44           634,368 fpos64.dll
09/12/2009  12:44         2,959,872 fpparser.dll
09/12/2009  12:44           239,616 FPStreams.dll
09/12/2009  12:44           565,760 FPUtils.dll
09/12/2009  12:44           244,224 FPXML.dll
09/12/2009  12:44           439,296 pai_module.dll
09/12/2009  12:44           390,656 xam.dll
09/12/2009  12:44            61,690 xam.lib
09/12/2009  12:44            11,776 xam_toolkit.dll
09/12/2009  12:44             2,826 xam_toolkit.lib
              12 File(s)      7,640,068 bytes
               2 Dir(s)  91,150,495,744 bytes free
```

Configuring the XAM connection

These steps describe how to configure the XAM connection.

1. Open the `<classpathRoot>/alfresco-global.properties` file.
2. Add the `xam.xri` property.

   For example, `xam.xri=snia xam://centera_vim!128.221.200.60?/opt/centera/us2_armTest1.pea`

   The `xam.xri` property specifies the details of the XAM server, which in this case, is `centera_vim!128.221.200.60?`. The property value also includes the location of the Centera `us2_armTest1.pea` file. For example, `/opt/centera/us2_armTest1.pea` or `C:\prog\centera\us2_armTest1.pea`.
3. There are various additional properties that can be set to control the behavior of the XAM Connector module.

   For example, the retention period for storing content is `xam.archive.retentionPeriodDays=1`.

   The sample `alfresco-global.properties` file supplied in the XAM connector AMP provides example settings and values.
4. Save the `alfresco-global.properties` file.
5. Ensure Java can find the libraries by setting the `PATH` and `LD_LIBRARY_PATH` environment variables.

For example:

```
export PATH=$PATH:/opt/centera/lib64
export LD_LIBRARY_PATH=/opt/centera/lib64
```

Alfresco XAM Connector module properties

The following properties can be set for the XAM connector module.

Set the Alfresco XAM Connector module properties are set in the `alfresco-global.properties file`.

snia-xam://centera_vim!128.221.200.60?/opt/centera/us2_armTest1.pea xam.xri=
Specifies the full XAM connection string.

xam.archive.storeName=xamArchive
Specifies the name of the XAM store that will be used by the `xam:archive` behavior.

xam.archive.retentionPeriodDays=0
Specifies the number of days to retain a XAM document. Use `0` to ignore; `>0` days to retain.

xam.archive.addLock=true
Specifies whether to add the `cm:lockable` aspect automatically. Set to true to apply a lock when the aspect is added; set to false to not apply a lock

xam.archive.cronExpression=0 0 21 * * ?
Specifies a cron expression for the XAM archive cleaner job.

xam.archive.bindingPropertiesPattern=vnd\\.com\\.alfresco\\..*
Specifies the pattern for all binding properties. Any property (full property name at time of writing) that does not match will be written as non-binding. For example, `vnd\\.com\\.alfresco\\..*` will match all properties prefixed with `vnd.com.alfresco`. Refer to http://download.oracle.com/javase/tutorial/essential/regex/, also http://download.oracle.com/javase/6/docs/api/.

xam.archive.app.vendor= xam.archive.app.name= xam.archive.app.version= xam.archive.app.db=${db.url}
The XAM well-known properties, which will be automatically populated.

xam.archive.globalPropertiesPrefix=vnd.com.alfresco. xam.archive.globalPropertiesToWrite=xam.archive.app.vendor, xam.archive.app.name, xam.archive.app.version, xam.archive.app.db
The list of global properties to add to the XSet (comma-separated). For example, `${xam.archive.globalPropertiesPrefix}xam.archive.app.vendor`. This can be a list of any value that can be set in the `alfresco-global.properties` file but you should import any required properties using variable replacement to get consistent naming.

xam.archive.contentFieldName=${xam.archive.globalPropertiesPrefix}content
Specifies the name of the property against which to store content.

xam.archive.nodePropertiesPrefix=xam.archive.node. xam.archive.nodePropertiesToWrite=sys:ref, sys:path, cm:name, cm:created, cm:creator, cm:owner
The list of node properties to add to the XSet (comma-separated, namespace-prefixes). For example, `${xam.archive.globalPropertiesPrefix}${xam.archive.nodePropertiesPrefix}cm:name`. Properties that are not present on the node are ignored. Implicit properties are generated and can be listed, for example, `sys:ref`, `sys:path`.

xam.archive.forceBackgroundStoreMove
Specifies whether to move content to the XAM store immediately or as a background job. The aspect `xam.archivemodel:archivePending` is added to the document, pending the move to the XAM store. Set to true to move the content binaries to XAM as soon as the retention date is set. Set to false to move the content when the scheduled job runs.

Testing the XAM connection

These steps describe how to test the XAM connection.

The shXAM tool is provided within the XAM tools. Use the shXAM tool to connect to the XAM server using the `xam.xri` property that you specified in the `alfresco-global.properties` file.

1. Run the shXAM tool.
2. Run the following command:

   ```
   connect snia-xam://centera_vim!128.221.200.60?/opt/centera/
   us2_armTest1.pea
   ```

   An example of the output is as follows:

   ```
   shXAM>connect snia-xam://centera_vim!128.221.200.60?/opt/centera/
   us2_armTest1.pea

   Connected to an XSystem with XRI: snia-xam://centera_vim!128.221.200.60?/
   opt/centera/us2_armTest1.pea
   ```

Installing the XAM Connector module

These steps describe how to install the XAM Connector module to an instance of Alfresco.

The XAM Connector module functionality is packaged as an Alfresco Module Package (AMP) file.

1. Browse to the Alfresco Support Portal.

   http://support.alfresco.com
2. Download the `alfresco-xamconnector-<release_number>.amp` file.

   For example:

   ```
   alfresco-xamconnector-3.4.2.amp
   ```
3. Use the Module Management Tool (MMT) to install the AMP. If your Alfresco installation is running within the Tomcat application server, you can use the `<installLocation>\bin\apply_amps` command to apply all AMP files that are located in the amps directory.
4. Restart the Alfresco server.

   Note the following message in the logs:

   ```
   Starting module org_alfresco_module_xamconnector version 1.0.
   ```

Testing the XAM Connector module

These steps describe how to test the XAM Connector module with Alfresco.

1. Enable `DEBUG` logging for the Alfresco XAM components.

   For example:

   ```
   log4j.logger.org.alfresco.enterprise.repo.content.xam=DEBUG
   log4j.logger.org.alfresco.enterprise.repo.xam=DEBUG
   ```
2. Add the `xam:archived` aspect in the `share-config-custom.xml` file.

   For example:

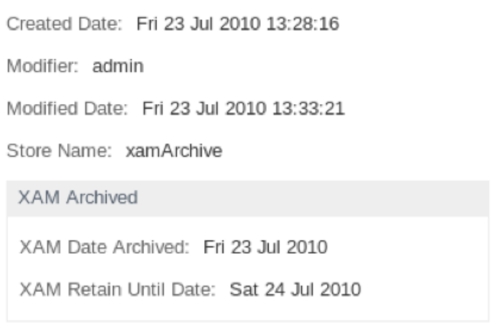
   ```
   <alfresco-config>

      <config evaluator="node-type" condition="cm:content">
         <forms>
            <form>

               <!-- 2 column template -->
               <edit-form />

               <field-visibility>
   ```

```
            <!-- aspect: cm:storeSelector -->
            <show id="cm:storeName" />

            <!-- aspect: xam:archive -->
            <show id="xam:dateArchived" for-mode="view" />
            <show id="xam:retainUntil" for-mode="view" />

            <show id="cm:content" for-mode="view" />

            </field-visibility>
            <appearance>
               <!-- Store Selector -->
               <field id="cm:storeName" label="Store Name"
 description="Content Store Name" />
               <set id="xam-archive" appearance="bordered-panel"
 label="XAM Archived" />
               <field id="xam:dateArchived" label="XAM Date Archived"
 set="xam-archive" />
               <field id="xam:retainUntil" label="XAM Retain Until Date"
 set="xam-archive" />

            </appearance>
         </form>
      </forms>
   </config>

<config evaluator="string-compare" condition="DocumentLibrary">
   <aspects>
         <visible>
            <aspect name="cm:storeSelector" label="Store Selector"/>
            <aspect name="xam:archive" label="XAM Archive" />
         </visible>
         <addable>
            <aspect name="xam:archive" label="XAM Archive" />
         </addable>
   </aspects>
</config>

</alfresco-config>
```

3. Create a sample document.

   For example, `abc.txt`.

4. Apply the `xam:archived` aspect to the document.



Created Date: Fri 23 Jul 2010 13:28:16

Modifier: admin

Modified Date: Fri 23 Jul 2010 13:33:21

Store Name: xamArchive

XAM Archived

XAM Date Archived: Fri 23 Jul 2010

XAM Retain Until Date: Sat 24 Jul 2010

5. View the metadata for the document.

   You must also ensure that the new store is the **xamStore** and that the **retainedUntil** date is set.

6. Use the Node Browser to locate the content URL for the node.

   The URL must be a XAM XRI-based URL. The debug output should also show the XUID used.

7. Copy the XAM XRI, and then open the XSet using the shXAM tool.

For example:

```
shXAM>openxset
 AAAEcwA9f4xCRlE4MU1OM1Q4NzRGZTIySkQ5NVFINjM2RUNHNDE1SkpPRDlCUDFHQkdMUExMQVJMTlNMR

XSet opened
```

a. Use the following command to check that the base retention has been set:

   `viewFields .xset.retention.base`

b. Use the following command to check that node properties have been copied over:

   `viewFields xam.archive`

Setting up the XAMContentStore as the primary store

These steps describe how to set up the XAMContentStore to be the primary store for all content. This setup relates to new content and cannot be done retrospectively, unless all content is moved from the file system to XAM.

1. Create a bean called `fileContentStore` that uses the XAMContentStore.
2. Copy the `org_alfresco_module_xamconnector_xamContentStore` bean to a custom context and rename it `fileContentStore`.

Installing and configuring Alfresco DocLib Portlets

This describes how to install and configure Alfresco DocLib Portlets within Liferay. DocLib Portlets provide the rich document management capabilities of the Share Document Library page component within a portal. This feature consists of three portlets for accessing Share sites and the Alfresco repository. In the Share sites portlet, you have access to the sites you are already a member of and all public sites.

Once deployed to Liferay, you will be unable to log in to the native Share application. Therefore, to create and manage Share sites (including managing site membership and accessing other functionality outside the Document Library component), you will require a second Share instance deployed to a separate Tomcat server.

Before proceeding with the installation and configuration, ensure the following:

- The Alfresco repository (`alfresco.war`) running must be Enterprise 3.3.3 or later.
- Alfresco has been installed using the installers or is running in a Tomcat 6 container.
- Liferay Portal 5.2.3 is installed and working.
- The administrative user knows the location to which Liferay is deployed.
- The required modifications have been completed if you are using Tomcat 6. The modifications must be made for both Alfresco and Liferay if you are using different servers.
- The deployed version of `share.war` in Liferay must be the same as the deployed version of `alfresco.war`.

DocLib Portlets capabilities

The Share DocLib Portlets include most of the functionality available in a standard Share Document Library.

The following Document Library features are not available in DocLib Portlets:

- The **View in Alfresco Explorer** action is not available for folders.
- When viewing the Details page for a folder or content item, the **Share** section does not display.

- User names do not link to the related Profile page.

As the Share header does not display in the DocLib Portlet, the following framework functionality is not available:

Share toolbar:
My Dashboard, My Profile, Sites menu, People Finder, Search, Help, Logout

Other page components:
Wiki, Blog, Calendar, Links, Discussions, Data Lists

Site dashboard:
Invite, Customize Dashboard, Edit Site Details, Customize Site, Leave Site

Refer to the Document Library page component section of the Share User Help for full details of the functionality available.

Configuring Liferay

If you are running Liferay and Alfresco on the same machine, you need to change the port numbers used by the Liferay Tomcat server to prevent conflicts.

1. Open the `<LIFERAY_HOME>/tomcat-6.0.18/conf/server.xml` file.
2. Locate the following lines and update the port numbers as shown:
   ```
   <Server port="8105" shutdown="SHUTDOWN">

       <Connector port="8180" protocol="HTTP/1.1"
                  connectionTimeout="20000"
                  redirectPort="8443" URIEncoding="UTF-8" />

       <Connector port="8109" protocol="AJP/1.3" redirectPort="8443"
   URIEncoding="UTF-8" />
   ```
3. Save the file.

Configuring Alfresco

This task describes how to configure Alfresco for Doclib Portlets.

1. Browse to `<ALFRESCO_HOME>/tomcat/shared/classes/alfresco/`.
2. Open the file `alfresco-global.properties`.
3. Add the following:
   ```
   authentication.chain=alfrescoNtlm1:alfrescoNtlm,external1:external
   external.authentication.proxyUserName=
   ```
4. Save the file.

Configuring the Liferay Share web application

This task describes how to deploy the web application.

1. Deploy the Share web application to Liferay by copying the `share.war` file from your Alfresco Tomcat instance into Liferay's `deploy` folder.
2. Locate the `<LIFERAY_HOME>/tomcat-6.0.18/conf/catalina.properties` file and open it in an editor.
3. Locate the `shared.loader` property and set it to the following value:
   ```
   shared.loader=${catalina.home}/shared/classes,${catalina.home}/shared/
   lib/*.jar
   ```
4. Create the directory `<LIFERAY_HOME>/tomcat-6.0.18/shared/classes/alfresco/web-extension/`.

5. Add the following configuration to a new file called `share-config-custom.xml`.

   If your Alfresco Tomcat instance is running on another host or a non-standard port, you must modify the endpoint-url parameters to point to the correct location of your repository. For example:

```
<alfresco-config>
   <!-- Overriding endpoints to reference a remote Alfresco server
 -->
   <config evaluator="string-compare" condition="Remote">
     <remote>

       <endpoint>
         <id>alfresco-noauth</id>
         <name>Alfresco - unauthenticated access</name>
         <description>Access to Alfresco Repository WebScripts that
 do not require authentication</description>
         <connector-id>alfresco</connector-id>
         <endpoint-url>http://localhost:8080/alfresco/s</endpoint-
url>
         <identity>none</identity>
       </endpoint>

       <endpoint>
         <id>alfresco-feed</id>
         <name>Alfresco Feed</name>
         <description>Alfresco Feed - supports basic HTTP
 authentication</description>
         <connector-id>http</connector-id>
         <endpoint-url>http://localhost:8080/alfresco/s</endpoint-
url>
         <basic-auth>true</basic-auth>
         <identity>user</identity>
       </endpoint>

       <connector>
         <id>alfrescoCookie</id>
         <name>Alfresco Connector</name>
         <description>Connects to an Alfresco instance using cookie-
based authentication</description>

 <class>org.springframework.extensions.webscripts.connector.AlfrescoConnector
class>
       </connector>

       <endpoint>
         <id>alfresco</id>
         <name>Alfresco - user access</name>
         <description>Access to Alfresco Repository WebScripts that
 require user authentication</description>
         <connector-id>alfrescoCookie</connector-id>
         <endpoint-url>http://localhost:8080/alfresco/wcs</endpoint-
url>
         <identity>user</identity>
         <external-auth>true</external-auth>
       </endpoint>

     </remote>
   </config>

 </alfresco-config>
```

Creating Liferay users

This task describes how to create the Liferay users.

Ensure that the Alfresco server is started first, and then start up Liferay. Check that no errors are recorded in the application logs.

1. Log in to Liferay as an administrator user.
2. Create a new user account for each of the Alfresco users that you wish to give access to the portal.

   The users must have already been set up in Alfresco with the correct permissions. The screen name of the user in Liferay must match their Alfresco user name.

Adding portlets to Liferay

This task describes how to add the portlets to Liferay.

Ensure that the Alfresco server is started first, and then start up Liferay. Check that no errors are recorded in the application logs.

1. Log in to Liferay.
2. Create a new page and set the layout to one full-sized portlet.
3. In the **Add Application** menu, expand **Alfresco** and select **Share: My Document Libraries**.

   Liferay creates the My Document Libraries portlet.
4. Create another page with the same layout and add the **Share: Repository Browser** portlet.
5. Create another full-sized page and add the **Share: Site Document Library** portlet. A message displays indicating that the portlet must be configured before use. Select the portlet **Preferences** option, and then select the site to which the portlet will be bound.

   Each of the three Alfresco Share portlets must be deployed to its own Liferay page. There is no support for deploying more than one portlet to the same page.

Installing Microsoft Office Add-ins

This task describes how to install Alfresco Add-ins for Microsoft® Office applications, such as Word, Excel, and PowerPoint. The Alfresco Add-Ins have been designed for Microsoft Office 2003.

Before you start, make sure that:

- The .NET Programmability Support option is installed for each of the Office applications that you are installing the Add-ins (such as Word, Excel, and PowerPoint). To find these options, run the Office Setup program and expand the list of available options for each application. You may require your original Office 2003 install media to add these required components.
- The installing user has Windows administrator privileges.
- Any Microsoft Office applications on your system are NOT running, including Outlook if you use Word as an email editor.

If you are running Office 2007 on Windows Vista, note that Microsoft have rewritten the WebDAV parts of Vista which means you will experience READ ONLY access to the Alfresco repository over WebDAV. This is a known problem with Vista and affects many applications, including Microsoft's own SharePoint Server. There is no known workaround at the time of writing. CIFS access is unaffected and works as it does with Windows XP. Therefore, use CIFS to obtain read/write access to Alfresco using Windows Vista.

1. Browse to the Alfresco Enterprise download area.

2. Run the Microsoft setup file:

   `alfresco-enterprise-office-addins-3.4.2.zip`

   This example refers to the Office installer that installs all three Add-ins. You can also use individual installers to add Alfresco to one of the three Office applications.

   These individual installers are:

   - `alfresco-enterprise-word2003-addin-3.4.2.zip`
   - `alfresco-enterprise-excel2003-addin-3.4.2.zip`
   - `alfresco-enterprise-powerpoint2003-addin-3.4.2.zip`
3. Run `setup.exe`.

   If required, the setup program will download the required components from the Microsoft website. These components are .NET 2.0 framework, and Visual Studio 2005 Tools for Office Second Edition runtime.

   The setup is complete.
4. Run the Office application, for example, run Word.

   A Welcome window with configuration options displays. You can return to the configuration options at any time using the link at the bottom of the Add-In window.
5. In the **Web Client URL** field, enter the location of Alfresco Explorer.

   For example: `http://server:8080/alfresco/`
6. In the **WebDAV URL** field, append `webdav/` to the Alfresco Explorer URL.

   For example: `http://server:8080/alfresco/webdav/`
7. In the **CIFS Server** field, enter the path to the CIFS server. The Add-in will try to auto-complete this value, but you should verify for the correct address.

   For example: `\\server_a\alfresco\` or `\\servera\alfresco\`

   If you intend to use the CIFS interface to save documents via the Add-in, it is very important that you are authenticated automatically. Limitations in the Microsoft Office APIs mean that an error is shown instead of an authentication dialog box if the Alfresco CIFS interface rejects your connection attempt. If you are not in an Enterprise environment, where it may not be possible to configure automatic authentication, you can map a network drive to the Alfresco CIFS interface instead.
8. In the **Authentication** area, enter your Alfresco user name and password.

   The Add-In will always try to automatically log you in to Alfresco in order to present your checked-out documents and your assigned tasks. If you are using the CIFS interface, authentication is usually automatic. However, sometimes the Add-In needs to present your Alfresco user name and password for authentication. It is recommended that you enter and save your Alfresco credentials. All values are stored in the Windows registry and your password is encrypted against casual hacking attempts.
9. Click **Save Settings**.

Setting up Microsoft Office Add-ins to work with HTTPS

This section describes how to configure the Alfresco server and a client machine to run the Alfresco Microsoft Office Add-ins over HTTPS.

1. Use the Java `keytool` utility to generate a key pair for further HTTPS connections for Tomcat.

   For example:

   ```
   %JAVA_HOME%\bin\keytool.exe -genkeypair -alias alfresco -keystore
   ```

```
   D:\temp\keystore.jks -storepass changeit -keypass changeit  -keyalg
RSA -validity 360
   -keysize 2048 -storetype JKS
```

If you use a different tool, refer to the relevant vendor's documentation.

Your certificate (created in the remaining sections) must be `VALID` for the appropriate host name and trusted to be able to communicate with Alfresco without warnings and errors. If you see warnings and errors with the HTTPS configuration, double check your certificate.

a. Configure the key pair using the following method:

   When prompted to enter the **First Name and Last Name**, enter a host DNS name. For example, if you are using Alfresco in the Intranet and you are using the host with a URL `https://my-host-name:8443/alfresco, enter my-host-name` as a value for the **First Name and Last Name** field. This is required to prevent Internet Explorer from requesting details about a valid certificate or host. If you are using URL such as `https://www.alfresco.org/alfresco`, your **First Name and Last Name** field value should be `www.alfresco.org`.

b. Export the generated associated certificate into a file.

```
%JAVA_HOME%\bin\keytool.exe -exportcert -alias alfresco -file
   D:\temp\alfresco-ssl.cer -keystore  D:\BUGS\ALF-6390\keystore.jks
 -storepass changeit
   -storetype JKS
```

2. Configure Tomcat using the HTTPS connector.
3. Add the generated certificate to the Windows **Trusted Root Certification Authorities** on each client machine using one of the following two methods.

   Method One:

   a. Run the Certificate Manager (`certmgr.msc`).
   b. Navigate to **Certificates - Current User** > **Trusted Root Certification Authorities** > **Certificates**.
   c. Right-click on the **Certificates** node in the tree and invoke **All Tasks** > **Import..** from the context menu.

   Method Two:

   a. Invoke an installation of the certificate from Internet Explorer.

      From IE6 or IE7, navigate to `https://my-host:8443/alfresco` and on the **Security Alert** window, click **View Certificate**.

      From IE8, navigate to `https://my-host:8443/alfresco`, select Certificate Error, and then click **View certificates**.
   b. View the certificate and then click **Install certificate...** .
   c. Click **Next** to run through the steps in the wizard.
   d. On the Certificate Store page, select the option **Place all certificates in the following store**.
   e. Click **Browse**, and then select the **Trusted Root Certification Authorities** store.
   f. Click **Finish** to complete the certificate import.
   g. At the security warning, click **Yes** to install the certificate.

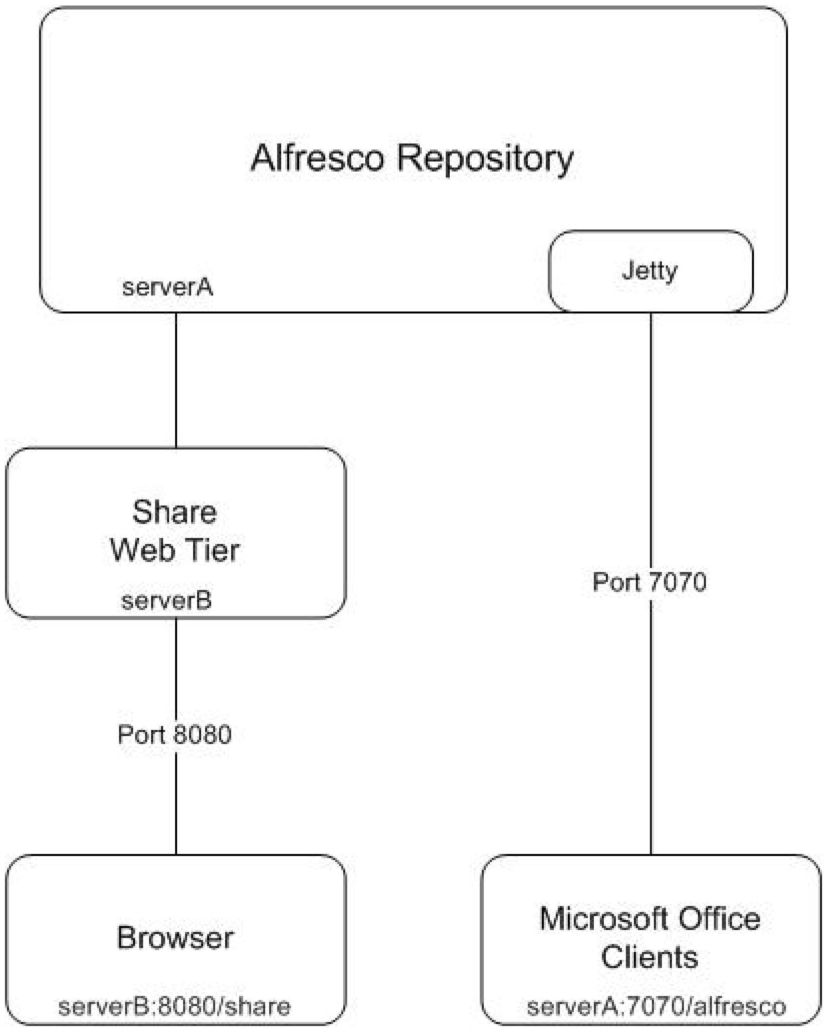
When the certificate is added to the Trusted Store, you will be able to work with Alfresco Office Add-In via HTTPS.

Installing and configuring Microsoft Office SharePoint Protocol Support

The Microsoft Office SharePoint Protocol Support offers Microsoft users greater choice by providing a fully-compatible SharePoint repository that allows the Microsoft Office Suite applications (for example, Word, PowerPoint, Excel) to interact with Alfresco as if it was SharePoint. This enables your users to leverage the Alfresco repository directly from Microsoft Office.

You can also use Microsoft Office SharePoint Protocol Support to enable online editing for Office documents within Alfresco Share. It enables your users to modify Office files without checking them in and out. Alfresco locks the file while it is being modified and releases the lock when the file is saved and closed.

The following diagram shows the architecture of the SharePoint Protocol Support in relation to an Alfresco installation.



The SharePoint Protocol Support architecture embeds a Jetty web server within the Alfresco repository. The Microsoft Office clients communicate directly with the Jetty server using WebDAV-like calls with proprietary extensions and on different port number from Alfresco Share. This port number can be configured in the SharePoint Protocol Support properties files.

Installing the SharePoint Protocol Support AMP

The SharePoint Protocol support functionality is installed from an Alfresco AMP. If you use the Windows or Linux installers to install Alfresco, the SharePoint Protocol Support is installed by default. These instructions describe how to install the SharePoint Protocol Support into the Alfresco WAR.

When you install this file, it responds to the SharePoint requests from Office, and therefore allows Alfresco to appear as the SharePoint server.

1. Shut down your Alfresco server.
2. Browse to the Alfresco Enterprise download area.
3. Download the `alfresco-enterprise-spp-3.4.2.zip` file.
4. Move the `vti-module.amp` file to the `amps` directory.
5. Install the `vti-module.amp` file into the `alfresco.war` file using the Module Management Tool (MMT).

   The `vti-module.amp` file holds the functionality for the SharePoint connector.

   For Tomcat, alternatively, run the `apply_amps` command in the Alfresco `\bin` directory, which applies all the AMP files that are located in the `amps` and `amps_share` directories.
6. Start your Alfresco server to expand the directory structure.
7. Verify that you have applied the SharePoint AMP to Alfresco by checking that you have the following directory:

   ```
   /webapps/alfresco/WEB-INF/classes/alfresco/module/
   org.alfresco.module.vti/context
   ```

Configuring SharePoint Protocol Support

This section describes how to configure the SharePoint Protocol Support properties to complete the set up process.

Ensure that you have applied the SharePoint Protocol Support AMP.

The SharePoint Protocol Support functionality uses the properties in the default configuration file called `vti.properties` in `<TOMCAT_HOME>/webapps/alfresco/WEB-INF/classes/alfresco/module/org.alfresco.module.vti/context`. The properties have a format of `vti.share.*`.

These properties do not need to be changed as they point to specific pages in Share. However, if, for example, you wish to run the repository and Share on different machine, you may need to modify the first three properties (`vti.server.*`). Set your custom properties and overrides in the `alfresco-global.properties` file.

1. Open the `alfresco-global.properties` file.
2. The following table describes the full list of properties that you can add.

Property	Description
`vti.server.port`	This property configures the port on which the SharePoint server listens. This is the port for the vti embedded server. The default port number is 7070. Use this port in File Open/ Save windows and for Document Workspace creation.

Property	Description
`vti.server.external.host= ${localname}vti.server.external.port= ${vti.server.port}`	These values are used by Share to generate the **Edit Online** link, which opens the document using the SharePoint module. These parameters are used by `vti-server.get` web script. Share uses this script to determine vti host and port.
`vti.share.siteInBrowser=/page/ site/.../dashboard`	If you click the **Open site in browser** link in the **Shared Workspace** panel, the site dashboard will open in a browser. This property generates the browser URL. Dots in this template are replaced with the site `shortname`.
`vti.share.siteSettings=/page/ site/.../customise-site`	This property generates the Share URL for **Change Site Settings**.
`vti.share.siteGroupMembership=/ page/site/.../site-members`	This property generates the Share URL for the **Site Group Membership** page.
`vti.share.userInformation=/page/ user/.../profile`	This property generates the Share URL for the **Edit User Information** page.
`vti.share.documentLibrary=/page/ site/.../documentlibrary`	This property is not used.
`vti.share.documentDetails=/page/ site/.../document-details`	This property generates the Share URL for the **Modify settings for document version**s page. This link is in the Version History.
`vti.share.calendar=/page/site/.../ calendar`	This property is used only for Outlook. The SharePoint Protocol Support module generates the Share URL for Outlook Meeting Workspace and places this link to mail template.

The value for the context path of the Alfresco repository being used is specified using the sysAdmin subsystem property `alfresco.context`. The default is `alfresco`.

3. Save the `alfresco-global.properties` file.
4. Restart your Alfresco server.

The Microsoft SharePoint Protocol Support functionality is installed and configured.

Configuring SharePoint Protocol for Online Editing

The following issues are known for configuring the SharePoint Protocol for Online Editing

- There is a known issue with Office 2003 and 2007 Office documents opening as read-only in Internet Explorer for all versions before Vista SP1.

  Refer to the knowledge base article 870853 on the Microsoft website to enable the Online Editing functionality.
- To use Online Editing on Windows 7, you must set `BasicAuthLevel` in the registry.

  Basic authentication is disabled on Office 2010 by default. To enable it, create or edit the following registry key: `HKCU\Software\Microsoft\Office\14.0\Common\Internet: BasicAuthLevel=2`.

  Alternatively, use Pass-through or Kerberos authentication.

  It is important to set the `vti.server.external.host` and `vti.server.external.port` properties in the `alfresco-global.properties` file to the externally resolvable host and port name that SharePoint clients will communicate with. These properties default to the host machine's local name and port 7070, respectively. These values are used by Share to generate the **Edit Online** link, which opens the document using the SharePoint module.

Setting up sticky sessions with SharePoint Protocol Support

This section describes how to configure sticky sessions in a high availability environment with the SharePoint Protocol Support embedded Jetty server.

The SharePoint Protocol Support module uses an embedded jetty server (running on port 7070) which receives the client's SharePoint Protocol requests and then communicates with the Alfresco services. When using a clustered environment (for example, two nodes with shared content) using a load balancer between the nodes and the clients, you should set sticky sessions for the SharePoint Protocol Support module.

1. Open the `alfresco-global.properties` file for each cluster node.
2. Set the `vti.server.sessionIdManager.workerName` property for the VTI server. For example:

   For Alfresco node 1:

   ```
   vti.server.sessionIdManager.workerName=Alfresco1
   ```

   For Alfresco node 2:

   ```
   vti.server.sessionIdManager.workerName=Alfresco2
   ```
3. Configure the load balancer stickyness.

   For example, in apache 2.2 using `mod_proxy` and `mod_proxy_balancer`.

   ```
   # map to cluster with session affinity (sticky sessions)
   ProxyPass /balancer !
   ProxyPass / balancer://my_cluster/ stickysession=jsessionid
    nofailover=On

   <Proxy balancer://my_cluster>
       BalancerMember http://yourjetty1:7070 route=Alfresco1
       BalancerMember http://yourjetty2:7070 route=Alfresco2
   </Proxy>
   ```

Setting up SharePoint Protocol Support to work with HTTPS

This section describes how to configure the Jetty server so that the SharePoint Protocol Support will run over HTTPS.

1. Open the `vti-context.xml` file.
2. Configure `SslSocketConnector` for Jetty.
3. Comment out the existing `vtiServerConnector` bean, and then paste the following replacement bean:

   ```
       <bean id="vtiServerConnector"
    class="org.mortbay.jetty.security.SslSocketConnector">
        <property name="port">
        <value>${vti.server.port}</value>
        </property>
           <property name="headerBufferSize">
                <value>8192</value>
           </property>
           <property name="maxIdleTime">
                <value>30000</value>
           </property>
           <property name="keystore">
                <value>D:/BUGS/ALF-6390/keystore.jks</value>
   ```

```
        </property>
        <property name="keyPassword">
             <value>changeit</value>
        </property>
        <property name="password">
             <value>changeit</value>
        </property>
        <property name="keystoreType">
             <value>JKS</value>
        </property>
    </bean>
```

For more information, refer to http://docs.codehaus.org/display/JETTY/Ssl+Connector+Guide and http://jetty.codehaus.org/jetty/jetty-6/apidocs/org/mortbay/jetty/security/SslSocketConnector.html.

This example configures HTTPS using the default port 7070, which avoids rewrites in some configuration files and templates.

4. Use the Java `keytool` utility to generate a key pair for the connector:

   ```
   %JAVA_HOME%\bin\keytool.exe -genkeypair -alias alfresco -keystore
       D:\BUGS\ALF-6390\keystore.jks -storepass changeit -keypass changeit
    -keyalg RSA -validity 360
       -keysize 2048 -storetype JKS
   ```

   Use the same store in this command and in the `vtiServerConnector keystore` property.
5. Export the generated associated certificate into a file.

   ```
   %JAVA_HOME%\bin\keytool.exe -exportcert -alias alfresco -file
       D:\BUGS\ALF-6390\alfresco-ssl.cer -keystore  D:\BUGS
   \ALF-6390\keystore.jks -storepass changeit
       -storetype JKS
   ```
6. Configure Alfresco and Tomcat for HTTPS following the instructions on the Apache website http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

   It is possible to use the same key store for Tomcat and Jetty.
7. Ensure that you set the sysAdmin subsystem properties.
8. Configure Share to connect to Alfresco using SSL.
   a. Import the certificate into a Java Trusted Store.

      This allows Java to connect successfully to the Alfresco context using HTTPS.

      ```
      %JAVA_HOME%\bin\keytool.exe -importcert -alias alfresco -file D:\BUGS
      \ALF-6390\alfresco-ssl.cer -keypass changeit -noprompt -trustcacerts -
      storetype
      JKS -keystore %JAVA_HOME%\jre\lib\security\cacerts -storepass changeit
      ```

      Note!

      The `keystore` parameter points to the Java trusted cacerts file for JDK, which is configured for Tomcat. For example, `%JAVA_HOME%\jre\lib\security\cacerts`. For more information on trusted certificates in Java, refer to http://download.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html#Certificates
   b. Locate the `<web-extension>\share-config-custom.xml` file and edit or create following section.

      The following example shows the default HTTPS port as 8443.

      ```
      <config evaluator="string-compare" condition="Remote">
            <remote>
               <endpoint>
      ```

```
            <id>alfresco-noauth</id>
            <name>Alfresco - unauthenticated access</name>
            <description>Access to Alfresco Repository WebScripts that
 do not require authentication</description>
            <connector-id>alfresco</connector-id>
            <endpoint-url>https://localhost:8443/alfresco/s&lt;/
endpoint-url>
            <identity>none</identity>
         </endpoint>

         <endpoint>
            <id>alfresco</id>
            <name>Alfresco - user access</name>
            <description>Access to Alfresco Repository WebScripts that
 require user authentication</description>
            <connector-id>alfresco</connector-id>
            <endpoint-url>https://localhost:8443/alfresco/s&lt;/
endpoint-url>
            <identity>user</identity>
         </endpoint>

         <endpoint>
            <id>alfresco-feed</id>
            <name>Alfresco Feed</name>
            <description>Alfresco Feed - supports basic HTTP
 authentication via the EndPointProxyServlet</description>
            <connector-id>http</connector-id>
            <endpoint-url>https://localhost:8443/alfresco/s&lt;/
endpoint-url>
            <basic-auth>true</basic-auth>
            <identity>user</identity>
         </endpoint>
      </remote>
   </config>
```

c. Change the <endpoint-url> values.

d. Save the `<web-extension>\share-config-custom.xml` file.

The SharePoint Support module will be able to handle requests using HTTPS on 7070 port only.

If you cannot login to Share, and you see message saying `The remote server may be unavailable or your authentication details have not been recognized.`, check the endpoints URLs and enable the `DEBUG` option in the Share `log4j.properties` for `org.springframework.extensions=DEBUG`. Ensure that there are no error messages saying `IO Error: during getObject() ... sun.security.validator.ValidatorException: PKIX path building failed`. If you see this message, this means that your certificate is not trusted. Check step 7a.

Upgrading

This section describes the recommended procedure for performing an upgrade.

Upgrading Alfresco

The procedure involves a new installation of the Alfresco binaries and configuration, and an in-place upgrade of a copy of the repository. In-place upgrade of the Alfresco binaries and configuration is not recommended.

Before starting an upgrade:

- Ensure that you have backed up your production environment
- If you have any customizations (for example, AMPs) in your existing Alfresco installation, recompile all Java code against the new version of Alfresco and regression test against the new version of Alfresco
- When you upgrade Alfresco with Oracle, the `alfresco` user needs more privileges than connect and resource. At minimum, the `alfresco` user should have permission to delete objects. A safer option is to give a `sysdba` role for the upgrade process only. After the upgrade, this role should be removed.

You must perform a test upgrade using a backup copy of the repository before attempting to upgrade your production environment. Therefore it is important that your backups are up-to-date.

1. Validate your platform is still on the supported stacks for the new version of Alfresco. See Supported stacks on page 25.
2. Shut down your existing Alfresco instance, including any virtualization servers and File System Receivers. Alfresco runtimes may be left running and upgraded at a later time using this same process.
3. Perform a cold back up of your repository. See Backing up and restoring the repository on page 200.
4. Back up any configuration overrides from the `<extension>` directory.

   Do not copy the files. Copy only the override settings so that you will not overwrite the new extension files in the upgraded version.
5. Download and install the new version of the Alfresco WAR in a different directory to the existing installation. See Installing Alfresco on page 18.
6. Validate the new installation to check that it is working correctly. See Validating an upgrade on page 98.
   a. Configure the new installation with a new repository (not the existing one).
   b. Start Alfresco and validate that the system works correctly.
   c. Shut down Alfresco and (optionally) clear the new repository.
7. Restore the backup into the new repository (not the existing one). See Restoring the backupThis task describes how to restore the Alfresco repository..
8. Manually apply your backed up configuration override settings into the relevant new override files in the `<extension>` directory. Ensure that you do not overwrite the new extension files. See Configuring an upgrade on page 97.
9. Reinstall all customizations into the new Alfresco instance.

10. Restart the Alfresco server for the configuration changes to take place. Monitor the startup log messages for information on the status of the upgrade. See Starting the Alfresco server on page 101.
11. Remove the old Alfresco installation and repository.

If you are satisfied that the upgrade is successful, remove the old Alfresco installation and repository. This may be done at a later time, once the new installation has been thoroughly validated.

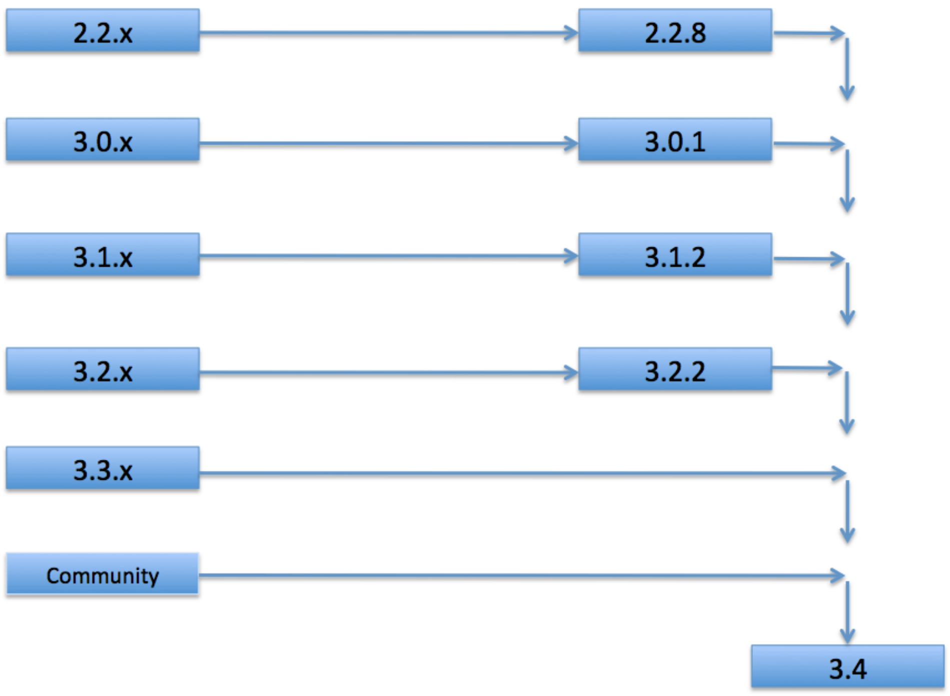
Alfresco upgrade paths

When you upgrade Alfresco, it is recommended that you follow a structured upgrade path between versions.

Alfresco supports upgrading up to two major versions above your existing version. In the table, 3.x, 2.2, 2.1, and 2.0 are all considered to be major version. This means that you can upgrade directly from 2.1 to 3.x; whereas 2.0 would require an intermediate step.

Major version upgrades

To upgrade to the latest version, first apply the latest service pack for your current version, then upgrade to the latest version (including service pack). The following diagram shows the upgrade paths for major versions:



For example, if your production environment currently runs Alfresco Version 2.2.2, you need to upgrade to Version 2.2.8 before you can upgrade to Version 3.4.

If you are upgrading from an earlier release that is not shown on this diagram, contact Support for assistance.

Minor version upgrades

From:	To:
2.1 SP7; 2.2 SP8; 3.1 SP2; 3.2 SP1; 3.3	3.3 SP1

From:	To:
2.1 SP7; 2.2 SP7; 3.1 SP2; 3.2 SP1; Community 3.3	3.3
2.1 SP7; 2.2 SP7; 3.1 SP2; 3.2R	3.2 SP1
2.1 SP7; 2.2 SP6; 3.1 SP2; 3.2; Community 3.2	3.2r
2.1 SP7; 2.2 SP5; 3.1 SP2; Community 3.2	3.2
2.1 SP7; 2.2 SP5; 3.1 SP1	3.1 SP2
2.1 SP7; 2.2 SP4; 3.1	3.1 SP1
2.1 SP7; 2.2 SP3; 3.0 SP1; Community	3.1
2.1 SP6; 2.2; 2.2 SP2; 3.0	3.0 SP1
2.1 SP5; 2.2; 2.2 SP1; Community	3.0
Previous service pack, and latest service pack available from previous release.	2.2 - 2.2 SP8
2.1 SP5; 2.1 SP6	2.1 SP7
Previous service pack. For Legacy upgrades, Alfresco recommend engaging consulting.	1.2 - 2.1 SP4

Configuring an upgrade

This section describes how to configure an upgraded installation of Alfresco.

Before running the server for the first time, check the database connection details and Alfresco data folder locations, and set them according to the environment in which the server is running.

By default, the server creates a data folder for storing content binaries and indexes at a location relative to the caller's location when the server starts. This is appropriate for quick previews and tests, but should be changed when running a server that will be storing long-lived data.

1. Locate the distribution's configuration files and samples.
2. Reapply any configuration changes to the new installation in the `<extension>` directory.
3. Open the `alfresco-global.properties` file.
4. Choose a root location for the storage of content binaries and index files.
5. Adjust the properties to change the database connection details.
6. Note the choice of JDBC driver used with each connection type.
7. Choose a Hibernate schema most appropriate to your database.
8. Save the file.
9. If you have any customizations (AMPs, patches, and so on) in your existing Alfresco installation, do the following:
   a. Recompile all Java code against the new version of Alfresco and regression test against the new version of Alfresco (this is best done prior to the upgrade itself, since it could be a lengthy exercise).
   b. Reinstall all customizations into the new Alfresco instance.
10. Start the server.

The configuration overrides will ensure that the server immediately directs data to the appropriate locations.

Upgrading configurations

This page describes the important information for upgrading from Alfresco Enterprise releases prior to version 3.2.

Alfresco includes the concept of subsystems. Overall defaults for subsystem properties are set in the `alfresco-global.properties` file.

When you upgrade from releases prior to Version 3.2, the recommendation is that you move all your repository and database configurations from the `<extension>custom-repository.properties` file to the `alfresco-global.properties` file.

For example, you should move the configuration settings for the following properties:

Sample custom content and index data location property:

- `dir.root=`

Sample database connection properties:

- `db.name=`
- `db.username=`
- `db.password=`
- `db.host=`
- `db.port=`

External locations for third-party products:

- `ooo.exe=soffice`
- `img.root=./ImageMagick`
- `swf.exe=./bin/pdf2swf`

Database connection properties:

- `db.driver=`
- `db.url=`
- `hibernate.dialect=`

Also, move any Hibernate settings from the `custom-hibernate-dialect.properties` file to the `alfresco-global.properties` file.

When you have moved your configurations, delete the `custom-repository.properties` file and the associated Spring context file `custom-repository-context.xml`, then restart the server for the settings to take effect.

If you continue to use the `custom-repository.properties` file to set your configurations, the settings may override those set in the `alfresco-global.properties` file requiring more complex ongoing administration and maintenance and possibly leading to unexpected results.

If you currently have configuration using any of these services, it is recommend that you move or reconfigure them using the new `alfresco-global.properties` configuration. This new method simplifies the setup and maintenance of these systems and it also simplifies future upgrades.

Validating an upgrade

Once you have upgraded, follow these steps to validate the new installation.

1. Restart the Alfresco server.

The configuration overrides ensure the server immediately directs data to the appropriate locations.

2. Monitor the startup log messages for information on the status of the upgrade.
3. Validate the new installation using a blank repository.
4. Configure the new installation with a new repository (not the existing one).
5. Verify the database connection details and Alfresco data folder locations are set according to the environment in which the server is running.
6. Start Alfresco and validate the system works correctly.
7. Shut down Alfresco.
8. When you are certain the new installation is thoroughly validated, remove the old Alfresco installation and repository.

WCM-specific upgrade

This section describes the specific instructions required for upgrading WCM.

To avoid problems with deployment from one version of Alfresco to another, you should plan your upgrade such that an Alfresco instance, and all of its dependent runtimes, are upgraded at the same time.

If you avoid deployment, these components do not all need to be taken offline, upgraded, and brought back online at exactly the same time. You can use a rolling upgrade process to avoid downtime on your site.

When upgrading, virtualization servers are considered to be an integral part of Alfresco and must be upgraded in lock-step with the main Alfresco instance(s).

Upgrading an Alfresco runtime

Any Alfresco runtimes in your environment must be upgraded using the same general upgrade process.

This process requires downtime, so to achieve an interruption-free upgrade, configure at least two Alfresco runtimes and upgrade each of them separately (so that at least one remains online at all times).

Upgrading a cluster

If you have configured an Alfresco cluster, you must perform this task when upgrading Alfresco.

1. Shut down all nodes in the cluster.
2. Perform the steps described in the upgrading general process on each node in turn, ensuring that each node starts fully before restarting the next one.

   You only have to copy the database once as it will be upgraded by the first node to be upgraded. The other nodes will detect it has been upgraded and skip the database upgrade step.

Upgrading multi-tenancy

If you have configured Alfresco multi-tenancy, you must perform this task when upgrading Alfresco

1. Perform the steps described in the upgrading general process.

2. Replace the three multi-tenancy extension files with the latest extension samples from the new Alfresco version.

   You will need to rename the files by removing `.sample` suffix.

Administering

This section provides guidance on configuring, maintaining, and administering an Alfresco production environment.

Starting and stopping

This section describes how to run the Alfresco server, Share, Explorer, virtualization server, and standalone deployment engine.

Starting the Alfresco server

The server must be running before you can use Alfresco Share or Alfresco Explorer. When you install Alfresco using the installation wizard, the server is automatically installed and started as a service.

- (Windows)
    - Browse to `C:\Alfresco`, and double-click `servicerun.bat`, or open the Control Panel **Services** window and start the following services:
        - `alfrescoMySQL`
        - `alfrescoOpenOffice`
        - `alfrescoTomcat`
    - If you installed Alfresco as a service, from the **Start** menu, select **All Programs > Alfresco Enterprise > Alfresco Enterprise Service > Start Alfresco Enterprise service.**
- (Linux) Browse to `/opt/alfresco/` and run `alfresco.sh start`.

  If you installed Alfresco using the installation wizard, the alfresco.sh script included in the installation disables the Security-Enhanced Linux (SELinux) feature across the system.

  The default shell for this script is `sh`. You can edit the `alfresco.sh` file to change to your preferred shell. For example, change the `#!/bin/sh` line to `#!/bin/bash`.

A command prompt opens with a message indicating the server has started.

```
INFO: Server startup in nnnn ms
```

Stopping the Alfresco server

- (Windows)
    - Open the Control Panel **Services** window and stop the following services:
        - `alfrescoMySQL`
        - `alfrescoOpenOffice`
        - `alfrescoTomcat`
    - Click the **Start** menu, and select **All Programs > Alfresco Enterprise > Alfresco Enterprise Service > Stop Alfresco Enterprise service**.

  The command prompt that opened during startup closes. Alfresco has now stopped.
- (Linux) Browse to `/opt/alfresco/`, and run `alfresco.sh stop`.

Starting Alfresco Share

Once you have installed Alfresco, you can start Alfresco Share using a browser.

1. Browse to the location of your Alfresco installation. If you installed Alfresco on your local machine, browse to `http://localhost:8080/share`.

   In Windows, alternatively, you can click the **Start** menu, and select **All Programs > Alfresco Enterprise > Alfresco Share**.

   Alfresco Share opens.
2. Log in using `admin` as the default user name and password.

Starting Alfresco Explorer

Once you have installed Alfresco, you can start Alfresco Explorer using a browser.

1. Browse to the location of your Alfresco installation. If you installed Alfresco on your local machine, browse to `http://localhost:8080/alfresco`.

   In Windows, alternatively, you can click the **Start** menu, and select **All Programs > Alfresco Enterprise > Alfresco Explorer**.

   Alfresco Explorer opens.
2. Log in using `admin` as the default user name and password.

Starting the Alfresco virtualization server

If you have installed Alfresco WCM, you can use the Website preview feature by starting the Alfresco virtualization server.

- (Windows)
  - Click the **Start** menu, and select **All Programs > Alfresco Enterprise > Alfresco Enterprise Virtual Server > Start Virtual Server**.
- (Linux) Browse to `/opt/alfresco/` and run `virtual_alf.sh start`.

  The default shell for this script is `sh`. You can edit the `virtual_alf.sh` file to change to your preferred shell. For example, change the `#!/bin/sh` line to `#!/bin/bash`.

Stopping the Alfresco virtualization server

- (Windows)
  - Click the **Start** menu, and select **All Programs > Alfresco Enterprise > Alfresco Enterprise Virtual Server > Stop Virtual Server**.
- (Linux) Browse to `/opt/alfresco/`, and run `sh virtual_alf.sh stop`.

Starting the standalone deployment engine

The standalone deployment engine is implemented as a set of Java libraries and is multi-platform.

Bourne shell scripts are provided for UNIX and Windows batch files are provided for Windows.

- (Windows) To start the standalone deployment engine:
  - Open a command prompt, and run the `deploy_start` script, or

    - Select **Start Menu > All Programs > Alfresco Standalone Deployment Receiver > Start Alfresco Standalone Deployment Receiver**.

  The Start menu action is available if you have used the deployment installer to install the Standalone Deployment Engine. This action is calling the `deploy_start.bat` script.

  It is also possible to install the standalone deployment engine as a Windows service, which can automatically start when Windows starts.

- (Linux) To start the standalone deployment engine, open a command prompt and run the `deploy_start.sh` script.

  The default shell for this script is `sh`. You can edit the `alfresco.sh` file to change to your preferred shell. For example, change the `#!/bin/sh` line to `#!/bin/bash`.

When deploying to a deployment engine running on a multi-NIC system, it may be necessary to bind the RMI registry to a particular IP address. To do this, add the following to the Java command in `deploy_start.sh` or `deploy_start.bat`:

```
-Djava.rmi.server.hostname=x.x.x.x
```

Where `x.x.x.x` is the IP address assigned to the NIC to which you want to bind.

Stopping the standalone deployment engine

The standalone deployment engine is implemented as a set of Java libraries and is multi-platform.

Bourne shell scripts are provided for UNIX and Windows batch files are provided for Windows.

- (Windows) To stop the standalone deployment engine:
    - Open a command prompt, and run `deploy_stop.bat`, or
    - Select **Start Menu > All Programs > Alfresco Standalone Deployment Receiver > Stop Alfresco Standalone Deployment Receiver**.
- (Linux) To stop the standalone deployment engine, open a command prompt, and run the `deploy_stop.sh` script.

Configuring Alfresco

This section provides information on the mechanisms for configuring Alfresco.

Configuration overview

Alfresco is preconfigured with a set of system configuration parameters. Many of the system configuration parameters are completely exposed as properties, which you can extend or override.

The system configuration parameters are found in the following files:

- `<configRoot>/alfresco/repository.properties`
- `<configRoot>/alfresco/hibernate-cfg.properties`
- `<configRoot>/alfresco/subsystems/<category>/<type>/*.properties`

There are two methods of extending the properties:

- Editing the global properties (`alfresco-global.properties`) file
- Using a JMX client, such as JConsole

The global properties file is used by Alfresco to detect the extended properties. For example, when you install Alfresco, many of the installation settings are saved in the global properties file. You can continue to use the global properties to do all your property extensions; however, whenever you make a change, you must restart the Alfresco server.

The JMX client allows you to edit the settings while the system is running. The settings you change are automatically persisted in the database and synchronized across a cluster. When you start up Alfresco, the system initially uses the `alfresco-global.properties` file to set the properties within the JMX client, but then any changes you make in the JMX client persist in the database but are not reflected back into the `alfresco-global.properties` file.

There are two types of property that you may need to edit:

Type 1: Properties specified directly in XML files

For example:

```
<bean id="wcm_deployment_receiver"
class="org.alfresco.repo.management.subsystems.ChildApplicationContextFactory"
        <parent="abstractPropertyBackedBean">
        <property name="autoStart">
                <value>true</value>
        </property>
</bean>
```

The value for the property `autoStart` is set to true directly in the `wcm-bootstrap-context.xml` file.

Type 2: Properties set by variables in XML files

For example:

```
<bean id="userInstallationURI" class="org.alfresco.util.OpenOfficeURI">
      <constructor-arg>
         <value>${ooo.user}</value>
      </constructor-arg>
   </bean>
```

The value for the property `constructor-arg` is replaced with a variable `${ooo.user}`.

When Alfresco starts up, type 1 properties are read from the XML file; type 2 properties get their values read from all the various property files. Then, the database is checked to see if there are any property values set there, and if any property has been changed, this value is used instead.

Some of the type 2 properties can be viewed and changed by the JMX console, some cannot. For example. `ooo.exe` can be viewed and changed using the JMX client; `index.recovery.mode` cannot be viewed or changed using the JMX client.

In a new Alfresco installation, none of these properties are stored in the database. If you set a property using the JMX interface, Alfresco stores the value of the property in the database. If you never use JMX to set the value of a property, you can continue using the `alfresco-global.properties` file to set the value of the property. Once you change the property setting using JMX, and it is therefore stored in the DB, you cannot use the properties files to change the value of that property.

For advanced configuration, you can also extend or override the Spring bean definitions that control Alfresco's Java classes. To do so, add or copy a Spring bean file named `*-context.xml` to the `<extension>` directory, or `<web-extension>` directory to extend Share. For examples of the Spring bean extensions, download the sample extension files.

Runtime administration with a JMX client

By default, you can reconfigure Alfresco by shutting down the server, editing the relevant property in the configuration files, and then restarting the server. There are some support operations that can be performed on-demand at runtime without needing to restart the server.

The Java Management Extension (JMX) interface allows you to access Alfresco through a standard JMX console that supports JMX Remoting (JSR-160). This lets you:

- Manage Alfresco subsystems
- Change log levels
- Enable or disable file servers (FTP/CIFS/NFS)
- Set server read-only mode
- Set server single-user mode
- Set server maximum user limit - including ability to prevent further logins
- Count user sessions/tickets
- User session/ticket invalidation

Example consoles include:

- JConsole (supplied with Java SE 5.0 and higher)
- MC4J
- JManage

Some of these consoles also provide basic graphs and/or alerts for monitoring JMX-managed attributes.

Connecting to Alfresco through JMX client

You can connect to Alfresco through a JMX client that supports JSR-160.

1. Open a JMX cilent that supports JMX Remoting (JSR-160).
2. Enter the JMX URL:

   `service:jmx:rmi:///jndi/rmi://<hostname>:50500/alfresco/jmxrmi`

   Where `<hostname>` is the name of your host or IP address.
3. Enter the default JMX user name: `controlRole`
4. Enter the default JMX password: `change_asap`

   You must change the default JMX password as soon as possible.
5. Change the JMX password in the following files:
   - `<configRoot>/alfresco/alfresco-jmxrmi.access`
   - `<configRoot>/alfresco/alfresco-jmxrmi.password`

Disabling JMX

The JMX functionality is enabled using the `RMIRegistryFactoryBean` in the `core-services-context.xml` file.

1. Open the `<configRoot>\classes\alfresco\core-service-context.xml` file.
2. Comment out the `RMIRegistryFactoryBean` section.
3. Save the file.

Configuring Alfresco with JConsole

This section describes how to use the JMX client, JConsole for Alfresco runtime administration. JConsole is a JMX client available from Sun Microsystems Java SE Development Kit (JDK).

The initial configuration that displays in JConsole is set from the `alfresco-global.properties` file.

1. Open a command console.
2. Locate your JDK installation directory.

   For example, the JDK directory may be `java/bin`.
3. Enter the following command:

   ```
   jconsole
   ```

   The **JConsole New Connection** window displays.
4. Double-click on the Alfresco Java process.

   For Tomcat, this the Java process is usually labelled as **org.apache.catalina.startup.Bootstrap start**.

   JConsole connects to the managed bean (or MBean) server hosting the Alfresco subsystems.
5. Select the **MBeans** tab.

   The available managed beans display in JConsole.
6. Navigate to **Alfresco > Configuration**.

   The available Alfresco subsystems display in an expandable tree structure. When you select a subsystem, the **Attributes** and **Operations** display below it in the tree.
7. Select **Attributes** and set the required Alfresco subsystem attribute values.

   Values that can be edited are shown with blue text.

   When you change a configuration setting, the subsystem automatically stops.
8. Restart the Alfresco subsystem:
   a. Navigate to the subsystem.
   b. Select **Operations**.
   c. Click **Start**.
9. To stop the Alfresco subsystem without editing any properties:
   a. Navigate to the subsystem.
   b. Select **Operations**.
   c. Click **Stop**.
10. To revert back to all the previous edits of the Alfresco subsystem and restores the default settings:
    a. Navigate to the subsystem.
    b. Select **Operations**.
    c. Click **Revert**.
11. Click **Connection > Close**.

The settings that you change in a JMX client, like JConsole, are persisted in the Alfresco database. When you make a dynamic edit to a subsystem:

1. When a subsystem, that is currently running, is stopped, its resources are released and it stops actively listening for events. This action is like a sub-part of the server being brought down. This ‘stop’ event is broadcast across the cluster so that the subsystem is brought down simultaneously in all nodes.
2. The new value for the property is persisted to the Alfresco database.

There are two ways to trigger a subsystem to start:

- The start operation
- An event that requires the subsystem

Global properties file

The global properties `alfresco-global.properties` file contains the customizations for extending Alfresco.

If you install Alfresco using one of the installation wizards, the `alfresco-global.properties` file is modified with the settings that you chose during installation. If you install Alfresco using the WAR file, you must modify properties in the sample `alfresco-global.properties` file manually.

A sample global properties file is supplied with the Alfresco installation. By default, the file contains sample settings for running Alfresco, for example, the location of the content and index data, the database connection properties, the location of third-party software, and database driver, and Hibernate properties.

Modifying the global properties file

This section describes the steps for modifying the `alfresco-global.properties` file.

For edits to the `alfresco-global.properties` file, when specifying paths for Windows systems, you must replace the Windows path separator characters with either the `\\` separator or the forward slash `/` Unix path separator. Also, when using folder names like `User Homes`, you must manually escape the space. For example, change the value to `User_x0020_Homes`.

1. Browse to the `<classpathRoot>` directory.

   For example, for Tomcat 6, browse to the `$TOMCAT_HOME/shared/classes/` directory.
2. Open the `alfresco-global.properties.sample` file.

   This file contains sample configuration settings for Alfresco. To enable or modify a setting, ensure that you remove the comment (#) character.
3. Add a root location for the storage of content binaries and index files in the `dir.root=` property.

   For example, `dir.root=C:/Alfresco/alf_data`.
4. Set the database connection properties.

Property	Description
`db.username=alfresco`	Specifies the name of the main Alfresco database user. This name is used to authenticate with the database.
`db.passowrd=alfresco`	Specifies the password for the Alfresco database user. This password is used to authenticate with the database.

   Additional database properties may be set for further configuration. Refer to the Configuring databases on page 114 for more information.
5. Specify the locations of the following external software:

Property	Desctiption
`ooo.exe=`	Specifies the location of the OpenOffice installation.
`ooo.enabled=`	Specifies the whether to use the Direct OpenOffice subsystem.

Property	Desctiption
`jodconverter.officeHome=`	Specifies the location of the OpenOffice installation for JODConverter transformations. To use the JODConverter, uncomment the `ooo.enabled=false` and `jodconverter.enabled=true` properties.
`jodconverter.portNumbers=`	Specifies the port numbers used by each JODConverter processing thread. The number of process will match the number of ports.
`jodconverter.enabled=`	Specifies whether to use the JODConverter. Set the property to `jodconverter.enabled=true`.
`img.root=`	Specifies the location of the ImageMagick installation.
`swf.exe=`	Specifies the location of the SWF tools installation.

6. Uncomment the `db.driver=` and `db.url=` properties for the database that you require.

   These properties are grouped into sections for MySQL, Oracle, SQL Server, and PostgreSQL connection, each containing sample settings.
7. Select a JDBC driver used with each connection type.
8. (Optional) Set the Hibernate dialect for your database.

   If you do not specify a dialect, Hibernate will attempt to detect the dialect of your database automatically from the JDBC connection.
9. Add your global custom configurations.
10. Save your file without the `.sample` extension.

You need to restart the Alfresco server for the configuration changes to take effect.

Setting composite properties in the global properties file

This section uses the the `imap.server.mountPoints` property as an example.

The `ImapConfigMountPointsBean` class that holds the component beans has four properties of its own:

- `beanName`
- `store`
- `rootPath`
- `mode`

1. Open the `<classpathRoot>/alfresco-global.properties` file.
2. To set some overall defaults for all component instances, use the format:

   ```
   <property>.default.<component property>
   ```

   These values would show up, for example, when you added a new component instance but did not specify its properties.

   For example:

   ```
   imap.server.mountPoints.default.store=${spaces.store}
   imap.server.mountPoints.default.rootPath=/
   ${spaces.company_home.childname}
   imap.server.mountPoints.default.mode=virtual
   ```

This example does not define a default for `beanName` because there is a way of populating it for each instance.

3. To set up the `imap.server.mountPoints` with a composite value, set the master composite property using a comma-separated list.

   For example:

   ```
   imap.server.mountPoints=Repository_virtual,Repository_archive
   ```

   This defines that the property contains two `ImapConfigMountPointsBean` instances, named `Repository_virtual` and `Repository_archive`. Because `ImapConfigMountPointsBean` implements the `BeanNameAware` Spring interface and has a `beanName` property, these instance names are automatically set as the bean names.

4. To define component properties specific to each component instance, use the format:

   ```
   <property>.value.<component instance name>.<component property>
   ```

   For example:

   ```
   imap.server.mountPoints.value.Repository_virtual.mode=virtual
   imap.server.mountPoints.value.Repository_archive.mode=archive
   ```

Java command line

All the Alfresco properties can be set using the standard `alfresco-global.properties` configuration file. There may be circumstances where it is more convenient to change properties on the fly. The Java command line provides an alternative method of setting the properties.

The most common use of the Java command line is in a multiple-machine environment where the basic, common customizations are set using standard properties and the machine-specific values are set using command line options. For example, an administrator is likely to configure all Alfresco installs to behave similarly by setting properties in the configuration files, but will use the Java command line to vary settings like the database connection, Content Store locations, and CIFS domain name.

You can set any property that is specified in the `alfresco-global.properties` file, including CIFS, JGroups, and Hibernate.

Setting properties on the Java command line

This section describes how to use the `-D` options for setting properties on the Java command line.

- Add a `-Dprop=value` to `JAVA_OPTS` or for anything that is sent to the Java command line.

  For example, `-Ddir.root=/alfresco/data -Ddb.url=xxxx`.

Modifying Spring bean definition files

For advanced configuration, you can also extend or override the Spring bean definitions that control the Alfresco Java classes.

The Spring bean definitions are within configuration files in the following directories:

- The `<extension>` directory contains the configuration files for extending Alfresco.
- The `<web-extension>` directory contains the configuration files for extending Alfresco Share.

1. Browse to the `<extension>` directory. For example, for Tomcat 6:

   - (Windows) `C:\Alfresco\tomcat\shared\classes\alfresco\extension`
   - (Linux) `tomcat/shared/classes/alfresco/extension`

   Each file has a copy with a `.sample` extension.

2. Open the configuration file with the `.sample` extension.
3. Add your configurations to the file.
4. Save the file without the `.sample` extension.

Modifying system configuration files

This section describes the recommended method for modifications to the system configuration files.

Before you start, back up all your configuration files for security. The system configuration files that are read by Alfresco are contained in the `<configRoot>` and `<configRootShare>` directories.

The preferred method of configuration is to extend the system files using the global properties file (`alfresco-global.properties`). If you choose to modify the system files directly, there is a risk that you will lose your changes when you next upgrade. To minimize the risk, use the following approach.

1. Make a copy of the default file you want to modify, and rename it.
2. Make your customization. Make only one logical change at one time (one logical change may mean several physical changes).
3. Check any XML is well-formed. You can use any XML editor or you can open the file in a browser, such as Firefox.
4. Before making further changes, test each logical change by stopping and restarting Alfresco.
5. If you need to roll back the changes for troubleshooting, roll them back in the reverse sequence to which you applied them. Stop and restart Alfresco after each rollback.

Repository system configuration files

The Alfresco system configuration files are in the application WAR file. When the server starts, the files expand to `<configRoot>`.

The path for `<configRoot>` is different depending on your application server. For example:

- Tomcat: `<TOMCAT_HOME>\webapps\alfresco\WEB-INF`
- JBoss: `<JBOSS_HOME>\server\default\tmp\deploy\tmp*alfresco-exp.war\WEB-INF`

The system configuration files are maintained by Alfresco and contained in `<configRoot>` and `<configRoot>\classes\alfresco`. The preferred method of configuring Alfresco is to extend the default files using the global properties file (`alfresco-global.properties`).

The following four files represent the core of the application configuration:

1. `<configRoot>\classes\alfresco\application-context.xml`

   This file is the starting point of the Spring configurations. This file only performs imports, including a wildcard import of all `classpath*:alfresco/extension/*-context.xml` files.
2. `<configRoot>\classes\alfresco\core-services-context.xml`

   Core Alfresco beans are defined here, including the importing of properties using the `repository-properties` bean.
3. `<configRoot>\classes\alfresco\repository.properties`

   This file is imported by the `repository-properties` bean. The file defines some of the core system properties, including:

   - `dir.root`

This folder is where the binary content and Lucene indexes are stored. The `alf_data` folder is where they are stored by default, but you should change this to your own location. It is relative by default, but must point to a permanent, backed-up location for data storage.

- `dir.auditcontentstore`

  This folder is where the audit's content store is stored.

- `dir.indexes`

  This folder contains all Lucene indexes and deltas against those indexes.

  Alfresco recommends that you do not store Lucene indexes on an NFS volume. The indexes must be on a local disk. For best performance, use a separate hardware chain (for example, controller, disk, and so on) to avoid I/O contention with other operations, like storing content and other applications.

- `db.*`

  These are the default database connection properties.

- `db.schema.update`

  This property controls whether the system bootstrap should create or upgrade the database schema automatically.

- `hibernate.hbm2ddl.auto`

  This determines whether Hibernate updates the database schema or just validates it.

  - `update`: checks and updates the database schema as appropriate
  - `validate`: checks the database schema and fails if it is not compliant

4. `<configRoot>\classes\alfresco\domain\hibernate-cfg.properties`

   This file defines Hibernate default system properties. The file is imported by the `hibernateConfigProperties` bean, which is in `hibernate-context.xml`. The important Hibernate property is:

   - `hibernate.dialect`

     This alters the SQL dialect that Hibernate uses when issuing queries and updates to the database. Normally, this is the only Hibernate property that will need changing, depending on the database you are running against.

Customizing individual configuration items

This section provides information about the types of configuration files available in Alfresco, and how to configure them.

The Alfresco configuration is implemented using three types of files:

- Properties files
- Configuration files
- Bean files

Customizing properties files

Properties files contain properties and end with the extension `.properties`. Each property is defined on one line. A `.properties` file has no header, so you do not need to take any action to preserve the header.

1. Open the file you want to customize.

For example, open the `alfresco-global.properties` file.

2. Comment out all the properties you do not want to modify by adding the “#” character.

   For example, to override the `db.driver` property, you only require one line:

   ```
   db.driver=oracle.jdbc.OracleDriver
   ```
3. Uncomment all the properties that you want to activate by removing the “#” character.
4. Save the file.

Customizing configuration files

Configuration files end with the extension `.xml`, and define `<config>` tags. A typical configuration file is `<extension>/web-client-config-custom.xml`.

A configuration file contains `<alfresco-config>` tags outside the `<config>` tags. You must preserve these tags in your customized file.

1. Open the configuration file that you want to customize.
2. Delete each pair of `<config> </config>` tags that you do not want to modify.
3. To delete part of an item:
   a. Copy the original `<config>` statement.
   b. Delete the children you do not want.
   c. Use the replace=“true” attribute.
4. To add another item, you only need a single item. The other items will remain enabled.
5. Customize the contents of the remaining `<config>` tags.
6. Save your customized file.

Configuration files

The configuration files contain configurations that either augment or replace the standard configuration. The system configuration files are located in `<configRoot>\classes\alfresco\web-client-config-*`

Replacing a configuration

To replace the configuration, add a `replace=“true”` attribute to the configuration element. For example: `<config evaluator="xx" condition=“yy” replace=“true”>`

Any configuration within a section marked this way completely replaces any configuration found in the Alfresco-maintained files.

For example, to replace the list of languages shown in the login page, add the following:

```
<config evaluator="string-compare" condition="Languages" replace="true">
 <languages>
    <language locale="fr_FR">French</language>
    <language locale="de_DE">German</language>
 </languages>
</config>
```

Modifying one property

The attribute `replace` completely replaces the configuration. To modify one property, you can add the changed piece.

For example, to add another language, you need a single `<language>` item. The other `<language>` items remain enabled. For example, if you want Spanish in addition to English and German:

```
<config evaluator="string-compare" condition="Languages">
 <languages>
```

```
   <language locale="es_ES">Spanish</language>
   ..
  </languages>
</config>
```

For example configurations, see Configuring Explorer.There are several different ways that you can customize the Explorer configuration items. The Explorer configuration file is called `web-client-config-custom.xml`.

Customizing bean files

Bean files end with the extension `.xml` and contain `<bean>` tags. You can modify `<bean>` tags to define properties or point to customized files.

There are two common uses of beans:

- To define properties
- To point to one or more of your customized files

A typical bean file is `<extension>/custom-repository-context.xml`. A bean file contains `<?xml>` and `<!DOCTYPE>` headers, and `<beans>` tags outside the `<bean>` tags. You must preserve these items in your customized file.

When you override a `<bean>`, the entire effects of the original bean are lost. The effect is the same as if you had overridden a `<config>` by using `replace="true"`. Therefore, the overriding `<bean>` must contain any information from the default bean that you want to keep, as well as any additional information.

For example, if a core bean has four values, and you want to modify a single value, the resultant bean must still have four values. However, if you want to add a value, then the resultant bean must have five values - the original four values plus the added value.

1. Open the bean file that you want to customize.

   For example, the following `<bean>` is from the `<configRoot>/classes/alfresco/action-services-context.xml` file:

   ```
   <bean id="mail"
    class="org.alfresco.repo.action.executer.MailActionExecuter"
    parent="action-executer">
      <property name="publicAction">
         <value>true</value> <!-- setting to true -->
      </property>
      <property name="mailService">
         <ref bean="mailService"></ref>
      </property>
   </bean>
   ```
2. Delete each pair of `<bean> </bean>` tags that you do not want to modify.
3. Modify the contents of the remaining `<bean>` tags.

   For example, the following overrides the `publicAction` property from the previous example:

   ```
   <bean id="mail"
    class="org.alfresco.repo.action.executer.MailActionExecuter"
    parent="action-executer">
      <property name="publicAction">
         <value>false</value> <!-- setting to false -->
      </property>
      <property name="mailService">
         <ref bean="mailService"></ref>
      </property>
   </bean>
   ```
4. Save the file.

Configuring databases

This section describes how to configure supported databases for use with Alfresco.

Configuring a PostgreSQL database

This section describes how to configure a PostgreSQL database for use with Alfresco.

1. Copy the appropriate PostgreSQL driver JAR to:
   - (Tomcat) `$TOMCAT_HOME/lib`
   - (JBoss) `/jboss/server/default/lib`
2. Create a database named `alfresco`.
3. Create a user named `alfresco`.
4. Set the new user's password to `alfresco`.
5. Ensure the Alfresco user has the required privileges to create and modify tables.
6. Open the `<classpathRoot>/alfresco-global.properties.sample` file.
7. Locate the following line:

   `dir.root=./alf_data`
8. Edit the line with an absolute path to point to the directory in which you want to store Alfresco data. For example: `dir.root=C:/Alfresco/alf_data`
9. Uncomment the following properties:

   ```
   # PostgreSQL connection (requires postgresql-8.2-504.jdbc3.jar or
    equivalent)
   #
   #db.driver=org.postgresql.Driver
   #db.url=jdbc:postgresql://localhost:5432/alfresco
   ```
10. Ensure that the other database connection properties are commented out.
11. Save the file without the `.sample` extension.
12. To allow password-authenticated connections through TCP/IP, ensure the PostgreSQL configuration file contains the following:

    ```
    host all all 127.0.0.1/32 password
    ```

    For PostgreSQL version 8.1.3, the file name is `pg_hba.conf`. For every other version, the file name is `postgresql.conf`.
13. Change the ownership of the directory tree specified in the `custom-data-location.properties` file to be owned by the user running the alfresco server.

    The tree must be owned by the user running the Alfresco server.
14. Restart the Alfresco server.

Configuring an Oracle database

This section describes how to configure an Oracle RDBMS database for use with Alfresco.

The Oracle database is case sensitive, so any configuration setting that you add into the `alfresco-global.properties` file must match the case used in Oracle.

1. Create a new `alfresco` user and schema in Oracle.

   The `alfresco` user must have Connect and Resource privileges in Oracle.
2. Ensure the `alfresco` user has the required privileges to create and modify tables.

You can remove these privileges once the server has started, but they may also be required for upgrades.

3. Open the `<ClassPathRoot>\alfresco-global.properties.sample` file.
4. Locate the following line:

   `dir.root=./alf_data`
5. Edit the line with an absolute path to point to the directory in which you want to store Alfresco data. For example: `dir.root=C:/Alfresco/alf_data`
6. Override the repository properties by removing the comments on each of the following lines:

```
#db.driver=oracle.jdbc.OracleDriver
#db.url=jdbc:oracle:thin:@localhost:1521:alfresco
```
7. Set the `host` and `port` number to the location of your Oracle JDBC driver.
8. (Optional) If you have multiple Alfresco instances installed on your Oracle server, add the following:

   `hibernate.default_schema=ALFRESCO`

   This forces the database metadata queries to target the schema that each database user is using.
9. Ensure that the other database connection settings are commented out.
10. Save the file without the `.sample` extension.
11. Copy the Oracle `JDBC driver JAR` into `/lib`.
12. Start the Alfresco server.

    If you receive JDBC errors, ensure the location of the Oracle JDBC drivers are on the system path, or add them to the relevant `lib` directory of the application server. The Oracle JDBC drivers are located in the `<orainst>/ora<ver>/jdbc/lib` directory (for example, `c:\oracle\ora92\jdbc\lib`).

    The JDBC driver for Oracle is in the JAR file: `ojdbc14.jar`.

Configuring a SQL Server database

This section describes how to configure a Microsoft SQL Server database for use with Alfresco. To modify the default database configuration, you must edit values in the `<ClasspathRoot>\alfresco-global.properties` file.

1. Create a new `alfresco` database and and user in SQL Server.

   Create the database with a UTF8 character set and the default collation settings.
2. Ensure the `alfresco` user has the required privileges to create and modify tables.

   This can be removed once the server has started, but may be required during upgrades.
3. Enable snapshot isolation mode with the following command:

   `ALTER DATABASE alfresco SET ALLOW_SNAPSHOT_ISOLATION ON;`
4. Ensure that the TCP connectivity is enabled on the fixed port number 1433.
5. Copy the jTDS JDBC driver to `$TOMCAT_HOME\lib`.

   This release requires the jTDS driver Version 1.2.5 for compatibility with the SQL Server database.
6. Edit the `alfresco-global.properties.sample` file.
7. Edit the `dir.root=` property with an absolute path to point to the directory in which you want to store Alfresco data.

For example: `dir.root=C:/Alfresco/alf_data`.

8. Set the database connection properties.

   For example:

   ```
   db.name=alfresco
   db.username=alfresco
   db.password=alfresco
   db.host=localhost
   db.port=1433
   db.driver=net.sourceforge.jtds.jdbc.Driver
   db.url=jdbc:jtds:sqlserver://{db.host}:${db.port}/${dbname}
   db.txn.isolation=4096
   ```
9. Ensure that the other database connection settings are commented out.
10. Save the file without the `.sample` extension.
11. Start the Alfresco server.

Configuring the MySQL database

This section describes how to configure a MySQL database for use with Alfresco.

1. Install the MySQL database connector.

   The MySQL database connector is required when installing Alfresco with MySQL. The database connector allows MySQL database to talk to the Alfresco server.

   a. Browse to the MySQL download site: http://dev.mysql.com/
   b. Download **MySQL Connector/J x.x**, and extract the following file from the downloaded `.zip` or `.tar.gz` file:

      `mysql-connector-java-5.x.x-bin.jar`
   c. Copy the JAR file into the `<TOMCAT_HOME>/lib` directory for Tomcat 6.
2. Create a database named `alfresco`.
3. Create a user named `alfresco`.
4. Set the new user's password to `alfresco`.
5. Open the `<classpathRoot>/alfresco-global.properties.sample` file.
6. Locate the following line:

   `dir.root=./alf_data`
7. Edit the line with an absolute path to point to the directory in which you want to store Alfresco data. For example: `dir.root=C:/Alfresco/alf_data`
8. Locate the MySQL connection section, and then uncomment the following lines:

   ```
   #db.driver=org.gjt.mm.mysql.Driver
   #db.url=jdbc:mysql://localhost/alfresco?
   useUnicode=yes&characterEncoding=UTF-8
   ```
9. Set the host, port, and name to the location of your MySQL JDBC driver.

   ```
   db.url=jdbc:mysql://your-host:3306/alfresco?
   useUnicode=yes&characterEncoding=UTF-8
   ```

   If you are using MySQL and require the use of non-US-ASCII characters, you need to set the encoding for internationalization. This allows you to store content with accents in the repository. The database must be created with the UTF-8 character set and the utf8_bin collation. Although MySQL is a unicode database, and Unicode strings in Java, the JDBC driver may corrupt your non-English data. Ensure that you keep the `?useUnicode=yes&characterEncoding=UTF-8` parameters at the end of the JDBC URL.
10. (Optional) Enable case sensitivity.

The default, and ideal, database setting for Alfresco is to be case-insensitive. For example, the user name properties in the `<configRoot>\classes\alfresco\repository.properties` file are:

```
# Are user names case sensitive?
user.name.caseSensitive=false
domain.name.caseSensitive=false
domain.separator=
```

If your preference is to set the database to be case-sensitive, add the following line to the `alfresco-global.properties` file:

```
user.name.caseSensitive=true
```

You also must ensure that the MySQL database is set to use UTF-8 and InnoDB. Refer to Configuration settings for using MySQL with Alfresco on page 27

11. Save the file.

Configuring a DB2 database

This section describes how to configure a DB2 database for use with Alfresco.

These steps assume that you are using DB2 v9.7 or later.

1. The following registry variables need to be set.
   - `db2set DB2_EVALUNCOMMITTED=ON`
   - `db2Set DB2_SKIPDELETED=ON`
   - `db2set DB2_SKIPINSERTED=ON`

   The default access to DB2 from Alfresco uses the cursor stability isolation level, which produces concurrency issues arising from read locks. The registry settings provide a workaround for this issue; however, they do not resolve all issues.
2. Create a database named `alfresco`.

   Create the database with a larger page size of 32K. Ensure that the database is created with the UTF-8 character set.

   If you do not create the database with these settings, you will see error SQL0286N (`sqlCode -286, sqlstate 42727`) because the schema is created for tables that do not fit the page size.
3. Set up the `alfresco` user and associated schema.

   DB2 only integrates with the operating system security. You can not add a database user with a password as you can say in oracle.
4. Open the `alfresco-global.properties.sample` file.
5. Add the following properties.

   ```
   db.name=alfresco
   db.username=alfresco
   db.password=alfresco
   db.host=localhost
   db.port=50000
   db.driver=com.ibm.db2.jcc.DB2Driver
   db.url=jdbc:db2://{db.host}:${db.port}/${db.name}
   ```
6. Save the file without the `.sample` extension.

Configuring Alfresco subsystems

An Alfresco subsystem is a configurable module responsible for a sub-part of Alfresco functionality. Typically, a subsystem wraps an optional functional area, such as IMAP bindings, or one with several alternative implementations, such as authentication.

A subsystem can be thought of as miniature Alfresco server embedded within the main server. A subsystem can be started, stopped, and configured independently, and it has its own isolated Spring application context and configuration.

The application context is a child of the main context, therefore, it can reference all the beans in the main application context. However, the subsystem's beans cannot be seen by the main application context and communication with the subsystem must be through explicitly imported interfaces. The main features of subsystems are:

Multiple ‘instances’ of the same type
The same template spring configuration can be initialized with different parameters in different instances. This enables, for example, the chaining of multiple authentication subsystems through property file edits.

Dynamic existence
JMX-based server configuration capabilities in Alfresco Enterprise releases.

Own bean namespace
There is no problem of bean name uniqueness if you need multiple instances of the same subsystem. Again, this vastly simplifies the problem of building an authentication chain as there is no need to edit any template Spring configuration.

Clearly defined interfaces with the rest of the system
A subsystem's interfaces must be 'imported' in order to be used anywhere else in the system. This is done by mounting them as dynamic proxies.

Hidden implementation specifics
Implementation specifics are not visible because all of its beans are hidden in a private container.

Swapping of alternative implementations
To switch over from native Alfresco authentication to NTLM passthru authentication, you switch to a passthru authentication subsystem and the correct components are swapped in.

Separate product from configuration
A subsystem binds its configuration settings to properties and can even do this for composite data. There is no longer a need to edit or extend prepackaged Spring configuration in order to configure a subsystem for your own needs.

Subsystem categories

Every subsystem has a category and a type.

- Category is a broad description of the subsystem's function, for example, Authentication.
- Type is a name for the particular flavor of implementation, where multiple alternative implementations exist, for example, `ldap`. Where a subsystem has only one implementation, you can use the default type name of `default`.

The Alfresco-supplied subsystem categories are:

Audit
Handles the audit related functions.

Authentication
Handles all authentication related functions, including:

- Password-based authentication
- Single Sign-on (SSO) for WebClient, WebDAV, Web Scripts, and SharePoint Protocol
- CIFS and FTP authentication
- User registry export (LDAP only)

The subsystem is chained so that multiple instances of different types can be configured and used together.

OOoDirect
Handles the settings for OpenOffice transformations. With this subsystem, the Alfresco server directly manages OpenOffice.

OOoJodconverter
Handles the JODConverter settings for OpenOffice transformations. With this subsystem, the JODConverter manages OpenOffice, including a pool of separate OpenOffice processes, automatic restart of crashed OpenOffice processes, automatic termination of slow OpenOffice operations, automatic restart of any OpenOffice process after a number of operations.

Synchronization
Performs regular synchronization of local user and group information with the user registry exporters (usually LDAP directories) in the authentication chain.

fileServers
Handles the properties for the CIFS, FTP, and NFS servers.

email
Handles the outbound and inbound SMTP property settings.

imap
Handles the properties for the IMAP service.

sysAdmin
Handles the properties for server administration.

thirdparty
Handles the properties for SWF Tools and ImageMagick content transformers.

wcm_deployment_receiver
Handles the properties for WCM Deployment Receiver.

Subsystem configuration files

The prepackaged subsystem configuration files form part of the core product and should not be edited.

The prepackaged subsystems are found in the `<configRoot>/classes/alfresco/subsystems` directory.

Each subsystem directory should contain one or more Spring XML bean definition metadata files, with names matching the `*-context.xml` pattern. These files are loaded by the child application context that belongs to the subsystem instance.

The XML bean definitions may contain place holders for properties that correspond to configuration parameters of the subsystem. As per standard Spring conventions, these place holders begin with `${` and end with `}`. In the following example, the value of the `ooo.user` configuration parameter will be substituted into the bean definition when it is loaded:

```
<bean id="userInstallationURI" class="org.alfresco.util.OpenOfficeURI">
      <constructor-arg>
         <value>${ooo.user}</value>
```

```
        </constructor-arg>
    </bean>
```

There is no need to declare a `PropertyPlaceholderConfigurer` bean. An appropriate one is added into the application context automatically.

Subsystem properties

A subsystem declares default values for all the properties it requires in one or more `.properties` files in its subsystem directory.

For example, there could be a `mysubsystem.properties` file, containing the following:

```
ooo.user=${dir.root}/oouser
```

Place holders are used for system-wide properties, such as `dir.root` in the `-context.xml` and `.properties` files, as the child application context will recursively expand place holders for its own properties and all the place holders recognized by its parent.

Properties files in the subsystem directory declare the configuration parameters and provide default values where these have not been supplied elsewhere. These files should not be edited in order to configure the subsystem.

Use the following methods to modify the subsystem properties:

- Subsystems and all their composite properties show under the `Alfresco:Type=Configuration` tree in JConsole.
- See Modifying the global properties file on page 107 for more information on how to configure a prepackaged subsystem.
- `-D` options

Mounting a subsystem

A subsystem can be mounted, that is, its existence can be declared to the main server. To mount a susbsystem, use the `ChildApplicationContextFactory` bean. This is an object that wraps the Spring application context that owns the subsystem and its beans. It initializes its application context as a child of the main Alfresco context with an appropriate `PropertyPlaceholderConfigurer` that will expand its configuration parameters.

Any instances that you define should extend the `abstractPropertyBackedBean` definition. The identifier that you define for the bean automatically becomes the subsystem category and defines where the factory will look for configuration files, in the search paths.

1. Open the core `bootstrap-context.xml file` (the file that controls the startup of beans and their order).
2. Locate the following bean definition:

   ```
   <!--  Third party transformer Subsystem -->
    <bean id="thirdparty"
    class="org.alfresco.repo.management.subsystems.ChildApplicationContextFactory"

    parent="abstractPropertyBackedBean">
        <property name="autoStart">
            <value>true</value>
        </property>
    </bean>
   ```

   The `autoStart` property is set to true, meaning that the child application context will be refreshed when the server boots up, activating the beans it contains. For subsystems containing background processes or daemons (for example, the file server subsystem), it is very important to set this property, otherwise the subsystem will never activate.
3. Save your file.

Mounting a subsystem with composite properties

A subsystem is limited to flat property sets for its configuration, therefore it is difficult to allow structured data in this configuration. A composite property is a special property whose value is a list of beans.

- For example, the IMAP subsystem is mounted as:

  ```
  <!-- IMAP Subsystem -->
   <bean id="imap"
   class="org.alfresco.repo.management.subsystems.ChildApplicationContextFactory"

   parent="abstractPropertyBackedBean">
       <property name="autoStart">
           <value>true</value>
       </property>
       <property name="compositePropertyTypes">
           <map>
               <entry key="imap.server.mountPoints">

   <value>org.alfresco.repo.imap.config.ImapConfigMountPointsBean</value>
               </entry>
           </map>
       </property>
   </bean>
  ```

  The subsystem declares a single composite property called `imap.server.mountPoints` with component type `org.alfresco.repo.imap.config.ImapConfigMountPointsBean`.

- The configured value of this composite property is materialized in the child application context as a `ListFactoryBean`. The bean's ID should match the name of the composite property. So, for example, in the IMAP subsystem configuration:

  ```
   <!--The configurable list of mount points - actually a post-processed
   composite property! -->
      <bean id="imap.server.mountPoints"
   class="org.springframework.beans.factory.config.ListFactoryBean">
          <property name="sourceList">
              <list>
                  <!-- Anything declared in here will actually be ignored
   and replaced by the configured composite propery value, resolved on
   initialization -->
                  <bean id="Repository_virtual"
   class="org.alfresco.repo.imap.config.ImapConfigMountPointsBean">
                      <property name="mode">
                          <value>virtual</value>
                      </property>
                      <property name="store">
                          <value>${spaces.store}</value>
                      </property>
                      <property name="path">
                          <value>/${spaces.company_home.childname}</value>
                      </property>
                  </bean>
                  <bean id="Repository_archive"
   class="org.alfresco.repo.imap.config.ImapConfigMountPointsBean">
                      <property name="mode">
                          <value>archive</value>
                      </property>
                      <property name="store">
                          <value>${spaces.store}</value>
                      </property>
                      <property name="path">
                          <value>/${spaces.company_home.childname}</value>
                      </property>
                  </bean>
              </list>
          </property>
  ```

```
    </bean>
```

Other beans in the subsystem application context can use `imap.server.mountPoints` as though it were a regular list of `ImapConfigMountPointsBeans`.

Extension classpath

The `alfresco-global.properties` file can only be used to define properties that are global to the whole system. You can also control the properties of subsystems that may have multiple instances, for example, the Authentication subsystems. To do this, you need to target different values for the same properties, to each subsystem instance. You can use the extension classpath mechanism.

1. Add a property file to your application server's global classpath.

   For example, under `$TOMCAT_HOME/shared/classes`.
2. Create the path to match the following pattern to override specific properties of a subsystem instance:

   ```
   alfresco/extension/subsystems/<category>/<type>/<id>/*.properties
   ```

   The `<id>` is the subsystem instance identifier, which will be default for single instance subsystems, or the provided identifier for chained subsystems.

For example, if your authentication chain looked like this:

```
authentication.chain=alfrescoNtlm1:alfrescoNtlm,ldap1:ldap
```

Then you could put property overrides for alfrescoNtlm1 in the following file:

```
alfresco/extension/subsystems/Authentication/alfrescoNtlm/alfrescoNtlm1/
mychanges.properties
```

The default type and ID of non-chained subsystems is default, so you could put overrides for file server properties in the following file:

```
alfresco/extension/subsystems/fileServers/default/default/mychanges.properties
```

Configuring OpenOffice

Within Alfresco, you can transform a document from one format to another. This feature requires you to install OpenOffice.

Alfresco supports the following OpenOffice subsystems:

OOoDirect
The direct OpenOffice integration, in which the Alfresco server manages OpenOffice directly. This subsystem is enabled, by default.

OOoJodconverter
The JodConverter integration, which is a library that improves the stability and performance of OpenOffice.org (OOo) within Alfresco. This subsystem is disabled, by default. The OOoJodConverter runs on the same machine as the Alfresco server. The JodConverter supports:

- a pool of separate OpenOffice processes
- automatic restart of crashed OpenOffice processes
- automatic termination of slow OpenOffice operations
- automatic restart of any OpenOffice process after a number of operations (this is a workaround for OpenOffice memory leaks)

Changing the OpenOffice subsystem

The default subsystem for OpenOffice transformations is OOoDirect. You can change the preferred OpenOffice subsystem to OOoJodconverter.

The JodConverter requires OpenOffice.org 3.0.0 or later and recommends 3.1.0+.

There are two methods that you can use to change OpenOffice subsystem.

- Modifying the `alfresco-global.properties` file
- Runtime administration using your JMX client

Global properties file

1. Open the `alfresco-global.properties` file.
2. Uncomment the following lines:
   ```
   #ooo.enabled=false
   #jodconverter.enabled=true
   ```
3. Save the file.
4. Restart the Alfresco server.

JMX interface runtime administration

1. Open your JMX client, for example, JConsole.
2. Locate the **OOoDirect** subsystem.
3. Edit the **ooo.enabled** value to `false`.
4. Restart the subsystem.
5. Locate the **OOoJodconverter** subsystem.
6. Edit the **jodconverter.enabled** value to true.
7. Restart the subsystem.

Although it is possible to run both subsystems, Alfresco recommends that you enable only one at a time.

OOoDirect subsystem configuration properties

The following properties can be configured for the OOoDirect subsystem.

ooo.exe
Specifies the OpenOffice installation path.

ooo.enabled
Enables or disables the OOoDirect subsystem.

OOoJodconverter subsystem configuration properties

The following properties can be configured for the OOoJodconverter subsystem.

jodconverter.enabled
Enables or disables the JodConverter process(es).

jodconverter.maxTasksPerProcess
Specifies the number of transforms before the process restarts. The default is 200.

jodconverter.officeHome

Specifies the name of the OpenOffice install directory. The following are examples of install directory paths:

- Linux: `jodconverter.officeHome=/usr/lib/openoffice`
- Mac: `jodconverter.officeHome=/Applications/OpenOffice.org.app/Contents`
- Windows: `jodconverter.officeHome=c:/Alfresco/OpenOffice.org`

jodconverter.portNumbers

Specifies the port numbers used by each processing thread. The number of process will match the number of ports. The default numbers are 2022, 2023, and 2024.

jodconverter.taskExecutionTimeout

Specifies the maximum number of milliseconds that an operation is allowed to run before it is aborted. It is used to recover from operations that have hung. The default is 120000 milliseconds (2 minutes).

jodconverter.taskQueueTimeout

Specifies the maximum number of milliseconds a task waits in the transformation queue before the process restarts. It is used to recover hung OpenOffice processes. The default is 30000 milliseconds (30 seconds).

Configuring synchronization

The synchronization subsystem manages the synchronization of Alfresco with all the user registries (LDAP servers) in the authentication chain.

The synchronization subsystem supports two modes of synchronization:

Full

All users and groups are queried, regardless of when they were last modified. All local copies of these users and groups already existing are then updated and new copies are made of new users and groups. Since processing all users and groups in this manner may be fairly time consuming, this mode of synchronization is usually only triggered on the very first sync when the subsystem first starts up. However, synchronization can also be triggered in this mode by the scheduled synchronization job, if `synchronization.synchronizeChangesOnly` is set to false.

Differential

Only those users and groups changed since the last query are queried and created/updated locally. This differential mode is much faster than full synchronization. By default, it is triggered when the subsystem starts up after the first time and also when a user is successfully authenticated who does not yet have a local person object in Alfresco. This means that new users, and their group information, are pulled over from LDAP servers as and when required with minimal overhead.

Synchronization deletion

Users and groups that are created as a result of a synchronization operation are tagged with an originating zone ID. This records the identifier of the authentication subsystem instance from which the user or group was queried.

On synchronization with a zone, only those users and groups tagged with that zone are candidates for deletion. This avoids the accidental deletion of built-in groups, such as `ALFRESCO_ADMINISTRATORS`.

Collision resolution

If there are overlaps between the contents of two user registries in the authentication chain (for example, where two user registries both contain a user with the same user name), then the registry that occurs earlier in the authentication chain will be given precedence. This means that exactly the same order of precedence used during authentication will be used during synchronization.

For example, if user `A` is queried from zone `Z1` but already exists in Alfresco in zone `Z2`:

- `A` is moved to `Z1` if it is earlier in the authentication chain
- `A` is ignored if `Z1` is later in the authentication chain

Synchronization configuration properties

The following properties can be configured for the synchronization subsystem.

synchronization.synchronizeChangesOnly
Specifies if the scheduled synchronization job is run in differential mode. The default is false, which means that the scheduled sync job is run in full mode. Regardless of this setting a differential sync may still be triggered when a user is successfully authenticated who does not yet exist in Alfresco.

synchronization.import.cron
Specifies a cron expression defining when the scheduled synchronization job should run, by default at midnight every day.

synchronization.syncOnStartup
Specifies whether to trigger a differential sync when the subsystem starts up. The default is true. This ensures that when user registries are first configured, the bulk of the synchronization work is done on server startup, rather than on the first login.

synchronization.syncWhenMissingPeopleLogIn
Specifies whether to trigger a differential sync when a user is successfully authenticated who does not yet exist in Alfresco. The default is true.

synchronization.autoCreatePeopleOnLogin
Specifies whether to create a user with default properties when a user is successfully authenticated, who does not yet exist in Alfresco, and was not returned by a differential sync (if enabled with the property above). The default is true. Setting this to false allows you to restrict Alfresco to a subset of those users who could be authenticated by LDAP; only those created by synchronization are allowed to log in. You can control the set of users in this more restricted set by overriding the user query properties of the LDAP authentication subsystem.

Configuring file servers

The File Server subsystem allows access to the Alfresco data stores through the SMB/CIFS, FTP, and NFS protocols. This allows you to browse to the repository using Windows Explorer or by creating a Network Place.

CIFS, FTP, and NFS traffic must be targeted to a single-cluster node. In a clustered installation, concurrent writes to the same documents using file server protocols (CIFS, FTP, or NFS) and other clients are not currently recommended.

As with other Alfresco subsystems, the File Server subsystem exposes all of its configuration options as properties that can be controlled through a JMX interface or the global properties file.

The sections that follow describe each of the configurable properties supported by the File Server subsystem.

Configuring SMB/CIFS server

The server includes Java socket-based implementations of the SMB/CIFS protocol that can be used on any platform.

The server can listen for SMB traffic over the TCP protocol (native SMB) supported by Windows 2000 and later versions, and the NetBIOS over TCP (NBT) protocol, supported by all Windows versions. There is also a Windows-specific interface that uses Win32 NetBIOS API calls using JNI code. This allows the Alfresco CIFS server to run alongside the native Windows file server.

The default configuration uses the JNI-based code under Windows and the Java socket based code under Linux, Solaris, and Mac OS X.

CIFS file server properties

The following properties can be configured for the SMB/CIFS server.

cifs.enabled
Enables or disables the CIFS server.

cifs.serverName
Specifies the host name for the Alfresco CIFS server. This can be a maximum of 16 characters and must be unique on the network. The special token `{localname}` can be used in place of the local server's host name and a unique name can be generated by prepending/ appending to it.

cifs.domain
An optional property. When not empty, specifies the domain or workgroup to which the server belongs. This defaults to the domain/workgroup of the server, if not specified.

cifs.hostannounce
Enables announcement of the CIFS server to the local domain/workgroup so that it shows up in Network Places/Network Neighborhood.

cifs.sessionTimeout
Specifies the CIFS session timeout value in seconds. The default session timeout is 15 minutes. If no I/O occurs on the session within this time then the session will be closed by the server. Windows clients send keep-alive requests, usually within 15 minutes.

Java-based SMB properties

The following properties will only take effect on non-Windows servers, where the Java-based SMB implementation is used, unless it is enabled on Windows using the advanced Spring bean definition overrides.

cifs.broadcast
Specifies the broadcast mask for the network.

cifs.bindto
Specifies the network adapter to which to bind. If not specified, the server will bind to all available adapters/addresses.

cifs.tcpipSMB.port
Controls the port used to listen for the SMB over TCP/IP protocol (or native SMB), supported by Win2000 and above clients. The default port is 445.

cifs.ipv6.enabled
Enables the use of IP v6 in addition to IP v4 for native SMB. When `true`, the server will listen for incoming connections on IPv6 and IPv4 sockets.

cifs.netBIOSSMB.namePort
Controls the NetBIOS name server port on which to listen. The default is 137.

cifs.netBIOSSMB.datagramPort
Controls the NetBIOS datagram port. The default is 138.

cifs.netBIOSSMB.sessionPort
Controls the NetBIOS session port on which to listen for incoming session requests. The default is 139.

cifs.WINS.autoDetectEnabled
When `true` causes the `cifs.WINS.primary` and `cifs.WINS.secondary` properties to be ignored.

cifs.WINS.primary
Specifies a primary WINS server with which to register the server name.

cifs.WINS.secondary
Specifies a secondary WINS server with which to register the server name.

cifs.disableNIO
Disables the new NIO-based CIFS server code and reverts to using the older socket based code.

Windows native SMB

The following property will only take effect on Windows servers, where by default a JNI-based CIFS implementation is in use.

cifs.disableNativeCode
When `true`, switches off the use of any JNI calls and JNI-based CIFS implementations.

Running SMB/CIFS from a normal user account

On Unix-like systems such as Linux and Solaris, the default Alfresco setup must be run using the root user account so that the CIFS server can bind to the privileged ports (TCP 139/445 UDP 137/138).

The CIFS server can be configured to run using non-privileged ports and then use firewall rules to forward requests from the privileged ports to the non-privileged ports.

1. To configure the CIFS server to use non-privileged ports, use the following property settings:

   ```
   cifs.tcpipSMB.port=1445
   cifs.netBIOSSMB.namePort=1137
   cifs.netBIOSSMB.datagramPort=1138
   cifs.netBIOSSMB.sessionPort=1139
   ```

   Other port numbers can be used but must be above 1024 to be in the non-privileged range.

   The firewall rules should then be set up to forward requests:

   - TCP ports 139/445 to TCP 1139/1445
   - UDP ports 137/138 to UDP 1137/1138

2. On Mac OS X the following commands can be used:

   ```
   sysctl -w net.inet.ip.fw.enable=1
   sysctl -w net.inet.ip.forwarding=1
   sysctl -w net.inet.ip.fw.verbose=1
   sysctl -w net.inet.ip.fw.debug=0
   ipfw flush
   ipfw add 100 allow ip from any to any via lo0
   # Forward native SMB and NetBIOS sessions to non-privileged ports
   ipfw add 200 fwd <local-ip>,1445 tcp from any to me dst-port 445
   ipfw add 300 fwd <local-ip>,1139 tcp from any to me dst-port 139
   # Forward NetBIOS datagrams to non-privileged ports (does not currently
    work)
   ```

```
ipfw add 400 fwd <local-ip>,1137 udp from any to me dst-port 137
ipfw add 500 fwd <local-ip>,1138 udp from any to me dst-port 138
```

Replace `<local-ip>` with the IP address of the server that Alfresco is running on.

3. On Linux, the following commands can be used to get started, but be aware these commands will delete all existing firewall and NAT rules and could be a security risk:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
modprobe iptable_nat
iptables -F
iptables -t nat -F
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 445 -j REDIRECT --to-ports
 1445
iptables -t nat -A PREROUTING -p tcp --dport 139 -j REDIRECT --to-ports
 1139
iptables -t nat -A PREROUTING -p udp --dport 137 -j REDIRECT --to-ports
 1137
iptables -t nat -A PREROUTING -p udp --dport 138 -j REDIRECT --to-ports
 1138
```

   The UDP forwarding does not work, which affects the NetBIOS name lookups. A workaround is either to add a DNS entry matching the CIFS server name and/or add a static WINS mapping, or add an entry to the clients `LMHOSTS` file.

SMB/CIFS advanced Spring overrides

The SMB/CIFS server beans are declared in the `file-servers-context.xml` file in `<configRoot>\classes\alfresco\subsystems\fileServers\default\`. Using the subsystem extension classpath mechanism, you can place site specific customization of these default values in a Spring bean file in `<extension>\subsystems\fileServers\default\default\custom-file-servers-context.xml` (note that the `default\default` part of the path is intentional).

The main bean that drives the CIFS server configuration is called `cifsServerConfig`. This has several properties that can be populated with child beans that control various optional SMB implementations.

tcpipSMB
Controls the Java-based SMB over TCP/IP implementation, which is compatible with Windows 2000 clients and later.

netBIOSSMB
Controls the Java-based NetBIOS over TCP/IP implementation, which is compatible with all Windows clients.

win32NetBIOS
Controls the JNI-based NetBIOS over TCP/IP implementation, which is only enabled for Alfresco servers running on Windows.

When one of the above properties is not set, it deactivates support for the corresponding protocol implementation. The `tcpipSMB` and `netBIOSSMB` beans have a platforms property that allows their configuration to be targeted to Alfresco servers running on specific platforms. The property is formatted as a comma-separated list of platform identifiers. Valid platform identifiers are `linux`, `solaris`, `macosx`, and `aix`.

1. To run the native SMB over TCP/IP protocol under Windows, you need to disable Windows from using the port by editing, or creating, the following registry key:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]
 "SMBDeviceEnabled"=dword:00000000
```

2. To enable the Java socket based NetBIOS implementation under Windows disable NetBIOS on one or all network adapters.

This can be done using the Network Connections control panel in the advanced TCP/IP properties for each adapter.

3. The `serverComment` of the `cifsServerConfig` bean controls the comment that is displayed in various information windows.
4. The `sessionDebugFlags` property of the `cifsServerConfig` bean enables debug output levels for CIFS server debugging. The value should be in the form of a comma-separated list of the flag names.

Flag	Description
`NetBIOS`	NetBIOS layer
`State`	Session state changes
`Tree`	File system connection/disconnection
`Search`	Folder searches
`Info`	File information requests
`File`	File open/close
`FileIO`	File read/write
`Tran`	Transaction requests
`Echo`	Echo requests
`Errors`	Responses returning an error status
`IPC`	IPC$ named pipe
`Lock`	File byte range lock/unlock
`Pkttype`	Received packet type
`Dcerpc`	DCE/RPC requests
`Statecache`	File state caching
`Notify`	Change notifications
`Streams`	NTFS streams
`Socket`	NetBIOS/native SMB socket connections
`PktPool`	Memory pool allocations/de-allocations
`PktStats`	Memory pool statistics dumped at server shutdown
`ThreadPool`	Thread pool

5. The `log4j.properties` file must also have SMB/CIFS protocol debug output enabled using:

```
log4j.logger.org.alfresco.smb.protocol=debug
```

6. The following logging level must also be enabled to log debug output from the core file server code:

```
log4j.logger.org.alfresco.fileserver=debug
```

Configuring the FTP file server

This section describes how to configure the FTP file server.

FTP file server properties

The following properties can be configured for the FTP server.

ftp.enabled
Enables or disables the FTP server.

ftp.port
Specifies the port that the FTP server listens for incoming connections on. Defaults to port 21. On some platforms ports below 1024 require the server to be run under a privileged account.

ftp.ipv6.enabled
Enables or disables the IPv6 extensions to allow the use of an IPv6-style addresses.

ftp.dataPortFrom
Limits the data ports to a specific range of ports. This property sets the lower limit.

ftp.dataPortTo
Limits the data ports to a specific range of ports. This property sets the upper limit.

ftp.keyStore
Specifies the path to the `keystore` file for FTPS support.

ftp.trustStore
Specifies the path to the `truststore` file for FTPS support.

ftp.passphrase
Specifies the passphrase for the `keystore` and `truststore` files.

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`.

ftp.sslEngineDebug
Enables additional debug output from the Java SSLEngine class.

The FTPS support runs over the same socket as normal connections; the connection is switched into SSL mode at the request of the client, usually before the user name and password is sent. The client can switch the socket back to plain text mode using the `CCC` command.

The `ftp.keyStore`, `ftp.trustStore`, and `ftp.passphrase` values must all be specified to enable FTPS support. Only explicit FTP over SSL/TLS mode is supported. Encrypted data sessions are not supported.

To setup the `keystore` and `truststore` files, follow the instructions from the Java6 JSSE Reference Guide. This will provide the values required for the `ftp.keyStore`, `ftp.trustStore` and `ftp.passphrase` values.

Enable debug output by setting the `SSL` debug flag using `ftp.sessionDebug=SSL`, and also by enabling the `log4j.logger.org.alfresco.fileserver=debug` log4j output.

FTP advanced Spring overrides

The FTP server beans are declared in the `file-servers-context.xml` file in `<configRoot>\classes\alfresco\subsystems\fileServers\default`. Using the subsystem extension classpath mechanism, site specific customisation of these default values can be placed in a Spring bean file in `<extension>\subsystems\fileServers\default\default\custom-file-servers-context.xml` (note that the `default\default` part of the path is intentional).

The following properties can be overridden on the `ftpServerConfig` bean.

bindTo
Specifies the address the FTP server binds to, if not specified the server will bind to all available addresses.

rootDirectory
Specifies the path of the root directory as an FTP format path, that is, using forward slashes. The first part of the path should be the file system name, optionally followed by one or more folder names, for example:

```
/Alfresco/myfolder/
```

charSet
Specifies the character set to be used. The character set name should be a valid Java character set, see the Java `CharSet` class for more information.

1. The `debugFlags` property enables debug output levels for FTP server debugging. The value should be a comma-separated list of flag names from the following table:

Flag	Description
`State`	Session state changes
`Search`	Folder searches
`Info`	File information requests
`File`	File open/close
`FileIO`	File read/write
`Error`	Errors
`Pkttype`	Received packet type
`Timing`	Time packet processing
`Dataport`	Data port
`Directory`	Directory commands

2. Configure logging levels for the FTP server in `$ALF_HOME/tomcat/webapps/alfresco/WEB-INF/classes/log4j.properties` using:

```
log4j.logger.org.alfresco.ftp.protocol=debug
log4j.logger.org.alfresco.ftp.server=debug
```

Configuring the NFS file server

It is recommended that TCP connections are used to connect to the Alfresco NFS server. Using a read/write size of 32K will also help to optimize the performance.

NFS file server properties

The following properties can be configured for the NFS server.

nfs.enabled
Enables or disables the NFS server.

nfs.user.mappings
A composite property that configures the user ID/group ID to the Alfresco user name mappings that are used by the current RPC authentication implementation.

For example, the following configuration gives `admin` a `uid` and `gid` of 0 and `auser` a `uid` and `gid` of 501.

```
nfs.user.mappings=admin,auser
nfs.user.mappings.value.admin.uid=0
nfs.user.mappings.value.admin.gid=0
nfs.user.mappings.value.auser.uid=501
nfs.user.mappings.value.auser.gid=501
```

NFS advanced Spring overrides

The NFS server beans are declared in the `file-servers-context.xml` file in `<configRoot>\classes\alfresco\subsystems\fileServers\default`. Using the subsystem extension classpath mechanism, site specific customisation of these default values can be placed in a Spring bean file in `<extension>\subsystems\fileServers\default\default\custom-file-servers-context.xml` (note that the default\default part of the path is intentional).

The following properties can be overridden on the `nfsServerConfig` bean.

portMapperEnabled
Enables the built-in portmapper service. This would usually be enabled on Windows where there is no default portmapper service. Under Linux/Unix operating systems, the built-in portmapper service can be used, which also saves having to run the Alfresco server using the root account.

threadPool
Sets the size of the RPc processing thread pool. The minimum number of threads is 4, the default setting is 8.

packetPool
Sets the size of the packet pool used to receive RPC requests and send RPC replies. The minimum number of packets is 10, the default setting is 50.

portMapperPort
The port number to run the portmapper service on. The default port is 111.

mountServerPort
The port number to run the mountserver service on. The default is to allocate an available non-privileged port.

nfsServerPort
The port number to run main NFS server service on. The default is to allocate the default NFS port: 2049. This will likely clash with a running native NFS server.

1. The `debugFlags` property enables debug output levels for NFS server debugging. The value should be in the form of a comma-separated list of the flag names in the following table.

Flag	Description
`RxData`	Request data details
`TxData`	Response data details
`DumpData`	Hex dump request/response data
`Search`	Folder searches
`Info`	File information requests
`File`	File open/close
`FileIO`	File read/write
`Error`	Errors
`Directory`	Directory commands
`Timing`	Time packet processing
`Session`	Session creation/deletion

2. The log4j.properties file must also have NFS protocol debug output enabled using:

```
log4j.logger.org.alfresco.nfs.server=debug
```

3. The following logging level must also be enabled to log debug output from the core file server code:

   ```
   log4j.logger.org.alfresco.fileserver=debug
   ```

4. There are also the following log4j output options for the NFS/mount/portmapper services:

   ```
   log4j.logger.org.alfresco.nfs.protocol=debug
   ```

5. Output server level debug information from the NFS, mount and portmapper services.

   ```
   log4j.logger.org.alfresco.nfs.protocol.auth=debug
   ```

Configuring email

The email subsystem allows you to configure the outbound and inbound SMTP email settings to interact with Alfresco.

There are two methods of running Alfresco email server:

- Running the email server process in the same JVM context as the repository
- Running the email server remotely and communicate with the repository using Remote Method Invocation (RMI)

OutboundSMTP configuration properties

The following properties can be configured for the OutboundSMTP subsystem type.

You must set the Outbound email configuration for Share invitations to work correctly. If you do not set the email configuration, when you invite a user to a site, the user will not receive the assigned task notification.

mail.host=yourmailhost.com
Specifies the name of the SMTP host.

mail.port=25
Specifies the port number on which the SMTP service runs (the default is 25).

mail.username=username
Specifies the user name of the account from which you want email to be sent.

mail.password=password
Specifies the password for the user name.

mail.encoding=UTF-8
Specifies UTF-8 encoding for email.

mail.from.default=admin@alfresco.com
Specifies the email address from which all email notifications are sent.

mail.smtp.auth=false
Specifies whether you authorization is required.

mail.protocol=smtp
Specifies the default protocol to be used for email.

The following properties can be set to define a test message when the subsystem starts.

mail.testmessage.send=false
Defines whether or not to send a test message.

mail.testmessage.to=
Specifies the recipient of the test message.

mail.testmessage.subject=Outbound SMTP
Specifies the message subject of the test message.

mail.testmessage.text=Outbound SMTP email subsystem is working.
Specifies the message body of the test message.

InboundSMTP configuration properties

The InboundSMTP email subsystem type allows you to configure the behavior of the email server and service.

The following properties can be set for Inbound SMTP email.

email.inbound.unknownUser=anonymous
Specifies the user name to authenticate as when the sender address is not recognized.

email.inbound.enabled=true
Enables or disables the inbound email service. The service could be used by processes other than the email server (for example, direct RMI access), so this flag is independent of the email service.

email.server.enabled=true
Enables the email server.

email.server.port=25
Specifies the default port number for the email server.

email.server.domain=alfresco.com
Specifies the default domain for the email server.

email.server.allowed.senders=.*
Provides a comma-separated list of email REGEX patterns of allowed senders. If there are any values in the list, then all sender email addresses must match. For example: `.*\@alfresco\.com`, `.*\@alfresco\.org`.

email.server.blocked.senders=
Provides a comma-separated list of email REGEX patterns of blocked senders. If the sender email address matches this, then the message will be rejected. For example: `.*\@hotmail\.com`, `.*\@googlemail\.com`.

Configuring the RMI email service

You can run the email server remotely on a separate JVM and server, and have it interact with the Alfresco server using Remote Method Invocation (RMI).

1. Browse to the folder `<configRoot>/classes/alfresco`.
2. Open the configuration file `remote-email-service-context.xml`.

   This file contains the `emailService` bean, specifying the related RMI configuration.
3. Modify the RMI configuration as required. For example:

Value	Description
`<serviceUrl></serviceUrl>`	Specifies the valid RMI URL.
`<serviceInterface></serviceInterface>`	Specifies the interface used for RMI.

Handling messages by target node type

This section describes the default behaviors for incoming email to different types of referenced nodes.

You can modify or extend the default behaviors by adding in custom handlers.

Folder(Space)
Content added with emailed aspect.

Forum(Discussion)
Content specialized to Post with emailed aspect; if email subject matches a topic, then add to topic, otherwise create new topic based on subject.

Topic(Post)
Content specialized to Post with emailed aspect; if referenced node is a Post, add to Post's parent Topic.

Document(Content)
If discussion exists, same as for forums, otherwise add discussion with email as initial topic and post.

Groups and permissions for email

An email arriving at the Alfresco email server is unauthenticated. An authentication group, `EMAIL_CONTRIBUTORS` , must be created to allow permissions to be handled at a high level by the administrator.

When an email comes into the system, the only identification is the sender's email address. The user is look-up is based on the email address.

- If a matching user is not found, then the current user is assumed to be unknown, if unknown exists
- If unknown does not exist, then the email is rejected as authentication will not be possible
- If the user selected is not part of email contributor's group, then the email is rejected

The current request's user is set and all subsequent processes are run as the authenticated user. If any type of authentication error is generated, then the email is rejected. The authentication will also imply that the authenticated user may not have visibility of the target node, in which case the email is also rejected. Effectively, this means that the target recipient of the email does not exist, at least not for the sender.

The current default server configuration creates the `EMAIL_CONTRIBUTORS` group and adds the `admin` user to this group.

Configuring IMAP Protocol support

IMAP protocol support allows email applications that support IMAP (including Outlook, Apple Mail, Thunderbird, and so on) to connect to and interact with Alfresco repositories, directly from the email application.

Enabling the IMAP Protocol

The IMAP protocol server is disabled by default. You need to enable the IMAP protocol server to start interaction between the email client and the Alfresco repository.

1. Open the `alfresco-global.properties` file.
2. Add the following sample configuration entries:

```
imap.server.enabled=true
imap.server.port=143
imap.server.host=localhost
```

Do not use `localhost` as the `imap.server.host`. Replace this value with the IP address (or corresponding DNS address) of your external IP interface. A value of 0.0.0.0 in Unix will ensure it listens on the specified port on all IP interfaces.

3. Restart your Alfresco server.

Once the Alfresco server has restarted, the new configuration will take effect. Since the IMAP server has only one instance, make your configuration changes to the `<extension root>alfresco-global.properties` file. You can also make your changes to `<extension root>\alfresco\extension\subsystems\imap\default\default` for the IMAP subsystem configuration to take precedence.

IMAP subsystem properties

The following properties can be configured for the IMAP subsystem.

The following properties control the IMAP subsystem.

imap.server.enabled
Enables or disables the IMAP subsystem.

imap.server.port=143
IMAP has a reserved port number of 143. You can change it using this property.

imap.server.host=<your host name>
Replace this value with the IP address (or corresponding DNS address) of your external IP interface. A value of 0.0.0.0 in Unix will make it listen on the specified port on all IP interfaces.

You should also configure the following properties of the sysAdmin subsystem.

alfresco.protocol
The protocol component of the alfresco web application URL, for example, `http`.

alfresco.host
The host name of the Alfresco URL, which is externally resolved. Use `${localname}` for the locally-configured host name.

alfresco.port
The port number of the Alfresco URL, which is externally resolved. For example, `8080`

alfresco.context
The context path component of the Alfresco URL. Typically this is `alfresco`.

To configure the IMAP Home space, which is used to store user mailboxes in ARCHIVE mode, in particular the user's INBOX, use the following properties.

imap.config.home.store=${spaces.store}
Specifies the default location for the IMAP mount point. For example, `${spaces.store}`.

imap.config.home.rootPath=/${spaces.company_home.childname}
Specifies the default location for the IMAP mount point. For example, `/${spaces.company_home.childname}`.

imap.config.home.folderPath=Imap Home
Specifies the default locations for the IMAP mount point. For example, `Imap Home`.

An IMAP message may contain a message and a set of attachments, and the IMAP server can split the attachments into separate content nodes.

imap.server.attachments.extraction.enabled
Defines whether or not attachments are extracted.

IMAP mount points

IMAP mount points are used to control which folders are available using IMAP and the mode in which they are accessed. Modes are used to define the type of interaction available.

The IMAP integration offers the following access modes:

Archive
: Allows emails to be written to and read from Alfresco by the IMAP client by drag and drop, copy/paste, and so on, from the email client.

Virtual
: Documents managed by Alfresco may be viewed as emails from the IMAP client. Documents are shown as virtual emails with the ability to view metadata and trigger actions on the document, using links included in the email body.

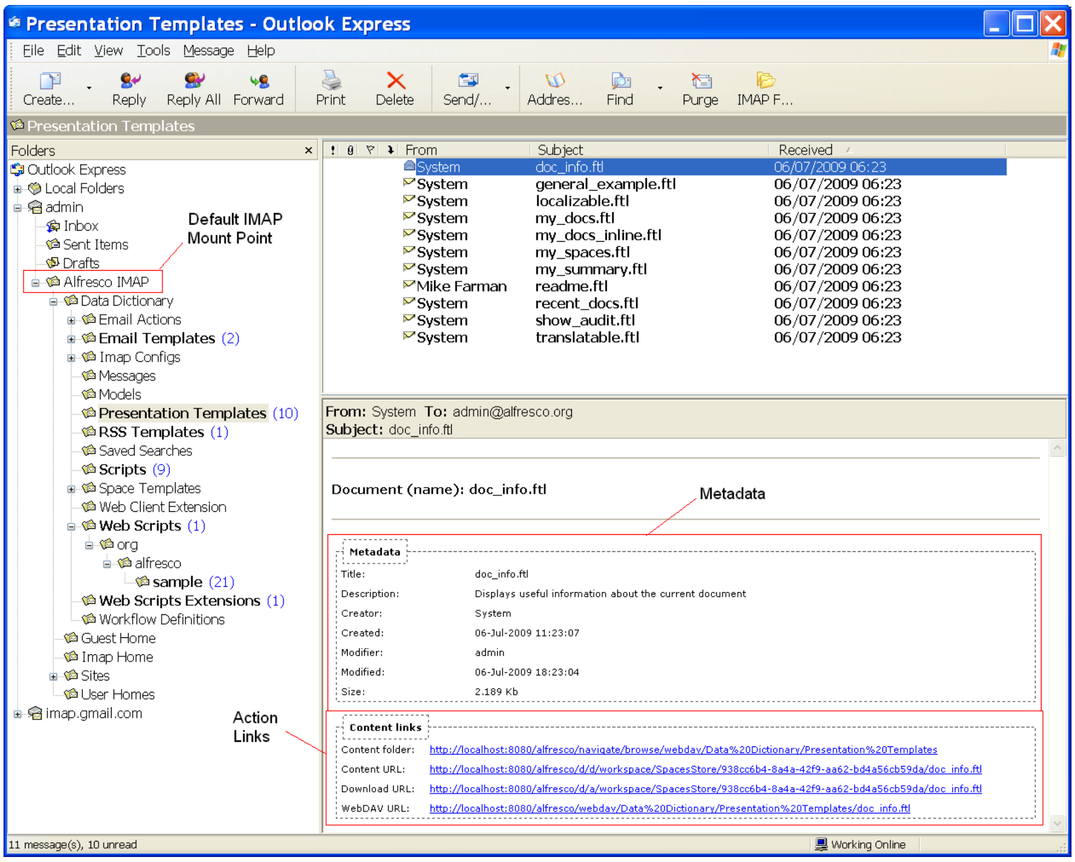
Mixed
: A combination of both archive and virtual modes, that is, both document access and email management are available.

By default, a single mount point called **AlfrescoIMAP** is defined for **Company Home** and you can change it or add more mount points.

Virtual view email format

The virtualized view uses presentation templates to generate the mail body and display document metadata, action links (for download, view, webdav, folder) and Start Workflow form (HTML view only).

The templates are stored in the repository in **Company Home > Data Dictionary > Imap Configs > Templates**. Separate templates are available to generate either a HTML or plain text body, based on the the format request by the email client. The templates can be customized to change the metadata and actions available in the email body.



From	Subject	Received
System	doc_info.ftl	06/07/2009 06:23
System	general_example.ftl	06/07/2009 06:23
System	localizable.ftl	06/07/2009 06:23
System	my_docs.ftl	06/07/2009 06:23
System	my_docs_inline.ftl	06/07/2009 06:23
System	my_spaces.ftl	06/07/2009 06:23
System	my_summary.ftl	06/07/2009 06:23
Mike Farman	readme.ftl	06/07/2009 06:23
System	recent_docs.ftl	06/07/2009 06:23
System	show_audit.ftl	06/07/2009 06:23
System	translatable.ftl	06/07/2009 06:23

From: System **To:** admin@alfresco.org
Subject: doc_info.ftl

Document (name): doc_info.ftl

Metadata

Title:	doc_info.ftl
Description:	Displays useful information about the current document
Creator:	System
Created:	06-Jul-2009 11:23:07
Modifier:	admin
Modified:	06-Jul-2009 18:23:04
Size:	2.189 Kb

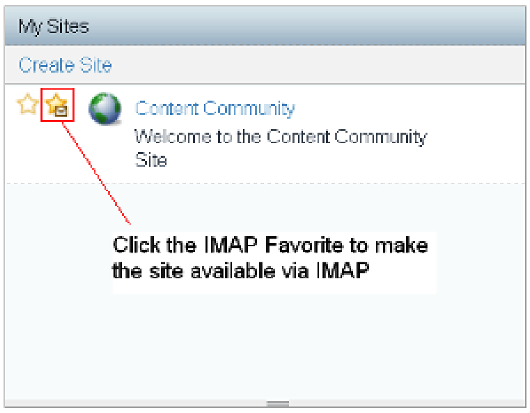
Content links

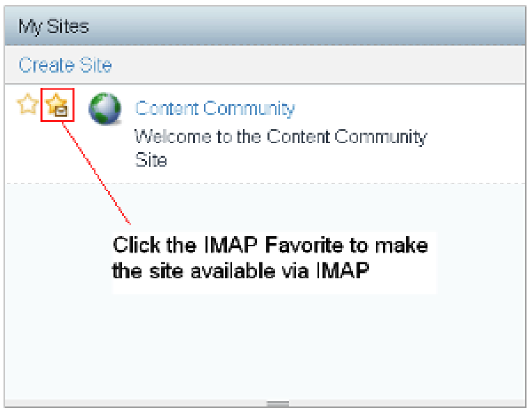
Content folder:	http://localhost:8080/alfresco/navigate/browse/webdav/Data%20Dictionary/Presentation%20Templates
Content URL:	http://localhost:8080/alfresco/d/d/workspace/SpacesStore/938cc6b4-8a4a-42f9-aa62-bd4a56cb59da/doc_info.ftl
Download URL:	http://localhost:8080/alfresco/d/a/workspace/SpacesStore/938cc6b4-8a4a-42f9-aa62-bd4a56cb59da/doc_info.ftl
WebDAV URL:	http://localhost:8080/alfresco/webdav/Data%20Dictionary/Presentation%20Templates/doc_info.ftl

Marking sites as IMAP favorites

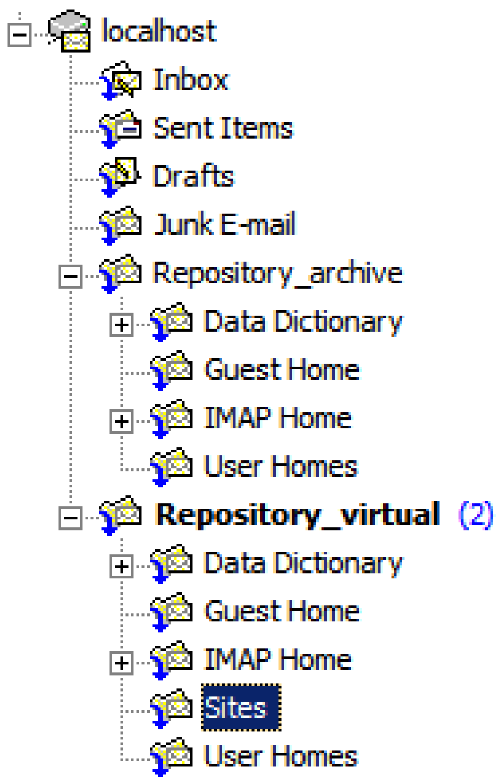
To have access to Alfresco Share sites using IMAP, the site(s) need to be added to your list of sites using Share IMAP Favorites.

1. Select **IMAP Favorites** in the Share **My Sites** dashlet on your **My Dashboard** page:


My Sites
Create Site
Content Community
Welcome to the Content Community Site
Click the IMAP Favorite to make the site available via IMAP


My Sites
Create Site
Content Community
Welcome to the Content Community Site
Click the IMAP Favorite to make the site available via IMAP

2. Refresh your IMAP view to see the new sites.



You can see the site added to the IMAP Sites folder.

Configuring system properties

The sysAdmin subsystem allows real time control across some of the general repository properties. The sysAdmin subsystem replaces the `RepoServerMgmt` management bean.

sysAdmin subsystem properties

The following properties can be configured for the sysAdmin subsystem.

server.maxusers
The maximum number of users who are allowed to log in or -1 if there is no limit.

server.allowedusers
A comma-separated list of users who are allowed to log in. Leave empty if all users are allowed to log in.

server.transaction.allow-writes
A Boolean property that when true indicates that the repository will allow write operations (provided that the license is valid). When false the repository is in read-only mode.

The following properties specify the parameters that control how Alfresco generates URLs to the repository and Share. These parameters may need to be edited from their default values to allow the URLs to be resolved by an external computer.

alfresco.context
Specifies the context path of the Alfresco repository web application. The default is `alfresco`.

alfresco.host
Specifies the externally resolvable host name of the UR Alfresco web application. The default value is `${localname}`. If this is used for the value of this property, the token `${localname}` will be automatically replaced by the domain name of the repository server.

alfresco.port
Specifies the externally resolvable port number of the Alfresco web application URL. The default is `8080`.

alfresco.protocol
Specifies the protocol component of the Alfresco web application. The default is `http`.

share.context
Specifies context path component of the Share web application URL The default is `share`.

share.host
Specifies the externally resolvable host name of the Share web application URL. The default value is `${localname}`.

share.port
Specifies the externally resolvable port number of the Share web application URL. The default is `8080`.

share.protocol
Specifies the protocol to use. The default is `http`.

Configuring the repository

This section describes how to configure the Alfresco repository.

Tuning the JVM

The hardware requirements for the Alfresco repository, and Explorer and Share, are variable and depend on the number of concurrent users that access the system. You can tune the memory and garbage collection parameters for the JVM to be appropriate for your situation. This section suggests metrics and estimates, but your system may vary.

Concurrent users are users who are constantly accessing the system through Alfresco Explorer with only a small pause between requests (3-10 seconds maximum) with continuous access 24/7. Casual users are users occasionally accessing the system through Alfresco Explorer or WebDAV/CIFS interfaces with a large gap between requests (for example, occasional document access during the working day).

Disk space usage

The size of your Alfresco repository defines how much disk space you will need; it is a very simple calculation. Content in Alfresco is, by default, stored directly on the disk. Therefore, to hold 1000 documents of 1 MB will require 1000 MB of disk space. You should also make sure there is sufficient space overhead for temporary files and versions. Each version of a file (whether in DM or WCM) is stored on disk as a separate copy of that file, so make sure you allow for that in your disk size calculations (for DM, use versioning judiciously).

Use a server class machine with SCSI Raid disk array. The performance of reading/writing content is almost solely dependent on the speed of your network and the speed of your disk array. The overhead of the Alfresco server itself for reading content is very low as content is streamed directly from the disks to the output stream. The overhead of writing content is also low but depending on the indexing options (for example, atomic or background indexing), there may be some additional overhead as the content is indexed or metadata is extracted from the content in each file.

JVM memory and CPU hardware for multiple users

The repository L2 Cache with initial VM overhead and basic Alfresco system memory is set up with a default installation to require approximately 512 MB (maximum).

This means you can run the Alfresco repository and Explorer with many users accessing the system with a basic single CPU server and only 512 MB of memory assigned to the Alfresco JVM. However, you must add additional memory as your user base grows, and add CPUs depending on the complexity of the tasks you expect your users to perform, and how many concurrent users are accessing the client.

For these metrics, **N** concurrent users is considered equivalent to **10xN** casual users that the server could support.

Number of users	Recommended memory / CPU settings per server
For 50 concurrent or up to 500 casual users	1 GB JVM RAM 2x server CPU (or 1 x Dual-core)
For 100 concurrent users or up to 1000 casual users	1 GB JVM RAM 4x server CPU (or 2 x Dual-core)
For 200 concurrent users or up to 2000 casual users	2 GB JVM RAM 8x server CPU (or 4 x Dual-core)

Concurrent users are considered to be users constantly accessing the system through the Alfresco web-client with only a small pause between requests (3-10 seconds maximum) - with continuous access 24/7. Casual users are considered to be users occasionally accessing the system through the Alfresco web-client or webdav/CIFS interfaces with a large gap between requests (for example, occasional document access during the working day).

Permanent Generation (PermGen) Size

The default PermGen size in Sun JVMs is 64M, which is very close to the total size of permanent objects (Spring beans, caches, and so on) that Alfresco creates. For this reason it is easy to overflow the PermGen as the result of configuration changes or with the addition of custom extensions. It is recommended that you increase the PermGen to avoid OutOfMemory errors, for example, -XX:MaxPermSize=128M is a good starting point.

The size of the PermGen is now increased in the Alfresco startup scripts, so provided you are using those scripts, no changes should be necessary.

Maximum JVM Heap Size 32/64bit

An important calculation to keep in mind is:

```
(Managed Heap + native heap + (thread stack size * number of threads)) cannot
exceed 2GB on 32bit x86 Windows or Linux systems
```

This is a limitation of the Sun Java VM. It means that even if you install 4GB of RAM into your server, a single instance of the JVM cannot grow beyond 2GB on a 32bit server machine.

A 64 bit OS/JVM has much bigger values. It is recommended that a 64bit OS with large memory hardware (>2GB assigned to the JVM) is used for deployments of >250 concurrent or >2500 casual users.

You can also set up your machine to cluster if you prefer to solve multi-user access performance issues with additional machines rather than a single powerful server.

JVM settings

Alfresco generates a high proportion of temporary objects, both in client threads as well as in the background processes. To reduce the number of temporary objects that spill into the OldGen portion of the heap, you need to set the NewSize option as large as possible.

The following settings reduce the garbage collections and reveal (with GC printing and JMX tracing) that the OldGen was not growing noticeably over and above the permanent space allocated for caches. Cache sizes are still estimated top out around 520M. So, for a typical 32 bit installation with at least 2GB available for the VM, you can use the following settings:

```
JAVA_OPTS=
-server
-Xss1024K
-Xms1G
-Xmx2G
-XX:MaxPermSize=128M
-XX:NewSize=512m
```

The following can also be adjusted to control the garbage collection behavior:

```
-XX:+UseConcMarkSweepGC
-XX:+CMSIncrementalMode
-XX:CMSInitiatingOccupancyFraction=80
```

Low end machines

This section applies if you have less than 2GB available.

The stack size of 1024K (-Xss1024K) is generous. Some installations may require a little over 512K on occasion. Many may only use 256K. If the per-thread memory consumption is too high for your installation, reduce the stack size to 512K and then to 256K and note any memory-related errors in the logs.

The `NewSize` should be kept as large as possible. It can be reduced, but the memory consumption should be watched on a monitoring tool, for example, JConsole, to ensure that the rate of spillover of temporary objects is kept down. If the machine is supporting 500 simultaneous operations, for instance, then the spillover of temporary objects (from `NewSize` being too small) will cause hold-ups on memory assignment as the garbage collector does sweeps.

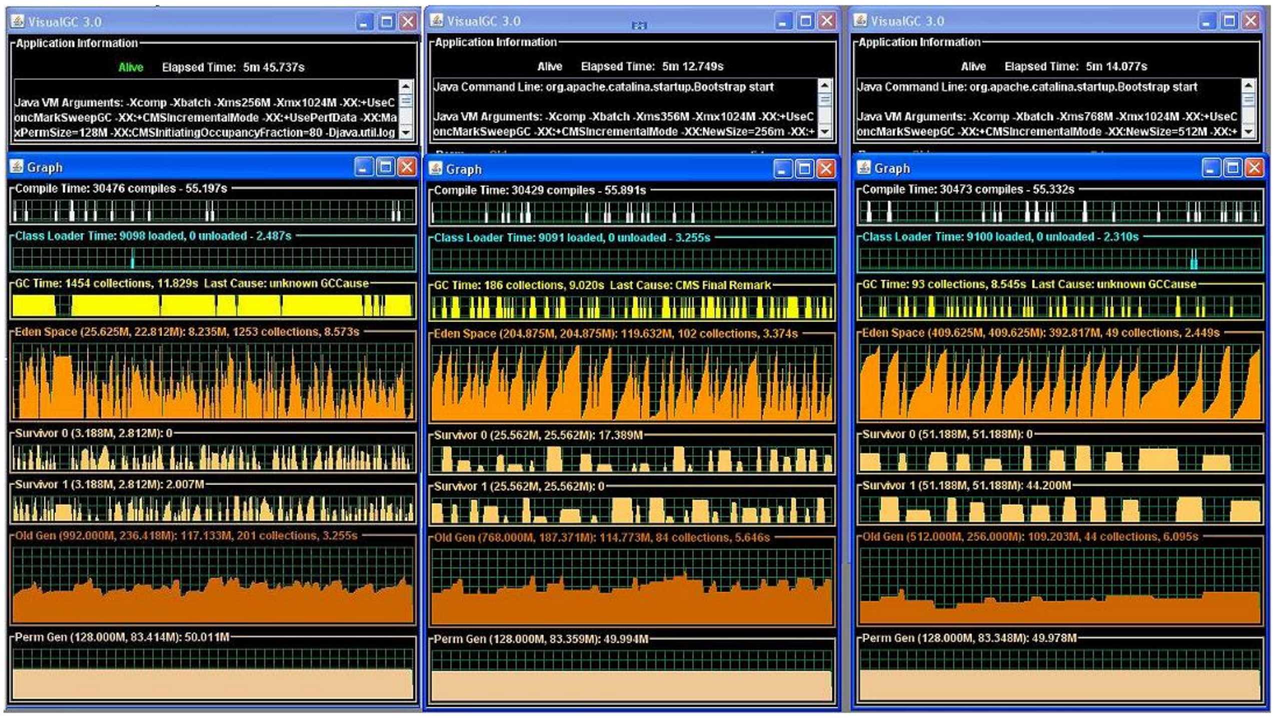
Effects of NewSize

This section describes the settings for OldGen.

Given that the OldGen is composed primarily of cache data of up to about 520M, at least 1GB should be reserved for OldGen. Once -Xmx increases, the OldGen can be increased to 2G. 512M should be left as a buffer to account for miscellaneous (PermGen, and so on). So the following variations might be applied:

```
-Xmx2G -Xms1G -XX:NewSIze=512M (OldGen at least 1G)
-Xmx3G -Xms1G -XX:NewSize=512M (OldGen at least 2G)
-Xmx4G -Xms2G -XX:NewSize=1G (OldGen at least 2.5G)
-Xmx6G -Xms3G -XX:NewSize=2G (OldGen at least 3.5G)
-Xmx8G -Xms4G -XX:NewSize=3G (OldGen at least 4.5G)
```

If you need these levels, you will need to run JConsole (and Java 6) to observe the rate of spillover from Eden space to Survivor to OldGen. If, after the system has been running for a while, the OldGen size stabilizes, then the NewSize can be increased appropriately. The following diagram (using VisualGC) shows how varying the NewSize value affects overall garbage collection activity:


VisualGC 3.0
Application Information
Alive Elapsed Time: 5m 45.737s
Java VM Arguments: -Xcomp -Xbatch -Xms256M -Xmx1024M -XX:+UseConcMarkSweepGC -XX:+CMSIncrementalMode -XX:+UsePerfData -XX:MaxPermSize=128M -XX:CMSInitiatingOccupancyFraction=80 -Djava.util.log
Graph
Compile Time: 30476 compiles - 55.197s
Class Loader Time: 9098 loaded, 0 unloaded - 2.487s
GC Time: 1454 collections, 11.829s Last Cause: unknown GCCause
Eden Space (25.625M, 22.812M): 8.235M, 1253 collections, 8.573s
Survivor 0 (3.188M, 2.812M): 0
Survivor 1 (3.188M, 2.812M): 2.007M
Old Gen (992.000M, 236.418M): 117.133M, 201 collections, 3.255s
Perm Gen (128.000M, 83.414M): 50.011M
VisualGC 3.0
Application Information
Alive Elapsed Time: 5m 12.749s
Java Command Line: org.apache.catalina.startup.Bootstrap start
Java VM Arguments: -Xcomp -Xbatch -Xms356M -Xmx1024M -XX:+UseConcMarkSweepGC -XX:+CMSIncrementalMode -XX:NewSize=256m -XX:+
Graph
Compile Time: 30429 compiles - 55.891s
Class Loader Time: 9091 loaded, 0 unloaded - 3.255s
GC Time: 186 collections, 9.020s Last Cause: CMS Final Remark
Eden Space (204.875M, 204.875M): 119.632M, 102 collections, 3.374s
Survivor 0 (25.562M, 25.562M): 17.389M
Survivor 1 (25.562M, 25.562M): 0
Old Gen (768.000M, 187.371M): 114.773M, 84 collections, 5.646s
Perm Gen (128.000M, 83.359M): 49.994M
VisualGC 3.0
Application Information
Alive Elapsed Time: 5m 14.077s
Java Command Line: org.apache.catalina.startup.Bootstrap start
Java VM Arguments: -Xcomp -Xbatch -Xms768M -Xmx1024M -XX:+UseConcMarkSweepGC -XX:+CMSIncrementalMode -XX:NewSize=512M -XX:+
Graph
Compile Time: 30473 compiles - 55.332s
Class Loader Time: 9100 loaded, 0 unloaded - 2.310s
GC Time: 93 collections, 8.545s Last Cause: unknown GCCause
Eden Space (409.625M, 409.625M): 392.817M, 49 collections, 2.449s
Survivor 0 (51.188M, 51.188M): 0
Survivor 1 (51.188M, 51.188M): 44.200M
Old Gen (512.000M, 256.000M): 109.203M, 44 collections, 6.095s
Perm Gen (128.000M, 83.348M): 49.978M

Command line configuration

The beans that load the `alfresco-global.properties` will give preferential treatment to any JVM-set properties.

Setting properties on the JVM

This section describes how to set the JVM properties.

- (Windows) At a command prompt, enter the following:

  ```
  Set JAVA_OPTS=-Ddir.root=e:/alfresco/data
  ```
- (Linux) At a command prompt, enter the following:

  ```
  export JAVA_OPTS==Ddir.root=/srv/alfresco/data
  ```

Mixing global properties and system property settings

You can use a combination of global properties and system properties for certain customizations. For example, if you wish to distribute a system that has a core set of properties overridden but need to customize the last few for each installation.

1. Activate the properties in the `<classpathRoot>/alfresco-global.properties` file.
2. Set all common defaults for your system.
3. On each installation, add the final configuration values. For example:

   ```
   -Ddb.username=alfresco
   -Ddb.password=alfresco
   -Dhibernate.dialect=org.alfresco.repo.domain.hibernate.dialect.
   AlfrescoOracle9Dialect
   -Dhibernate.default_schema=ALFRESCO_DEV
   -Dindex.tracking.cronExpression='0/5 * * * * ?'
   -Dindex.recovery.mode=AUTO
   -Dalfresco.cluster.name=ALFRESCO_DEV
   ```

Configuring the repository cache

The Alfresco repository uses *Ehcache* in-memory caches. These caches are transaction safe and can be clustered. Caches greatly improve repository performance but they use Java heap memory.

Cache settings depend on the amount of memory available to your Alfresco server. The default `ehcache-default.xml` file is enough for most systems and is currently set for 512MB of cache heap memory. This is the recommended default for a Java heap size of 1GB.

Individual cache settings

All cache settings are in the `<configRoot>\alfresco\ehcache-default.xml` file.

Do not directly modify this file.

Each cache is configured in an XML block similar to the following:

```
<!-- approx 50MB memory required -->
<cache name="org.alfresco.repo.domain.hibernate.NodeImpl.childAssocs"
 maxElementsInMemory="25000"
eternal="true" timeToIdleSeconds="0" timeToLiveSeconds="0"
 overflowToDisk="false" />
```

The comment shows the approximate amount of Java heap memory required for the specific example. Some object references are shared by the caches, so the amount of memory used is not as high as the approximate value may suggest. It is best to err on the side of caution. Cache tracing can show which caches fill quickly for your specific server usage pattern.

`name`
: The `name` attribute is the name of the cache and generally indicates the type of objects being cached.

`maxElementsInMemory`
: The `maxElementsInMemory` controls the maximum size of the cache. This value can be changed to tune the size of the cache for your system. Ehcache caches are implemented using a linked-map system, which means that memory is only required for objects that are actually in memory. If you set the `maxElementsInMemory` to a high value, it will not automatically allocate that number of slots. Instead, they are added to the linked list as required. When `maxElementsInMemory` is reached, the cache discards the oldest objects before adding new objects.

`timeToIdleSeconds` - `timeToLiveSeconds`
: `timeToIdleSeconds` and `timeToLiveSeconds` control the automatic timeout of cached objects.

`overflowToDisk`
: `overflowToDisk` controls whether the cache should overflow to disk rather than discarding old objects.

A typical trace is as follows:

The criteria are:

- (`MissCount - CurrentCount`) must be as low as possible.
- (`HitCount/MissCount`) must be as high as possible.

`Estimated maximum size` affects the permanent memory taken up by the cache. If the caches grow too large, they may crowd out transient session memory and slow down the system. It is useful to have this running, on occasion, to identify the caches with a low `HitCount/MissCount` ratio.

Tracing the caches

This task describes how to trace the repository caches.

1. To output detailed Ehcache usage information, set the following logging category to `DEBUG`:

   ```
   org.alfresco.repo.cache.EhCacheTracerJob
   ```
2. To target specific caches, you can append the cache name or package, for example:

   ```
   org.alfresco.repo.cache.EhCacheTracerJob.org.alfresco
   ```
3. Open to the `<configRoot>\alfresco\scheduled-jobs-context.xml` file.
4. Locate the following bean:

   ```
   ehCacheTracerJob
   ```

   Override this bean to change the trigger schedule.
5. Uncomment the `scheduler` property to activate the trigger.

   When `ehCacheTracerJob` is triggered, the job will collect detailed cache usage statistics and output them to the `log/console`, depending on how logging has been configured for the server.
6. To ensure that caches use statistics, set the statistics property for all caches.

   ```
   statistics="true"
   ```

   Use the cluster cache sample file or copy the default cache configuration file into the `<extensions>` directory.

Adding a MIME type

This section describes how to add a MIME type definition.

There are two files that contain MIME type default definitions:

- `<configRoot>mimetype-map.xml`
- `<configRoot>mimetype-map-openoffice.xml`

Do not edit these files directly but should Instead, override the `mimetypeConfigService` bean in an extension file.

1. Open the `<extension>\mimetypes-extension.xml.sample` file.
2. Modify the inserted MIME type to match your requirements.
3. Save the file without the `.sample` extension.
4. Ensure you have created and added the new file to the `<extension>` directory so that you can point to your new file.
5. To point to your new file:
   a. Browse to the file: `mimetype-map-extension-context.xml.sample`

      This file contains the following line, which points to your modified file: `<value>classpath:alfresco/extension/mimetypes-extension.xml</value>`
   b. Save the file without the `.sample` extension.

Configuring metadata extraction

Metadata extraction automatically extracts metadata information from inbound and/or updated content and updates the corresponding nodes properties with the metadata values.

Metadata extractors offer server-side extraction of values from added or updated content. Definitions of the default set of extractors are in the `<configRoot>/alfresco/content-services-context.xml` file.

1. Declare a new extractor in `<extension>/custom-repository-context.xml`.

   The following example shows a new extractor written in `class com.company.MyExtracter`:

   ```
   <bean id="com.company.MyExtracter" class="com.company.MyExtracter"
   parent="baseMetadataExtracter" />
   ```

About versioning

Versioning allows you to track content history. By default, content that is created in the repository is not versionable. When creating content, users must specify *versionable* on a case-by-case basis.

When content is versionable, the version history is started. The first version of the content is the content that exists at the time of versioning. If you want all content to be versionable at the instant of creation, you can modify the definition of that content type in the data dictionary. The definition must include the mandatory aspect *versionable*.

By default, all versionable content has auto-version *on*. As a result, when content is updated, the version number is updated. The auto-version capability can be turned off on a content-by-content basis in the user interface. If you want auto-versioning to be *off* for all content, you can modify the definition of that content type in the data dictionary.

Making all content versionable

This section describes enabling versioning for all content in the repository.

1. Open the data dictionary `<configRoot>\alfresco\model\contentModel.xml`.
2. Search for the `<type>`: `<type name="cm:content">`
3. Immediately after the closing `</properties>` tag, insert the following lines:

   ```
   <type name="cm:content">
      <properties>
      ...
      </properties>
      <mandatory-aspects>
         <aspect>cm:versionable</aspect>
      </mandatory-aspects>
   </type>
   ```
4. Save the file.
5. Restart the Alfresco server.

Disabling the auto-versioning feature

This section describes disabling versioning for all content in the repository.

1. Open the data dictionary file: `<configRoot>\alfresco\model\contentModel.xml`
2. Search for the following `<aspect>`: `<aspect name="cm:versionable">`
3. Change the boolean default to `false`, as follows:

   ```
   <property name="cm:autoVersion">
      <title>Auto Version</title>
      <type>d:boolean</type>
      <default>false</default>
   </property>
   ```

4. Save the file.
5. Restart the Alfresco server.

Setting up database replication

Replication allows you to continuously copy a database to a different server.

To enable replication, you set one server (the slave) to take all its updates from the other server (the master). During replication, no *data* is actually copied. It is the SQL *statements* that manipulate the data that is copied.

All statements that change the master database are stored in the master's binary logs. The slave reads these logs and repeats the statements on its own database. The databases will not necessarily be exactly synchronized. Even with identical hardware, if the database is actually in use, the slave will always be behind the master. The amount by which the slave is behind the master depends on factors such as network bandwidth and geographic location. The other server can be on the same computer or on a different computer. The effect of replication is to allow you to have a nearly current standby server.

Using more than one server allows you to share the read load. You can use two slaves. If one of the three servers fails, you can use one server for service while another server can copy to the failed server. The slaves need not be running continuously. When they are restarted, they catch up. With one or more slaves you can stop the slave server to use a traditional backup method on its data files.

Each slave uses as much space as the master (unless you choose not to replicate some tables) and must do as much write work as the master does to keep up with the write rate. Do not be without at least one slave or comparable solution if high reliability matters to you.

Replication is not another form of back up. You must do normal backups as well as replication. If a user mistypes a `DELETE` statement on the master, the deletion is faithfully reproduced on the slave.

Setting up MySQL replication

This section describes the replication steps for the MySQL database.

1. Open a MySQL command prompt on the master server.
2. Grant the slave permission to replicate:

   ```
   GRANT REPLICATION SLAVE ON *.* TO <slave_user> IDENTIFIED BY
    '<slave_password>'
   ```
3. If the master is not using the `binary update` log, add the following lines to `my.cnf` (Linux) or `my.ini` (Windows) configuration file on the master, and restart the server:

   ```
   [mysqld]
   log-bin
   server-id=1
   ```

   By convention, server-id for the master is usually `server-id 1`, and any slaves from 2 onwards, although you can change this. If the master is already using the binary update log, either note the offset at the moment of the backup (the next step), or use the `RESET MASTER` statement to clear all binary logs and immediately begin the backup. You may want to make a copy of the binary logs before doing this if you need to use the binary logs to restore from backup.
4. Make a backup of the database.

   This will be used to start the slave server. You can skip this step if you use the `LOAD DATA FROM MASTER` statement, but first review the following comments about locking the master.

5. Add the following to the configuration file on the slave:

   ```
   master-host=master-hostname
   master-user=slave-user
   master-password=slave-password
   server-id=2
   ```

   The slave user and slave password are those to which you set when you granted `REPLICATION SLAVE` permission on the master. The `server-id` must be a unique number, different to the master or any other slaves in the system. There are also two other options: `master-port`, used if the master is running on a non-standard port (3306 is default), and `master-connect-retry`, a time in seconds for the slave to attempt to reconnect if the master goes down. The default is 60 seconds.

   Restore the data from the master, either as you would normally restore a backup or with the statement `LOAD DATA FROM MASTER`. The latter will lock the master for the duration of the operation, which could be quite lengthy, so you may not be able to spare the downtime.

Configuring the connection pool

This task describes how to override the connection pool.

1. Open the `<extension>\custom-connection-pool-context.xml.sample` file.

   You can also set the basic pool information in the `alfresco-global.properties` file.
2. Set the connection pool properties. For example:

   ```
   db.pool.initial=10
   db.pool.max=100
   ```
3. Remove the `.sample` extension from this file.
4. Modify the properties where appropriate, paying particular attention to the `validationQuery` property. This property is an SQL query that validates connections from this pool before returning them to the caller. This query must returns at least one row.

   For explanations of each property shown in the file, refer to: http://jakarta.apache.org/commons/dbcp/configuration.html

Customizing content transformations

This task describes how to customize content transformations.

1. Copy the following file:

   `<configRoot>/alfresco/content-services-context.xml`
2. Paste this file into the `<extension>` directory or in your preferred directory.
3. Open the file. Transformers start below the comment:

   ```
   <!-- Content Transformations -->
   ```
4. Locate the bean containing a transformer that is most similar to the transformer that you want to add. (It is unlikely that you would want to *modify* an existing transformer.)
5. Delete every pair of `<bean> </bean>` tags except the pair containing the similar transformer.
6. Rename and modify the bean.
7. Save the file with a meaningful name.

   If you save the file in the `<extension>` directory, the filename must end with `#context.xml`.

Setting up Alfresco authentication and security

The first time you access a vanilla Alfresco installation through Alfresco Explorer, Alfresco identifies you as a 'guest' user. You can identify yourself as another user by clicking the Login link and entering a new user name and password in the Login window. If you log in with the credentials of a user with administrator privileges (Alfresco uses `admin` as the default user name and password), you can use the Administration Console to create additional users and assign them passwords.

In this out-of-the-box set up, you can manage the user base and their passwords manually from within Alfresco, and unauthenticated users still have limited access as the 'guest' user.

From here, there are a number of common customizations you might want to make to scale up to the needs of a larger enterprise. For example, you might want to:

- Disable unauthenticated guest access
- Enable automatic sign-on using operating system credentials or a Single Sign-On (SSO) server to remove the need for a Login page
- Delegate authentication responsibility to a central directory server to remove the need to set up users manually in the Administration Console

Alfresco security

Alfresco security comprises a combination of authentication and authorization.

Authentication is about validating that a user or principal is who or what they claim to be. Alfresco normally refers to users. A user's credentials can take many forms and can be validated in a number ways. For example, a password validated against an LDAP directory, or a Kerberos ticket validated against a Microsoft Active Directory Server.

Alfresco includes:

- An internal, password-based, authentication implementation
- Support to integrate with many external authentication environments
- The option to write your own authentication integration and to use several of these options simultaneously

Alfresco can integrate with LDAP, Microsoft Active Directory Server, the Java Authentication and Authorization Service (JASS), Kerberos, and NTLM. A user ID can also be presented as an HTML attribute over HTTPS to integrate with web-based single-sign-on solutions.

Authorization determines what operations an authenticated user is allowed to perform. There are many authorization models. Popular ones include: Role Based Access Control (RBAC), UNIX-style Access Control Lists (ACLs) and extended ACLs, Windows-style ACLs, and many more. Authorization requirements for the management of records are more detailed and include additional requirements, for example, enforcing access based on security clearance or record state.

Alfresco authorization is based on UNIX-extended ACLs. Each node in the repository has an ACL that is used to assign permissions to users and groups. Operations, such as creating a new node, describe what permissions are required to carry out the operation. ACLs are then used to determine if a given user may execute the operation based on the permissions that have been assigned directly to the user or indirectly through a group. An operation in Alfresco is invoking a method on a public service bean. For example, creating a user's home folder requires invoking methods on several public services; to create the folder, set permissions, disable permission inheritance, and so on. Each public service method invocation will check that the user is allowed to execute the method.

By convention, public service beans are the beans whose names start with capital letters, such as the NodeService. You configure the security requirements for public service beans in XML. A given method on a particular service may be available to all users, all users in a specified group, all users with a specified role, or users who have particular permissions on specified arguments to the method or its return value. In addition, for methods that return collections or arrays, their content may be filtered based on user permissions. If the authorization requirements for a method call are not met, the method call will fail and it will throw an AccessDeniedException. Non-public beans, such as nodeService, do not enforce security; use these only when the enforcement of authorization is not required.

Permission assignments are made in *Access Control Lists* (ACLs), which are lists of *Access Control Entries* (ACEs). An ACE associates an authority (group or user) with a permission or set of permissions, and defines whether the permission is denied or allowed for the authority. Every node has a related ACL. When you create a node, it automatically inherits an ACL from its parent. You can alter this behavior after node creation by breaking inheritance or modifying the ACL.

The XML configuration for permissions also defines a context-free ACL for ACEs that apply to all nodes. For example, you could use this to assign everyone Read access to all nodes regardless of what individual ACLs any node has set. (See the Permissions section in this chapter for more details on how to modify the permission model.)

```
<!-- Extension to alfresco\model\permissionDefinitions.xml -->
<globalPermission permission="Read" authority="GROUP_EVERYONE" />
```

A check that a user has Read permission for a node is done in two stages. First, the context-free ACL is checked to see if it allows access. If not, the ACL assigned or inherited by the node is checked. A user may be allowed to perform an operation because of permissions assigned to the context-free ACL, assigned to the node's ACL, inherited by the node from its parent, or a combination of all three.

Authentication subsystems

Authentication is one of the categories of the Alfresco subsystem. An authentication subsystem is a coordinated stack of compatible components responsible for providing authentication and identity-related functionality to Alfresco.

Alfresco offers multiple implementations of the authentication subsystem, each engineered to work with one of the different types of back-end authentication server that you may have available in your enterprise.

An authentication subsystem provides the following functions to Alfresco:

- Password-based authentication for web browsing, Microsoft SharePoint protocol, FTP, and WebDAV
- CIFS and NFS file system authentication
- Web browser, Microsoft SharePoint protocol, and WebDAV Single Sign-On (SSO)
- User registry export (the automatic population of the Alfresco user and authority database)

The main benefits of the authentication subsystem are:

- Subsystems for all supported authentication types are pre-wired and there is no need to edit template configuration.
- There is no danger of compatibility issues between sub-components, as these have all been pre-selected. For example, your CIFS authenticator and authentication filter are guaranteed to be compatible with your authentication component.
- Common parameters are shared and specified in a single place. There is no need to specify the same parameters to different components in multiple configuration files.

- There is no need to edit the `web.xml` file. The `web.xml` file uses generic filters that call into the authentication subsystem. The `alfresco.war` file is a portable unit of deployment.
- You can swap from one type of authentication to another by activating a different authentication subsystem.
- Your authentication configuration will remain standard and, therefore, more manageable to support.
- Authentication subsystems are easily chained

Authentication subsystem types

A number of alternative authentication subsystem types exist for the most commonly used authentication protocols. These are each identified by a unique type name.

The following table shows the authentication subsystem types supplied with Alfresco and the optional features they support.

Type	Description	Single sign-on (SSO) support	CIFS authentication	User registry entry
`alfrescoNtlm`	Native Alfresco authentication	Yes, NTLM	Yes	No
`ldap`	Authentication and user registry export through the LDAP protocol (for example, OpenLDAP)	No	No	Yes
`ldap-ad`	Authentication and user registry export from Active Directoy through the LDAP protocol	No	No	Yes
`passthru`	Authentication through a Windows domain server	Yes, NTLM	Yes	No
`kerberos`	Authentication through a Kerberos realm	Yes, SPNEGO	Yes	No
`external`	Authentication using an external SSO mechanism	Yes	No	No

If you configure a single authentication subsystem of a type that does not support CIFS authentication (for example, LDAP), then the CIFS server will be automatically disabled. If you want CIFS and LDAP, then you must set up an authentication chain.

Authentication subsystem components

This section describes the main components of an authentication subsystem.

authentication component
Handles the specifics of talking to the back-end authentication system.

authentication Data Access Object (DAO)
Decides what user management functions are allowed, if any. For example, the ability to create a user.

authentication service
Wraps the authentication component and DAO with higher-level functions.

user registry export service (optional)
Allows Alfresco to obtain user attributes, such as email address, organization, and groups automatically.

authentication filters
Provide form or SSO-based login functions for the following:

- web client
- WebDAV
- Web scripts
- SharePoint Protocol

file server authenticators
Provide authentication functions for the following:

- CIFS protocol (optional)
- FTP protocol

Authentication chain

At least one of the authentication subsystem types will allow you to integrate Alfresco with the authentication servers in your environment. However, if integrating Alfresco with only one of these systems is not sufficient, you may want to combine multiple authentication protocols against a collection of servers.

For this reason, Alfresco has a built-in authentication chain. The authentication chain is a priority-ordered list of authentication subsystem instances. Alfresco composes together the functions of the subsystems in this list into a more powerful conglomerate.

Authentication chain functions

The functions of the chain are composed in two different ways: chained functions and pass-through functions.

Chained functions

Chained functions combine together functions of more than one subsystem.

For example, when a user logs in, Alfresco tries to match the user's credentials against each of the subsystems in the chain in order.

- If a chain member accepts the credentials, the login succeeds
- If no chain member accepts, the login fails

User registry export is also chained. During a synchronize operation, users and groups are exported from each member of the chain supporting user registry export (that is, those of type LDAP) and imported into Alfresco. Ordering in the chain is used to resolve conflicts between users and groups existing in the same directory.

Pass-through functions

Pass-through functions cannot be chained and instead pass through to a single member of the chain, which handles them directly.

Examples of pass-through functions are:

- NTLM / SPNEGO - based Single Sign-On (SSO)
- CIFS Authentication

Such pass-through functions are handled by the first member of the chain that supports that function and has it enabled.

This means that only a subset of your user base may be able to use SSO and CIFS.

Configuring authentication

A number of examples demonstrate how to express various authentication configuration requirements in subsystem instances in the authentication chain. They also explain how the authentication chain integrates the functions of multiple subsystem instances into a more powerful conglomerate, letting you cater for even the most complex authentication scenarios.

These examples demonstrate the flexibility and power of an Alfresco authentication chain. You can combine the strengths of a variety of different authentication protocols and keep the Alfresco user database synchronized almost transparently.

The authentication configuration examples adopt the following structured approach:

1. Decide the authentication chain composition (required subsystem types, instance names, order of precedence) and express this in the alfresco-global.properties file.
2. For each subsystem instance:
    a. Locate the properties files for its subsystem type. These properties files define the configurable properties for that subsystem type and their default values.
    b. Create a folder named after the subsystem instance under the Alfresco extension folders.
    c. Copy the properties files into your new folder.
    d. Edit the properties files to record the desired configuration of the subsystem instance.

Default authentication chain

The default product configuration has a simple chain with one member. This is an instance of the `alfrescoNtlm` subsystem type with and ID of `alfrescoNtlm1`.

This is expressed in the built-in defaults in the `repository.properties` file as:

```
authentication.chain=alfrescoNtlm1:alfrescoNtlm
```

You can configure the properties of `alfrescoNtlm1` using the global properties file.

This subsystem instance does not have SSO enabled, by default.

To switch from password-based login to NTLM-based SSO, set the following property in the `alfresco-global.properties` file.

```
ntlm.authentication.sso.enabled=true
```

This basic use of NTLM requires Alfresco to store its own copies of your MD4 password hash, which means your user ID and password must be the same in both Alfresco and your Windows domain.

For direct authentication with a Windows domain server, without the need to synchronize accounts in Alfresco and the domain, use the pass-through (`passthru`) subsystem type.

Configuring the authentication chain

This section describes how you can add to or completely replace the default authentication chain.

The chain is controlled by the `authentication.chain` global property.

1. Open the `alfresco-global.properties` file.
2. Locate the `authentication.chain` global property.

This is a comma separated list of the form:

```
instance_name1:type1,...,instance_namen:typen
```

3. Set the property to the required values.

   For example, set the property to the following value:

   ```
   alfrescoNtlm1:alfrescoNtlm,ldap1:ldap
   ```

   When you navigate to the `Alfresco:Type=Configuration,Category=Authentication,id1=manager` MBean in global property overrides, then a new authentication subsystem instance called `ldap1` will be brought into existence and added to the end of the authentication chain.
4. Save the file.

The following example integrates Alfresco with Active Directory has the requirements:

- Built-in Alfresco users and Windows users should be able to log in, with Alfresco taking precedence
- The Windows domain server should handle CIFS authentication directly
- LDAP should be used to synchronize user and group details

To achieve these requirements, configure the following authentication chain:

```
alfrescoNtlm1:alfrescoNtlm,passthru1:passthru,ldap1:ldap
```

Next, deactivate SSO in order to activate chained password-based login, target CIFS at `passthru1` and target synchronization (but not authentication) at `ldap1` by setting the properties as follows:

alfrescoNtlm1

```
ntlm.authentication.sso.enabled=false
alfresco.authentication.authenticateCIFS=false
```

passthru1

```
ntlm.authentication.sso.enabled=false
passthru.authentication.authenticateCIFS=true
```

ldap1

```
ldap.authentication.active=false
ldap.synchronization.active=true
```

Authentication chain example with JConsole

This section describes an example walk through of setting up an authentication chain using the JMX client, JConsole.

The first time you access a vanilla Alfresco installation through Alfresco Explorer, you see a Guest home page. The login is identified as the user guest and it is unauthenticated with limited access to the Alfresco functionality.

When you login as a user with administrator privileges, you can create additional users and assign passwords. By default, users and passwords are managed from within Alfresco. Unauthenticated users, like guest, still have limited access.

The default authentication within Alfresco is adequate for small-scale environments, however, you may prefer to choose an authentication method that will scale up to a production environment. For example, you may wish to:

- Disable the unauthenticated guest user access

- Enable automatic sign-on using operating system credentials or a single sign-on (SSO) server, which removes the need for a login page
- Delegate authentication responsibility to a central directory server, which removes the need to set up users manually the Alfresco Users tool.

Alfresco authentication chain

Alfresco authentication and identity management functionality is provided by a prioritized list, or chain, of configurable subsystems.

An authentication subsystem provides the following functionality to Alfresco:

- Password-based authentication for Web browsing, Sharepoint, FTP, and WebDAV
- CIFS and NFS file system authentication
- Web browser and Sharepoint Single Sign on (SSO)
- User register export (the automatic population of the Alfresco user and authority database)

Several alternative authentication subsystems exist for the most commonly used authentication protocols. These subsystems enable you to tie Alfresco to some of the most widely used authentication infrastructures. If you include more than one of these subsystems in the chain, you can create complex authentication scenarios.

Using the alfrescoNtlm subsystem with JConsole

By default, Alfresco is preconfigured with a single subsystem in its authentication chain. This section describes the authentication chain from within the JMX client, JConsole.

1. Open a command console.
2. Locate your JDK installation directory.

   For example, the JDK directory may be `java/bin`.
3. Enter the following command:

   ```
   jconsole
   ```

   The **JConsole New Connection** window displays.
4. Double-click on the Alfresco Java process.

   For Tomcat, this the Java process is usually labelled as **org.apache.catalina.startup.Bootstrap start**.

   JConsole connects to the managed bean (or MBean) server hosting the Alfresco subsystems.
5. Select the **MBeans** tab.

   The available managed beans display in JConsole.
6. Navigate to **Alfresco > Configuration > Authentication**.

   An object called `manager` (JMX object name is `Alfresco:Type=Configuration, Category=Authentication, id1=manager`) displays, which represents the chain.
7. Navigate to **Alfresco > Configuration > Authentication > managed**.

   View the authentication chain members within managed.
8. Navigate to **alfrescoNtlm1 > Attributes**.

   The configuration settings of the only member of the authentication chain, `alfrescoNtlm1`, display.

   The subsystem special `$type` attribute indicates that it is of type `alfrescoNtlm`, which is the subsystem type that deals with Alfresco authentication.

The subsystem name `alfrescoNtlm1` is the same as its type but with a number appended. This is a common convention used for subsystem naming but it does not need to be followed as a rule. The subsystem could just as easily have been called `InternalAlfresco` and have functioned exactly the same.

As implied by the type name, subsystems of type `alfrescoNtlm` are capable of automatic sign-on to internal Alfresco accounts using the NTLM protocol. However, NTLM need not be used at all and is disabled by default.

Disabling the Guest user login page

This section describes how to set the authentication configuration in JConsole to disable the unauthenticated Guest user login.

1. Run JConsole.
2. In the **Attributes** panel, select the **Value** column next to **alfresco.authentication.allowGuestLogin**.
3. Change the value to **false**.

   This authentication change will be remembered by Alfresco, even if you restart the server. When running Alfresco in a clustered configuration, this edit will be mirrored immediately across all nodes in the cluster.
4. Check that the new value for the property is persisted to the Alfresco database by checking the output from the shell running the Alfresco server, or `alfresco.log` in the directory where Alfresco was started from. You see the lines:

```
17:30:03,033 User:System INFO
 [management.subsystems.ChildApplicationContextFactory] Stopping
'Authentication' subsystem, ID: [Authentication, managed, alfrescoNtlm1]
17:30:03,064 User:System INFO
 [management.subsystems.ChildApplicationContextFactory] Stopped
'Authentication' subsystem, ID: [Authentication, managed, alfrescoNtlm1]
```

   The subsystem is not started automatically after the edit, because, in a more complex scenario, you might want to reconfigure a number of attributes before trying them out on the live server. Only once the subsystem starts up again and reads its properties will the new settings take effect.
5. Log out from Alfresco Explorer in the browser.

   After logging out, immediately the log in screen appears and whenever you access Alfresco, you are always directed to the login page, not the guest access.

Removing the login page

This section describes how to set the authentication in JConsole not to display the login page.

1. Login to Alfresco Explorer using the Administration user.
2. Click **Admin Console**.
3. Create a users whose user name and password matches those of your operating system account.
4. Run JConsole.
5. Navigate to **Alfresco > Configuration > Authentication > managed > alfrescoNtlm1 > Attributes**.
6. In the **Attributes** panel, select the **Value** column next to **ntlm.authentication.sso.enabled** attribute.
7. Change the value to **true**.
8. Navigate to **Alfresco > Configuration > Authentication > managed > alfrescoNtlm1 > Operations**.

9. Click the **Start** operation.
10. Close and restart your browser and try accessing Alfresco.

    If your browser supports NTLM and its security settings allow, it will automatically log you in using your operating system account name.

Authentication using a central directory server

This section describes how to delegate authentication responsibility to a centralized directory server. Most organizations maintain their user database in a directory server supporting the LDAP protocol, such as Active Directory or OpenLDAP. When integrated with an LDAP server, Alfresco can delegate both the password checking and account setup to the LDAP server. This exposes Alfresco to your entire enterprise, and avoids the need for an administrator to manually set up user accounts, and the need to store passwords outside of the directory server.

To integrate Alfresco with a directory server, include the `ldap` or `ldap-ad` subsystem in the authentication chain. Both subsystems offer exactly the same capabilities and should work with virtually any directory server supporting the LDAP protocol. The only difference is the default values configured for their attributes: ldap is preconfigured with defaults appropriate for OpenLDAP; ldap-ad is preconfigured with defaults appropriate for Active Directory.

This example uses an Active Directory server and therefore configures in an instance of the `ldap-ad` subsystem. Insert an ldap-ad instance into the Alfresco authentication chain. There are two choices:

- Replace the authentication chain

  Remove `alfrescoNtlm1` and add an instance of `ldap-ad`. This hands over all authentication responsibility to Active Directory and means that the default accounts such as “admin” and “guest” can not be used. It is important to configure at least one user who exists in Active Directory as an administrator and enable the guest account in Active Directory, if guest access is required. As `ldap-ad` is not capable of supporting CIFS authentication (due to it requiring exchange of an MD5 password hash), it rules out use of the CIFS server for all users and the CIFS server would be disabled.
- Add to the authentication chain

  Supplement the existing capabilities of `alfrescoNtlm1` by inserting an `ldap-ad` instance before or after `alfrescoNtlm1` in the chain. This means that the default accounts can be used alongside those accounts in the directory server. The default accounts can also access Alfresco through the CIFS server, as `alfrescoNtlm` is able to drive CIFS authentication. The position of the `ldap-ad` instance in the chain will determine how overlaps or collisions between user accounts are resolved. If an “admin” account exists in both Alfresco and Active Directory, then the order for defining for who admin is would be Alfresco, if `alfrescoNtlm1` came first, or Active Directory, if the `ldap-ad` instance came first.

1. Open JConsole.
2. Navigate to **Alfresco > Configuration > Authentication > manager > Attributes**.
3. Edit the chain attribute so that its value is:

   ```
   alfrescoNtlm1:alfrescoNtlm,ldap1:ldap-ad
   ```

Configuring alfrescoNtlm

`alfrescoNtlm` is the subsystem configured by default in the Alfresco authentication chain. It performs authentication based on user and password information stored in the Alfresco repository. It is capable of supporting both form-based login and NTLM-based Single Sign-On (SSO), as well as providing authentication for the CIFS server.

The NTLM SSO functions are disabled by default, which means there are no assumptions about the availability of a Windows domain. You can activate SSO with a single property, without any changes to the `web.xml` file or further file server configuration.

NTLM

The alfrescoNtlm subsystem supports optional NTLM Single Sign-On (SSO) functions for WebDAV and the Alfresco Explorer client.

NTLM v2 is supported, which is more secure that the NTLM v1. If the client does not support NTLMv2, it will automatically downgrade to NTLMv1.

By using NTLM authentication to access Alfresco Explorer and Alfresco WebDAV sites, the web browser can automatically log in.

When SSO is enabled, Internet Explorer will use your Windows log in credentials when requested by the web server. Firefox and Mozilla also support the use of NTLM but you need to add the URI to the Alfresco site that you want to access to `network.automatic-ntlm-auth.trusted-uris` option (available through writing `about:config` in the URL field) to allow the browser to use your current credentials for login purposes.

The Opera web browser does not currently support NTLM authentication, the browser is detected and will be sent to the usual Alfresco logon page.

In this configuration, Alfresco must still store its own copy of your MD4 password hash. In order to remove this need and authenticate directly with a Windows domain controller, consider using the pass-through subsystem.

alfrescoNtlm configuration properties

The alfrescoNtlm subsystem supports the following properties.

ntlm.authentication.sso.enabled
A Boolean that when true enables NTLM based Single Sign On (SSO) functionality in the Web clients. When false and no other members of the authentication chain support SSO, password-based login will be used.

ntlm.authentication.mapUnknownUserToGuest
Specifies whether unknown users are automatically logged on as the Alfresco guest user during Single Sign-On (SSO).

alfresco.authentication.authenticateCIFS
A Boolean that when true enables Alfresco-internal authentication for the CIFS server. When false and no other members of the authentication chain support CIFS authentication, the CIFS server will be disabled.

alfresco.authentication.allowGuestLogin
Specifies whether to allow guest access to Alfresco.

If you add extra administrator users in the `authority-services-context.xml` file and are using alfrescoNtlm, the extra users (other than the admin user) will no longer have administrator rights until you add them to the `ALFRESCO_ADMINISTRATORS` group using the Administration Console.

Configuring Alfresco Share SSO to use NTLM

This section describes how to configure use NTLM with Alfresco Share SSO.

Alfresco Share exists as a separate web application to the main Alfresco repository/Explorer WAR file. It can run in the same application server instance on the same machine as the main web application, or it can run on a completely separate application server instance on a different machine. Share uses HTTP(S) to communicate with the configured Alfresco repository.

1. Locate the following `.sample` configuration override file:

`<web-extension>\share-config-custom.xml.sample`

Copy and rename the file to:

`<web-extension>\share-config-custom.xml`

2. Edit the file, and then uncomment the following section:

```
 <!--
        SSO authentication config for Share
        NOTE: change localhost:8080 below to appropriate alfresco server
 location if required
   -->
   <config evaluator="string-compare" condition="Remote">
      <remote>
         <connector>
            <id>alfrescoCookie</id>
            <name>Alfresco Connector</name>
            <description>Connects to an Alfresco instance using cookie-
based authentication</description>

 <class>org.springframework.extensions.webscripts.connector.AlfrescoConnector</
class>
         </connector>

         <endpoint>
            <id>alfresco</id>
            <name>Alfresco - user access</name>
            <description>Access to Alfresco Repository WebScripts that
 require user authentication</description>
            <connector-id>alfrescoCookie</connector-id>
            <endpoint-url>http://localhost:8080/alfresco/wcs</endpoint-
url>
            <identity>user</identity>
            <external-auth>true</external-auth>
         </endpoint>
      </remote>
   </config>
```

3. Change the `<endpoint-url>http://localhost:8080/alfresco/wcs</endpoint-url>` value to point to your Alfresco server location.
4. Set the `maxThreads` option in the `<TOMCAT_HOME>/conf/server.xml` file.

```
<Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443"
               maxThreads="200"
 />
```

If Share and Alfresco are installed on the same Tomcat, it is important to set the `maxThreads` option to 2*(expected number of concurrent requests). This is because each Share request spawns an Alfresco request.

5. Restart Share.

If you have configured alfrescoNtlm or `passthru` in your Alfresco authentication chain and enabled SSO, NTLM will be the active authentication mechanism.

Share SSO login bypass

When configuring Share authentication as NTLM SSO, you can bypass the SSO authentication so that it is possible to login as a different user than the one used in the Windows version.

1. Enable NTLM SSO.
2. Add external authentication to the chain using the following property:

```
external.authentication.proxyUserName=
```

This property is needed for respecting X-Alfresco-Remote-User header.

3. To login with another user to Share, use: http://localhost:8080/share/page?f=default&pt=login.
4. To logout from Share back to the NTLM, use: http://localhost:8080/share/logout.

Configuring pass-through

The pass-through (`passthru`) subsystem can be used to replace the standard Alfresco user database with a Windows server/domain controller, or list of servers, to authenticate users accessing Alfresco. This saves having to create user accounts within Alfresco.

The subsystem also supports optional NTLM Single Sign-On (SSO) functions for WebDav and the Alfresco Explorer and Share clients and direct CIFS authentication for the CIFS server. This method of authentication is much more secure than simple LDAP-based authentication or form-based authentication.

Only NTLM v1 is supported in this configuration. As NTLMv2 has been designed to avoid "man-in-the-middle" attacks, it would be impossible to use in this pass through style.

Pass-through configuration properties

The `passthru` subsystem supports domain level properties.

Also relevant are the configuration steps described in Alfresco Share SSO using NTLM if you want to enable NTLM-based Single Sign-On (SSO) for the Alfresco Share client.

Domain level properties

The following properties control the set of domain controllers used for authentication. The three properties are mutually exclusive. For example, to set the `passthru.authentication.servers` property, set `passthru.authentication.domain` to be empty and `passthru.authentication.useLocalServer` to be false.

passthru.authentication.useLocalServer
A Boolean that when true indicates that the local server should be used for pass through authentication by using loopback connections into the server.

passthru.authentication.domain
Sets the domain to use for pass through authentication. This will attempt to find the domain controllers using a network broadcast. Make sure that you use the Windows NetBIOS domain name, not the forest name. The network broadcast does not work in all network configurations. In this case use the `passthru.authentication.servers` property to specify the domain controller list by name or address.

passthru.authentication.servers
A comma delimited list of server names or addresses that are used for authentication. The pass through authenticator will load balance amongst the available servers, and can monitor server online/offline status.

- Each server name/address may be prefixed with a domain name using the format `<domain>\<server>`. If specifying this in `alfresco-global.properties`, remember that the backslash character must be escaped. For example

```
passthru.authentication.servers=DOMAIN1\\host1.com,DOMAIN2\
\host2.com,host1.com
```
- If the client specifies a domain name in its login request, then the appropriate server will be used for the authentication. Domain mappings may also be specified to route authentication requests to the appropriate server.
- If a server handles authentication for multiple domains then multiple entries can be added in the server list prefixed with each domain name.
- There must be at least one entry in the server list that does not have a domain prefix. This is the catch all entry that will be used if the client domain cannot be determined from the NTLM request or using domain mapping.

Other pass-through properties

The pass-through subsystem supports the following additional properties.

ntlm.authentication.sso.enabled
A Boolean that when true enables NTLM based Single Sign On (SSO) functionality in the Web clients. When false and no other members of the authentication chain support SSO, password-based login will be used.

ntlm.authentication.mapUnknownUserToGuest
Identifies whether unknown users are automatically logged on as the Alfresco guest user during Single Sign-On (SSO).

passthru.authentication.authenticateCIFS
A Boolean that when true enables pass-through authentication for the CIFS server. When false and no other members of the authentication chain support CIFS authentication, the CIFS server will be disabled.

passthru.authentication.authenticateFTP
A Boolean that when true enables pass-through authentication for the FTP server. The provided password is hashed and checked directly against the domain server securely using NTLM. When false and no other members of the authentication chain support FTP authentication, standard chained authentication will be used.

passthru.authentication.guestAccess
Identifies whether to allow guest access to Alfresco if the authenticating server indicates the login was allowed guest access.

passthru.authentication.defaultAdministratorUserNames
A comma separated list of user names who should be considered administrators by default. It is often useful to add the administrator user to this list.

passthru.authentication.connectTimeout
The timeout value when opening a session to an authentication server, in milliseconds. The default is 5000.

passthru.authentication.offlineCheckInterval
Specifies how often pass through servers that are marked as offline are checked to see if they are now online. The default check interval is 5 minutes. The check interval is specified in seconds.

passthru.authentication.protocolOrder
Specifies the type of protocols and the order of connection for pass through authentication sessions. The default is to use NetBIOS, if that fails then try to connect using native SMB/ port 445. Specify either a single protocol type or a comma delimited list with a primary and secondary protocol type. The available protocol types are NetBIOS for NetBIOS over TCP and TCPIP for native SMB.

Domain mappings

Domain mappings are used to determine the domain a client is a member of when the client does not specify its domain in the login request. If the client uses a numeric IP address to access the web server it will not send the domain in the NTLM request as the browser assumes it is an Internet address.

To specify the domain mapping rules that are used when the client does not supply its domain in the NTLM request you can use the `filesystem.domainMappings` composite property of the file server subsystem. Specify the file server subsystem settings in the `alfresco-global.properties` file.

There are two ways of defining a domain mapping, either by specifying an IP subnet and mask, or by specifying a range of IP addresses. The following example defines mappings for two domains: `ALFRESCO` and `OTHERDOM`.

```
filesystem.domainMappings=ALFRESCO,OTHERDOM
filesystem.domainMappings.value.ALFRESCO.subnet=192.168.1.0
filesystem.domainMappings.value.ALFRESCO.mask=192.168.1.0
filesystem.domainMappings.value.OTHERDOM.rangeFrom=192.168.1.0
filesystem.domainMappings.value.OTHERDOM.rangeTo=192.168.1.100
```

The mask value masks the IP address to get the subnet part, and in this example, the mask value is 192.168.1.0. An alternative is to use 255.255.255.0. A value of 255.255.255.0 will get the subnet, which is then checked against the subnet value. If there were two subnets, 192.168.1.0 and 192.168.2.0, then a mask value of 255.255.255.0 and subnet value of 192.168.1.0 would only match addresses in the 192.168.1.0 range.

The pass through subsystem can use the domain prefixed server name format of the `passthru.authentication.servers` property along with the domain mappings to route authentication requests to the appropriate server. A sample NTLM authentication component server list:

```
passthru.authentication.servers=ALFRESCO\\ADSERVER,OTHERDOM\\OTHERSRV
```

Example: customizing the pass-through subsystem

The authentication capabilities offered by the ldap-ad subsystem type cannot support CIFS and NTLM authentication. Instead, you would have to use form-based login for all users, and only Alfresco internal users could access CIFS. This is the compromise you would have to make if the directory server did not support any other authentication protocol. But for Active Directory, which also supports NTLM and Kerberos authentication, you can overcome this limitation by using either the Pass-through or the Kerberos subsystem types.

The Pass-through subsystem supports SSO, CIFS, and password authentication against a Windows domain server using the NTLM v1 protocol. Many prefer Kerberos for its enhanced security and you could consider it as an alternative.

1. Append an instance of passthru to the authentication chain.
2. Name the instance passthru1, and declare it by changing the authentication.chain property in alfresco-global.properties as follows:

   ```
   alfresco.authentication.authenticateCIFS=false
   ```

Functions such as NTLM SSO and CIFS authentication can only be targeted at a single subsystem instance in the authentication chain. This is a restriction imposed by the authentication protocols themselves. For this reason, Alfresco targets these ‘direct’ authentication functions at the first member of the authentication chain that has them enabled. By disabling CIFS in alfinst earlier, passthru1 has a chance to handle CIFS authentication for its larger user base. SSO is also left disabled in alfinst, which means that you can enable it in passthru1.

3. Stop ldap1 from performing authentication.

   You can leave that to passthru1, which will be authenticating against the same server using more secure protocols. This leaves the ldap1 user registry export capabilities still active, which you still rely on for account synchronization.

4. Edit the ldap.authentication.active property in the ldap-ad-authentication.properties file located in your ldap1 directory as follows:

   ldap.authentication.active=false

5. Create the properties files to configure passthru1.

```
mkdir <installLocation>\tomcat\shared\classes\alfresco\extension
\subsystems\
Authentication\passthru\passthru1

cd /d <installLocation>\tomcat\shared\classes\alfresco\extension
\subsystems\
Authentication\passthru\passthru1

copy <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco
\subsystems\
Authentication\passthru\*.properties
```

After running the previous commands, two separate properties files should appear in your passthru1 directory. These are:

- passthru-authentication-context.properties
- ntlm-filter.properties

Using a similar distinction to the alfrescoNtlm subsystem type, passthru-authentication-context.properties contains properties relating to core authentication capabilities, whereas ntlm-filter.properties groups those properties relating to automatic sign on. Unlike the alfrescoNtlm subsystem type, SSO is enabled by default in passthru subsystems so there is no need to edit ntlm-filter.properties.

The following lines show the set of properties you typically need to edit and how they might be set for a domain controller for the fictitious domain domain.com.

```
passthru.authentication.servers=DOMAIN\\domaincontroller.domain.com\
,domaincontroller.com
passthru.authentication.domain=# Leave blank
passthru.authentication.guestAccess=false
passthru.authentication.defaultAdministratorUserNames=Administrator,alfresco
```

The following list is a summary of the settings that have been changed:

- passthru.authentication.servers — A comma-separated list of domain controller host names, each prefixed by the name of the domain they correspond to and a double backslash. The last member of the list is a host name without a domain prefix, and this host will be used when a client does not include a domain name in an authentication request.
- passthru.authentication.domain — A property that is a less-reliable alternative to passthru.authentication.servers and should be left empty

- passthru.authentication.defaultAdministratorUserNames — A list of user IDs who should be given Alfresco administrator privileges by default. Additional users can be made administrators by another administrator if they add those users to the ALFRESCO_ADMINISTRATORS group.

Applying the Pass-through example

Restart the Alfresco server.

The main differences to notice are:

- All Active Directory users can point their browser to the Alfresco server and be signed on automatically. (In Internet Explorer, this requires adding the Alfresco server to the Local Intranet security zone.)
- All Active Directory users can access Alfresco as a CIFS file system using their Active Directory credentials.

Configuring LDAP

An LDAP subsystem supports two main functions:

- user authentication - checking a user's ID and password using an LDAP bind operation
- user registry export - exposing information about users and groups to the synchronization subsystem

Either of these functions can be used in isolation or in combination. When LDAP authentication is used without user registry export, default Alfresco person objects are created automatically for all those users who successfully log in. However, they will not be populated with attributes without user registry export enabled. LDAP user registry export is most likely to be used without LDAP authentication when chained with other authentication subsystems. For example, Kerberos against Active Directory, pass-through against ActiveDirectory, and possibly Samba on top of OpenLDAP.

The user registry export function assumes that groups are stored in LDAP as an object that has a repeating attribute, which defines the distinguished names of other groups, or users. This is supported in the standard LDAP schema using the `groupOfNames` type. See the example LDIF file in OpenLDAP tips on page 283.

LDAP configuration properties

Both the `ldap` and `ldap-ad` subsystem types support the following configurable properties.

The defaults for `ldap` are typical for Open LDAP, and the defaults for `ldap-ad` are typical for Active Directory.

ldap.authentication.active
This Boolean flag, when true enables use of this LDAP subsystem for authentication. It may be that this subsystem should only be used for user registry export, in which case this flag should be set to false and you would have to chain an additional subsystem such as passthru or kerberos to provide authentication functions.

ldap.authentication.java.naming.security.authentication

The mechanism to use to authenticate with the LDAP server. Should be one of the standard values documented here or one of the values supported by the LDAP provider. Sun's LDAP provider supports the SASL mechanisms documented here. Recommended values are:

simple

the basic LDAP authentication mechanism requiring the user name and password to be passed over the wire unencrypted. You may be able to add SSL for secure access, otherwise this should only be used for testing.

DIGEST-MD5

More secure RFC 2831 Digest Authentication. Note that with Active Directory, this requires your user accounts to be set up with reversible encryption, not the default setting.

ldap.authentication.userNameFormat

Specifies how to map the user identifier entered by the user to that passed through to LDAP.

If set to an empty string (the default for the ldap subsystem), an LDAP query involving `ldap.synchronization.personQuery` and `ldap.synchronization.userIdAttributeName` will be performed to resolve the DN from the user ID dynamically. This allows directories to be structured and does not require the user ID to appear in the DN.

If set to a non-empty value, the substring %s in this value will be replaced with the entered user ID to produce the ID passed to LDAP. This restricts LDAP user names to a fixed format. The recommended format of this value depends on your LDAP server.

Active Directory

There are two alternatives:

User Principal Name (UPN)

These are generally in the format of `<sAMAccountName>@<UPN Suffix>`. If you are unsure of the correct suffix to use, use an LDAP browser, such as Softerra, to browse to a user account and find its `userPrincipalName` attribute. For example:

```
%s@domain
```

DN

This requires the user to authenticate with part of their DN, so may require use of their common name (CN) rather than their login ID. It also may not work with structured directory layouts containing multiple organization units (OUs). For example:

```
cn=%s,ou=xyz,dc=domain
```

OpenLDAP

The format used depends on the value chosen for `ldap.authentication.java.naming.security.authentication`.

simple

This must be a DN and would be something like the following:

```
uid=%s,ou=People,dc=company,dc=com
```

DIGEST-MD5

Use this value to pass through the entered value as-is:

```
%s
```

When authenticating against LDAP, users are not always in the same subtree of LDAP. In this situation, it is necessary to support authentication against multiple branches of LDAP. For example, some users who can authenticate using `cn=%s,ou=myCity,ou=myState,o=myCompany` but others can authenticate using `cn=%s,ou=ANOTHERCity,ou=myState,o=myCompany`. Set `ldap.authentication.userNameFormat` to be empty (the default), and then it will derive a query from your personQuery to look up a user by UID. This ensures that you can support users in any branch structure.

ldap.authentication.allowGuestLogin
Identifies whether to allow unauthenticated users to log in to Alfresco as the 'guest' user.

ldap.authentication.java.naming.factory.initial
The LDAP context factory to use. There is no need to change this unless you do not want to use the default Sun LDAP context factory.

ldap.authentication.java.naming.provider.url
The URL to connect to the LDAP server, containing its name and port. The standard ports for LDAP are 389 (and 636 for SSL). For example: `ldap://openldap.domain.com:389`

ldap.authentication.escapeCommasInBind
Escape commas in the entered user ID when authenticating with the LDAP server? Useful when using simple authentication and the CN is part of the DN and contains commas.

ldap.authentication.escapeCommasInUid
Escape commas in the entered user ID when deriving an Alfresco internal user ID? Useful when using simple authentication and the CN is part of the DN and contains commas, and the escaped \, is pulled in as part of a synchronize operation. If this option is set to true it will break the default home folder provider as space names cannot contain \.

ldap.authentication.defaultAdministratorUserNames
A comma separated list of user names who should be considered administrators by default.

ldap.synchronization.active
This flag enables use of the LDAP subsystem for user registry export functions and decides whether the subsystem will contribute data to the synchronization subsystem. It may be that this subsystem should only be used for authentication, in which case this flag should be set to false.

ldap.synchronization.java.naming.security.principal
The LDAP user to connect as to do the export operation. Should be in the same format as `ldap.authentication.userNameFormat` but with a real user ID instead of `%s`.

ldap.synchronization.java.naming.security.credentials
The password for this user, if required.

ldap.synchronization.queryBatchSize
If set to a positive integer, this property indicates that RFC 2696 paged results should be used to split query results into batches of the specified size. This overcomes any size limits imposed by the LDAP server. The default value of 1000 matches the default result limitation imposed by Active Directory. If set to zero or less, paged results will not be used.

ldap.synchronization.groupQuery
The query to select all objects that represent the groups to export. This query is used in full synchronization mode, which by default is scheduled every 24 hours.

ldap.synchronization.groupDifferentialQuery
The query to select objects that represent the groups to export that have changed since a certain time. Should use the placeholder `{0}` in place of a timestamp in the format specified by `ldap.synchronization.timestampFormat`. The timestamp substituted will be the maximum value of the attribute named by `ldap.synchronization.modifyTimestampAttributeName` the last time groups were queried. This query is used in differential synchronization mode, which by default is triggered whenever a user is successfully authenticated that does not yet exist in Alfresco.

ldap.synchronization.personQuery
The query to select all objects that represent the users to export. This query is used in full synchronization mode, which by default is scheduled every 24 hours.

ldap.synchronization.personDifferentialQuery
The query to select objects that represent the users to export that have changed since a certain time. Should use the placeholder `{0}` in place of a timestamp in the format specified by `ldap.synchronization.timestampFormat`. The timestamp substituted will be the maximum value of the attribute named by `ldap.synchronization.modifyTimestampAttributeName` the last time users were queried. This query is used in differential synchronization mode, which by default is triggered whenever a user is successfully authenticated that does not yet exist in Alfresco.

ldap.synchronization.groupSearchBase
The DN below which to run the group queries.

ldap.synchronization.userSearchBase
The DN below which to run the user queries.

ldap.synchronization.modifyTimestampAttributeName
The name of the operational attribute recording the last update time for a group or user.

ldap.synchronization.timestampFormat
The timestamp format. This varies between directory servers.

Active Directory
`yyyyMMddHHmmss'.0Z'`

OpenLDAP
`yyyyMMddHHmmss'Z'`

ldap.synchronization.userIdAttributeName
The attribute name on people objects found in LDAP to use as the uid in Alfresco.

ldap.synchronization.userFirstNameAttributeName
The attribute on person objects in LDAP to map to the first name property in Alfresco.

ldap.synchronization.userLastNameAttributeName
The attribute on person objects in LDAP to map to the last name property in Alfresco.

ldap.synchronization.userEmailAttributeName
The attribute on person objects in LDAP to map to the email property in Alfresco.

ldap.synchronization.userOrganizationalIdAttributeName
The attribute on person objects in LDAP to map to the email property in Alfresco.

ldap.synchronization.defaultHomeFolderProvider
The default home folder provider to use for people created using LDAP import.

ldap.synchronization.groupIdAttributeName
The attribute on LDAP group objects to map to the group name in Alfresco.

ldap.synchronization.groupType
The group type in LDAP.

ldap.synchronization.personType
The person type in LDAP

ldap.synchronization.groupMemberAttributeName
The attribute in LDAP on group objects that defines the DN for its members.

Checking the supported SASL authentication mechanisms

This section describes how to check for which Simple Authentication and Security Layer (SASL) authentication mechanisms are supported.

1. Using an LDAP browser, such as the one from Softerra, check the values of the `supportedSASLMechanisms` attributes on the root node of your LDAP server.

The simple authentication method will not be reported because it is not a SASL mechanism.

2. If you use OpenLDAP, you can also query using `ldapsearch`. For example:

```
ldapsearch -h localhost -p 389 -x -b "" -s base -LLL
 supportedSASLMechanisms
dn:
supportedSASLMechanisms: DIGEST-MD5
supportedSASLMechanisms: NTLM
supportedSASLMechanisms: CRAM-MD5
```

Example: customizing an ldap-ad subsystem

This example addresses the more advanced goal of delegating authentication responsibility to a centralized directory server. Most organizations maintain their user database in a directory server supporting the LDAP protocol, such as Active Directory or OpenLDAP.

When integrated with an LDAP server, Alfresco can delegate both the password checking and account setup to the LDAP server, thus opening up Alfresco to your entire enterprise. This avoids the need for an administrator to manually set up user accounts or to store passwords outside of the directory server.

To integrate Alfresco with a directory server, you simply need to include an instance of the ldap or ldap-ad subsystem types in the authentication chain. Both subsystem types offer exactly the same capabilities and should work with virtually any directory server supporting the LDAP protocol. Their only differences are the default values configured for their attributes. The ldap type is preconfigured with defaults appropriate for OpenLDAP, whereas ldap-ad is preconfigured with defaults appropriate for Active Directory.

There are two choices in this scenario: replace or add to the authentication chain.

- Replace the authentication chain

  You could remove `alfinst` from the previous example and instead add an instance of `ldap-ad`. This would hand over all authentication responsibility to Active Directory and would mean that the built-in accounts, such as admin and guest, could not be used.

  In this scenario, it would be important to configure at least one user who exists in Active Directory as an administrator and enable the guest account in Active Directory, if guest access were required. Furthermore, because ldap-ad cannot support CIFS authentication (as it requires an MD5 password hash exchange), it would rule out use of the CIFS server for all users and the CIFS server would be disabled.
- Add to the authentication chain

  You could instead supplement the existing capabilities of `alfinst` by inserting an `ldap-ad` instance before or after `alfinst` in the chain. This means that you could use the built-in accounts alongside those accounts in the directory server. Furthermore, the built-in accounts could access Alfresco through the CIFS server, since alfrescoNtlm is able to drive CIFS authentication.

  In this scenario, where you chose to position your ldap-ad instance in the chain determines how overlaps or collisions between user accounts are resolved. If an admin account existed in both Alfresco and Active Directory, then admin would be Alfresco if `alfinst` came first, or Active Directory if the ldap-ad instance came first.

This example uses an Active Directory server and configures an instance of the ldap-ad subsystem.

1. This example uses the second option to append an instance of ldap-ad to the authentication chain. This instance name is ldap1 and is declared by changing the authentication.chain property in alfresco-global.properties as follows:

```
authentication.chain=alfinst:alfrescoNtlm,ldap1:ldap-ad
```

2. Undo any previous modifications to alfinst and disable NTLM-based SSO.

   This is done because the ldap-ad and ldap subsystem types cannot participate in the NTLM handshake, so leaving SSO enabled would prevent any of the Active Directory users from logging in.
3. Disable SSO by opening the file ntlm-filter.properties in the alfinst directory in a text editor and editing the property ntlm.authentication.sso.enabled as follows:

   ```
   ntlm.authentication.sso.enabled=false
   ```
4. Create the properties files to configure ldap1:

   ```
   mkdir <installLocation>\tomcat\shared\classes\alfresco\extension
   \subsystems\
   Authentication\ldap-ad\ldap1

   cd /d <installLocation>\tomcat\shared\classes\alfresco\extension
   \subsystems\
   Authentication\ldap-ad\ldap1

   copy <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco
   \subsystems\
   Authentication\ldap-ad\*.properties
   ```

   A single file called ldap-ad-authentication.properties now appears in your ldap1 directory. You can edit this file to define your LDAP set up.

When you open ldap-ad-authentication.properties, the large number of configurable properties may alarm you. This demonstrates the flexibility of Alfresco's LDAP infrastructure. Luckily, because ldap-ad already has sensible defaults configured for a typical Active Directory set up, there are only a few edits you must make to tailor the subsystem instance to your needs.

The following lines show the set of properties you will typically need to edit and how you might set them for a domain controller for a fictitious domain called `domain.com`.

```
ldap.authentication.allowGuestLogin=false
ldap.authentication.userNameFormat=%s@domain.com
ldap.authentication.java.naming.provider.url=ldap://
domaincontroller.domain.com:389
ldap.authentication.defaultAdministratorUserNames=Administrator,alfresco
ldap.synchronization.java.naming.security.principal=alfresco@domain.com
ldap.synchronization.java.naming.security.credentials=secret
ldap.synchronization.groupSearchBase=ou=Security Groups,ou=Alfresco\
,dc=domain,dc=com

ldap.synchronization.userSearchBase=ou=User
 Accounts,ou=Alfresco,dc=domain,dc=com
```

The following list is a summary of the settings that have been changed:

- `ldap.authentication.allowGuestLogin` — Enables / disables unauthenticated access to Alfresco
- `ldap.authentication.userNameFormat` — A template that defines how Alfresco user IDs are expanded into Active Directory User Principal Names (UPNs) containing a placeholder `%s`, which stands for the unexpanded user ID. A UPN generally consists of the user's account ID followed by an `@` sign and then the domain's UPN suffix. You can check the appropriate UPN suffix for your domain by connecting to the directory with an LDAP browser, browsing to a user account, and looking at the value of the `userPrincipalName` attribute.
- `ldap.authentication.java.naming.provider.url` — An LDAP URL containing the host name and LDAP port number (usually 389) of your Active Directory server

- `ldap.authentication.defaultAdministratorUserNames` — A list of user IDs who should be given Alfresco administrator privileges by default. Another administrator can include more users as administrators by adding those users to the ALFRESCO_ADMINISTRATORS group.
- `ldap.synchronization.java.naming.security.principal` — The UPN for an account with privileges to see all users and groups. This account is used by Alfresco to retrieve the details of all users and groups in the directory so that it can synchronize its internal user and authority database. Passwords are never compromised and remain in the directory server.
- `ldap.synchronization.java.naming.security.credentials` — The password for the previous account
- `ldap.synchronization.groupSearchBase` — The Distinguished Name (DN) of the Organizational Unit (OU) below which security groups can be found. You can determine the appropriate DN by browsing to security groups in an LDAP browser.
- `ldap.synchronization.userSearchBase` — The distinguished name (DN) of the Organizational Unit (OU) below which user accounts can be found. You can determine the appropriate DN by browsing to user accounts in an LDAP browser.

Applying the ldap-ad example

This example demonstrates how you can further delegate authentication responsibility to Active Directory, but you still do not have the automatic sign-on and CIFS browsing capabilities that are available to internal Alfresco users.

1. Restart the Alfresco server.

   If you watch the output from Tomcat in alfresco.log in the installation directory, you will eventually see lines similar to the following:

   ```
   13:01:31,225 INFO
   [org.alfresco.repo.management.subsystems.ChildApplicationContextFactory]
   Starting 'Synchronization' subsystem, ID: [Synchronization, default]

   …

   13:01:49,084 INFO
   [org.alfresco.repo.security.sync.ChainingUserRegistrySynchronizer]
   Finished synchronizing users and groups with user registry 'ldap1'

   13:01:49,084 INFO
   [org.alfresco.repo.security.sync.ChainingUserRegistrySynchronizer]
   177 user(s) and 19 group(s) processed

   13:01:49,131 INFO
   [org.alfresco.repo.management.subsystems.ChildApplicationContextFactory]
   Startup of 'Synchronization' subsystem, ID: [Synchronization, default]
    complete
   ```

   This is output is from the Synchronization subsystem, which is another Alfresco subsystem responsible for synchronizing the Alfresco internal user and authority database with all user registries in the authentication chain. Since the authentication chain now provides a user registry, the Synchronization subsystem has some work to do when Alfresco starts up.
2. From the example logs, notice that the Synchronization subsystem automatically created 177 users and 19 groups using attributes, such as email address and group memberships, retrieved from Active Directory through an LDAP query. This reduces the workload of the admin user.

   The Synchronization subsystem uses an incremental timestamp-based synchronization strategy, meaning that it only queries for changes since the last synchronization run. So after the first start up, further synchronization runs can be almost instantaneous. Because synchronization runs are also triggered by a scheduled nightly job and whenever an unknown user successfully authenticates, you should find that Alfresco always stays synchronized with hardly any effort.

Now, if you enter the Alfresco Explorer URL: http://localhost:8080/alfresco/ into your browser, you can log in using the ID and password of any of the Active Directory users.

Passwords are validated through an LDAP bind operation on Active Directory in real time. Passwords for Active Directory users are not stored locally.

3. Navigate to a user profile.

   Notice that attributes such as email address were populated automatically from Active Directory.

Configuring Kerberos

The Java Authentication and Authorization Service (JAAS) is used within the Kerberos subsystem to support Kerberos authentication of user names and passwords. You may choose to use Kerberos against an Active Directory server in preference to LDAP or NTLM as it provides strong encryption without using SSL. It would still be possible to export user registry information using a chained LDAP subsystem.

The disadvantages of using LDAP authentication against Active Directory compared with JAAS/ Kerberos are:

- the simplest approach is to use the SIMPLE LDAP authentication protocol, which should be used with SSL
- AD requires special set up to use digest MD5 authentication (reversible encryption for passwords), which may be difficult retrospectively
- LDAP can use GSSAPI and Kerberos which would be equivalent but this is more difficult to configure and has not been tested

For some pointers and background information on JAAS, the Java Authentication and Authorization Service, refer to the following web sites:

- http://java.sun.com/products/jaas/
- http://en.wikipedia.org/wiki/Java_Authentication_and_Authorization_Service

Kerberos configuration properties

To enable full Kerberos support in Alfresco requires that the CIFS server and the SSO authentication filters each have a Kerberos service ticket.

The Kerberos subsystem supports the following properties.

kerberos.authentication.realm
The Kerberos realm with which to authenticate. The realm should be the domain upper cased; an example is that if the domain is `alfresco.org` then the realm should be `ALFRESCO.ORG`.

kerberos.authentication.sso.enabled
A Boolean that when true enables SPNEGO/Kerberos based Single Sign On (SSO) functionality in the web client. When false and no other members of the authentication chain support SSO, password-based login will be used.

kerberos.authentication.authenticateCIFS
A Boolean that when true enables Kerberos authentication in the CIFS server. When false and no other members of the authentication chain support CIFS authentication, the CIFS server will be disabled.

kerberos.authentication.user.configEntryName
The name of the entry in the JAAS configuration file that should be used for password-based authentication. The default value `Alfresco` is recommended.

kerberos.authentication.cifs.configEntryName
The name of the entry in the JAAS configuration file that should be used for CIFS authentication. The default value `AlfrescoCIFS` is recommended.

kerberos.authentication.http.configEntryName
The name of the entry in the JAAS configuration file that should be used for web-based single-sign on (SSO). The default value `AlfrescoHTTP` is recommended.

kerberos.authentication.cifs.password
The password for the CIFS Kerberos principal.

kerberos.authentication.http.password
The password for the HTTP Kerberos principal.

kerberos.authentication.defaultAdministratorUserNames
A comma separated list of user names who should be considered administrators by default.

Configuring Kerberos against Active Directory

The following instructions describe how to set up accounts under Active Directory for use by Alfresco.

1. Create a user account for the Alfresco CIFS server using the Active Directory Users and Computers application.
   a. Use the **Action > New > User** menu, then enter the full name as `Alfresco CIFS` and the user login name as `alfrescocifs`.
   b. Click **Next**.
   c. Enter a password.
   d. Enable **Password never expires** and disable **User must change password at next logon**.
   e. Click **Finish**.
   f. Right-click the new user account name, and then select **Properties**.
   g. Select the **Account** tab and enable the **Do not require Kerberos preauthentication** option in the **Account Options** section.
2. Create a user account for the Alfresco SSO authentication filters, following the instructions in step one, using the full name `Alfresco HTTP` and the user login name as `alfrescohttp`.
3. Use the `ktpass` utility to generate key tables for the Alfresco CIFS and web server.

   The `ktpass` utility is a free download from the Microsoft site, and is also part of the Windows Server 2003 Support Tools. The `ktpass` command can only be run from the Active Directory server.

   Note that the `-kvno 0` argument is required when using JDK 1.6 u22.

```
ktpass -princ cifs/<cifs-server-name>.<domain>@<realm> -pass <password> -
mapuser <domainnetbios>\alfrescocifs
-crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL -out c:\temp
\alfrescocifs.keytab -kvno 0
```

```
ktpass -princ HTTP/<web-server-name>.<domain>@<realm> -pass <password> -
mapuser <domainnetbios>\alfrescohttp
-crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL -out c:\temp
\alfrescohttp.keytab -kvno 0
```

a. Specify the `principal` using the server name and domain in lowercase with the realm in uppercase. Match the service types to `cifs` and `HTTP`. For example, `cifs/server.alfresco.org@ALFRESCO.ORG`.

b. Specify the `realm` as the domain in upper case. For example, if the domain is `alfresco.org` then the realm is `ALFRESCO.ORG`.

c. `<web-server-name>` is the host name that is running the Alfresco server.

d. Specify `<cifs-server-name>` as the NetBIOS name of the Alfresco CIFS server when running on an Active Directory client or the host name for a client that is not an Active Directory client, that is, not logged onto the domain.

e. Specify `<domain>` as the DNS domain. For example `alfresco.org`.

f. Specify `<domainnetbios>` as the netbios name. For example `alfresco`.

Some versions of the `ktpass` command can generate invalid `keytab` files. Download the latest version of the support tools from the Microsoft site to avoid any problems.

4. Create the Service Principal Names (SPN) for the Alfresco CIFS and web server using the `setspn` utility. The `setspn` utility is a free download from the Microsoft site, and is also part of the Windows 2003 Support Tools download.

```
setspn -a cifs/<cifs-server-name> alfrescocifs
setspn -a cifs/<cifs-server-name>.<domain> alfrescocifs
```

```
setspn -a HTTP/<web-server-name> alfrescohttp
setspn -a HTTP/<web-server-name>.<domain> alfrescohttp
```

Some versions of the `ktpass` command will add the SPN for the `principal` so you may only need to add the NetBIOS/short name versions of the SPNs. Use the `setspn -l <account-name>` command to check if the `ktpass` command set the SPN. You can list the SPNs for a server using the following:

```
setspn -l <account-name>
```

For example:

```
setspn -l alfrescocifs
setspn -l alfrescohttp
```

5. Copy the key table files created in step 3 to the server where Alfresco will run. Copy the files to a protected area such as `C:\etc\` or `/etc`.

6. Set up the Kerberos `ini` file.

The default location is `C:\WINNT\krb5.ini` or `/etc/krb5.conf`.

```
[libdefaults]
 default_realm = ALFRESCO.ORG
 default_tkt_enctypes = rc4-hmac
 default_tgs_enctypes = rc4-hmac

[realms]
 ALFRESCO.ORG = {
  kdc = adsrv.alfresco.org
  admin_server = adsrv.alfresco.org
 }

[domain_realm]
 adsrv.alfresco.org = ALFRESCO.ORG
 .adsrv.alfresco.org = ALFRESCO.ORG
```

The realm should be specified in uppercase.

7. Set up the Java login configuration file.

For JBoss 5, open the `$JBOSS_HOME/server/default/conf/login-config.xml` file. Add the following entries inside the `<policy>` tag:

```
 <application-policy name="Alfresco">
   <authentication>
     <login-module code="com.sun.security.auth.module.Krb5LoginModule"
 flag="sufficient"/>
   </authentication>
 </application-policy>

 <application-policy name="AlfrescoCIFS">
   <authentication>
     <login-module code="com.sun.security.auth.module.Krb5LoginModule"
 flag="required">
       <module-option name="debug">true</module-option>
       <module-option name="storeKey">true</module-option>
       <module-option name="useKeyTab">true</module-option>
       <module-option name="isInitiator">false</module-option>
       <module-option name="keyTab">C:/etc/alfrescocifs.keytab</module-
option>
       <module-option name="principal">cifs/<cifs-server-name>.domain</
module-option>
     </login-module>
   </authentication>
 </application-policy>

 <application-policy name="AlfrescoHTTP">
   <authentication>
     <login-module code="com.sun.security.auth.module.Krb5LoginModule"
 flag="required">
       <module-option name="debug">true</module-option>
       <module-option name="storeKey">true</module-option>
       <module-option name="isInitiator">false</module-option>
       <module-option name="useKeyTab">true</module-option>
       <module-option name="keyTab">C:/etc/alfrescohttp.keytab</module-
option>
       <module-option name="principal">HTTP/<web-server-name>.<domain></
module-option>
     </login-module>
   </authentication>
 </application-policy>
```

For other environments, in the `JRE\lib\security` folder (for example, `/usr/local/jdk1.6.0_03/jre/lib/security`), create a file named `java.login.config` with the following entries:

```
Alfresco {
   com.sun.security.auth.module.Krb5LoginModule sufficient;
};

AlfrescoCIFS {
   com.sun.security.auth.module.Krb5LoginModule required
   storeKey=true
   useKeyTab=true
   keyTab="C:/etc/alfrescocifs.keytab"
   principal="cifs/<cifs-server-name>.<domain>";
};

AlfrescoHTTP {
   com.sun.security.auth.module.Krb5LoginModule required
   storeKey=true
   useKeyTab=true
   keyTab="C:/etc/alfrescohttp.keytab"
   principal="HTTP/<web-server-name>.<domain>";
};

com.sun.net.ssl.client {
   com.sun.security.auth.module.Krb5LoginModule sufficient;
};

other {
   com.sun.security.auth.module.Krb5LoginModule sufficient;
};
```

8. Enable the login configuration file by adding the following line to the main Java security configuration file, usually at `JRE\lib\security\java.security`.

   ```
   login.config.url.1=file:${java.home}/lib/security/java.login.config
   ```

Kerberos client configuration

This section describes how to configure the Kerberos client authentication.

To make Internet Explorer negotiate Kerberos authentication, rather than NTLM, ensure that:

- Alfresco web server is in the Local Intranet security zone.

  Check **Tools > Internet Options > Security > Local Intranet**, and then ensure that a pattern matching the protocol and domain name is included, for example, http://server.com or http://*.company.com (the IP address does not work).
- Automatic log on is enabled.

  Check **Tools > Internet Options > Security > Custom Level**, and then ensure Automatic log on with the current user name and password is selected.

1. When using Firefox on Windows as your client, you need to add your Alfresco server name to the `network.negotiate-auth.trusted-uris` variable.

   Access the variable from the special URL: `about:config`.
2. When using Firefox on Linux, you need to add your Alfresco server name to `network.negotiate-auth.trusted-uris` but you will need, in addition, to get a Kerberos ticket using the `kinit` command.

   The ticket can correspond to a different user than your Linux user name.

   For example:

   ```
   kinit user1
   ```

   Where `user1` is an Active Directory user. If the client and the server are on the same machine, you will need to go to the `eternl` interface. The `loopback` interface will not be able to authenticate. You can view your tickets using `klist`.

Debugging Kerberos

You can debug Kerberos issues using the log4j properties.

For example:

```
log4j.logger.org.alfresco.web.app.servlet.KerberosAuthenticationFilter=debug
log4j.logger.org.alfresco.repo.webdav.auth.KerberosAuthenticationFilter=debug
```

The following is a sample login output:

```
18:46:27,915 DEBUG [app.servlet.KerberosAuthenticationFilter] New Kerberos auth
 request from 192.168.4.95 (192.168.4.95:38750)
18:46:28,063 DEBUG [app.servlet.KerberosAuthenticationFilter] User user1 logged
 on via Kerberos
```

Configuring Share Kerberos SSO

This section describes how to configure the Share server and Active Directory server to work with Kerberos Single Sign On (SSO).

1. Configure the Alfresco server.

2. Configure Share.
   a. Open the Share `<web-extension>` directory.
   b. Copy or rename the `share-config-custom.xml.sample` file to be called `share-config-custom.xml`.
   c. Locate the `<!-- Kerberos settings -->` section.

      ```
      <!-- Kerberos settings -->
         <!-- To enaable kerberos rename this condition to "Kerberos" -->
         <config evaluator="string-compare" condition="KerberosDisabled"
       replace="true">
           <kerberos>
      ```
   d. Replace the `password`, `realm`, and `endpoint-spn` optiona with the correct values.
   e. Uncomment the `<config evaluator="string-compare" condition="Remote">` section.
   f. In the (Sun Java) `jre/lib/security/java.login.config` file, add a new section:

      ```
      ShareHTTP {
         com.sun.security.auth.module.Krb5LoginModule required
         storeKey=true
         useKeyTab=true
         keyTab="/etc/keys/alfrescohttp.keytab"
         principal="HTTP/madona.example.foo";
      };
      ```
3. Configure Active Directory.
   a. Modify the `alfrescohttp` user created during the Alfresco Kerberos setup.
   b. In the user **Delegation** tab, tick the **Trust this user for delegation to any service (Kerberos only)** check box.

      If you do not see the delegation tab, follow the `Allow a user to be trusted for delegation for specific services` instruction on the Microsoft http://technet.microsoft.com website.
   c. If you cannot see the **Delegation** tab, do one or both of the following:

      - Register a Service Principal Name (SPN) for the user account with the Setspn utility in the support tools on your CD. Delegation is only intended to be used by service accounts, which should have registered SPNs, as opposed to a regular user account which typically does not have SPNs.
      - Raise the functional level of your domain to Windows Server 2003.

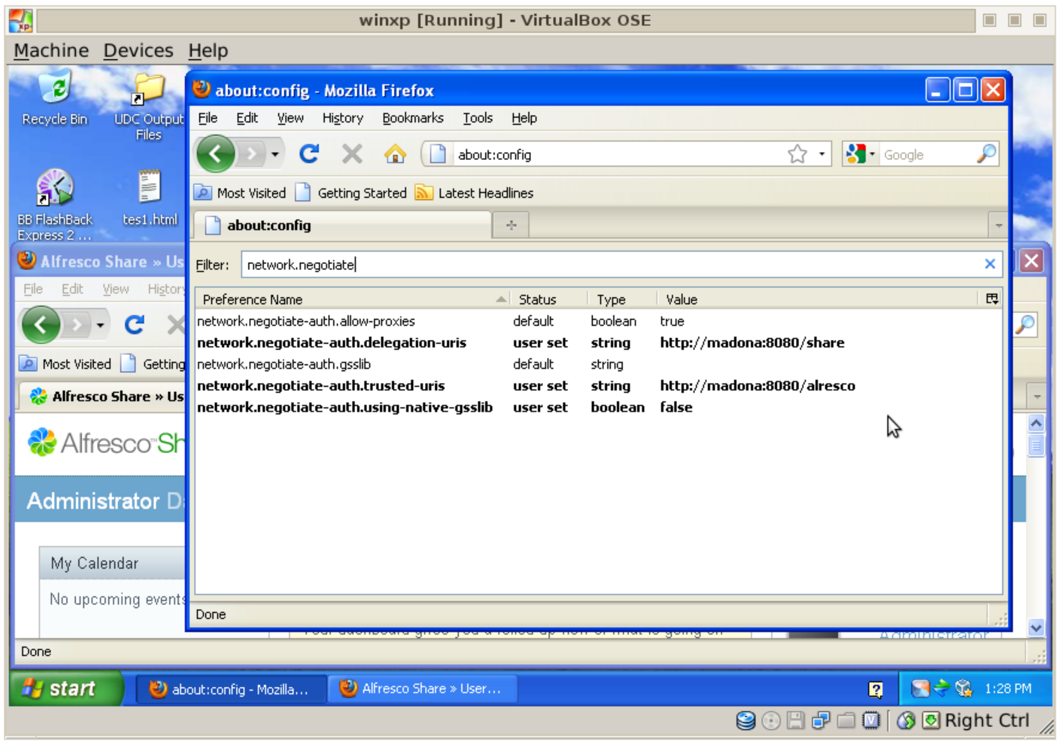
      To raise the domain functional level:

      1. Open **Active Directory Domains and Trusts**.
      2. In the console tree, right-click the domain for which you want to raise functionality, and then click **Raise Domain Functional Level**.
      3. In **Select an available domain functional level**, do one of the following:

         - To raise the domain functional level to Windows 2000 native, click **Windows 2000 native**, and then click **Raise**.
         - To raise domain functional level to Windows Server 2003, click **Windows Server 2003**, and then click **Raise**.
4. Configure the client.
   a. For Windows client configuration, Internet Explorer configured as described in Kerberos client configuration on page 175 should work without modifications.

b. To make Firefox work on windows on the share URL with Kerberos SSO, you need to modify (in the about:config special URL) the following variables:

```
network.negotiate-auth.delegation-uris
network.negotiate-auth.trusted-uris
network.negotiate-auth.using-native-gsslib
```


winxp [Running] - VirtualBox OSE
Machine Devices Help
about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
Most Visited Getting Started Latest Headlines
Recycle Bin
UDC Output Files
BB FlashBack Express 2 ...
tes1.html
Alfresco Share » Us
Administrator D
My Calendar
No upcoming events
Done
start
Right Ctrl

Filter: network.negotiate

Preference Name	Status	Type	Value
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	**user set**	**string**	**http://madona:8080/share**
network.negotiate-auth.gsslib	default	string	
network.negotiate-auth.trusted-uris	**user set**	**string**	**http://madona:8080/alfresco**
network.negotiate-auth.using-native-gsslib	**user set**	**boolean**	**false**

The following are known issues:

- Linux clients (Firefox) do not work
- Share Kerberos SSO does not work with IBM Java

Configuring external authentication

The `external` authentication subsystem can be used to integrate Alfresco with any external authentication system.

The external authentication system can be integrated with your application server in such a way that the identity of the logged-in user is passed to servlets via the `HttpServletRequest.getRemoteUser()` method. As this is the standard way for application servers to propagate user identities to servlets, it should be compatible with a number of SSO solutions, including Central Authentication Service (CAS).

The subsystem also allows a proxy user to be configured, such that requests made through this proxy user are made in the name of an alternative user, whose name is carried in a configured HTTP request header. This allows, for example, the Share application and other Alfresco Surf applications to act as a client to an SSO-protected Alfresco application and assert the user name in a secure manner.

External configuration properties

The external subsystem supports the following properties.

external.authentication.enabled
A Boolean property that when true indicates that this subsystem is active and will trust remote user names asserted to it by the application server.

external.authentication.defaultAdministratorUserNames
A comma separated list of user names who should be considered administrators by default.

external.authentication.proxyUserName
The name of the remote user that should be considered the proxy user. The default is `alfresco-system`. Requests made by this user will be made under the identity of the user named in the HTTP Header indicated by the `external.authentication.proxyHeader` property. If not set, then the HTTP Header indicated by the `external.authentication.proxyHeader` property is always assumed to carry the user name.

This is not secure unless this application is not directly accessible by other clients.

external.authentication.proxyHeader
The name of the HTTP header that carries the name of a proxied user. The default is `X-Alfresco-Remote-User`, as used by Share.

external.authentication.userIdPattern
An optional regular expression to be used to extract a user ID from the HTTP header. The portion of the header matched by the first bracketed group in the regular expression will become the user name. If not set (the default), then the entire header contents are assumed to be the proxied user name.

Authorities

Authorities are people (or persons) or groups.

A group may contain people or other groups as members. The authorities assigned to a user at any time are the userName from their associated Person node, all of the groups in which the user is a direct or indirect member, and any appropriate dynamic authorities. Dynamic authorities are used for internal roles.

Dynamic authorities and roles

Alfresco uses some custom roles. To implement a custom role, you create a dynamic authority for that role and assign global permissions to it. The Alfresco internal roles have not been assigned any object-specific rights. The internal roles are:

- ROLE_ADMINISTRATOR is assigned to the default administrators for the configured authentication mechanisms or members of the administration groups defined on the AuthorityServiceImpl bean. This role has all rights.
- ROLE_OWNER is assigned to the owner of a node. If there is no explicit owner, this role is assigned to the creator. This role has all rights on the owned node.
- ROLE_LOCK_OWNER is assigned to the owner of the lock on a locked node. This supports a lock owner’s right to check in, cancel a check out, or unlock the node.

The Alfresco Explorer and Alfresco Share currently support the assignment of permissions only to the owner role. You can use such things as the Java API and scripting to make other assignments.

Hierarchical and zoned roles may be added to Alfresco in the future to avoid the hidden group implementation for true roles.

People and users

When a user logs in, Alfresco validates the user’s identifier and password. Alfresco uses the identifier to look up the appropriate person details for the user, using the `userName` property on the Person type. You can configure this look-up to be case sensitive or case insensitive. The `userName` property on the matching Person node is used as the actual user authority; it may differ in case from the user identifier presented to the authentication system. After the Person node look-up, Alfresco is case sensitive when matching authorities to permissions, group membership, roles, and for all other authorization tests.

Any user, who authenticates by any mechanism, must have an associated person node in Alfresco. Person nodes may be:

- Explicitly created
- Created on demand with some default entries
- Created from LDAP synchronization

Person nodes are explicitly created when using the administration pages of the Alfresco Explorer and Alfresco Share web clients to manage users.

By default, person nodes are auto-created if not present. If an external authentication system is configured, such as NTLM, when any user authenticates, an appropriate person node may not exist. If a person node does not exist and auto-creation is enabled, a person node will then be created using the identifier exactly as presented by the user and validated by the authentication system. The auto-created Person node’s userName will have the same case as typed by the user. LDAP synchronization will create person nodes with the userName, as provided from the LDAP server.

It is possible that LDAP synchronization can change the userName associated with a Person node. For example, this can happen with a system that uses NTLM authentication, LDAP synchronization, or a system that creates person nodes on demand, or uses case-insensitive authentication. For example, Andy could log in as “Andy” and the associated Person node is created with the userName “Andy.” Later, the LDAP synchronization runs and changes the userName to “andy”.

From version 3.2, changes to Person node userNames will cause updates to other related data in Alfresco, such as ACL assignment.

Groups

Groups are collections of authorities with a name and display name.

Groups may include other groups or people. You can include a group in one or more other groups, as long as this inclusion does not create any cyclic relationships.

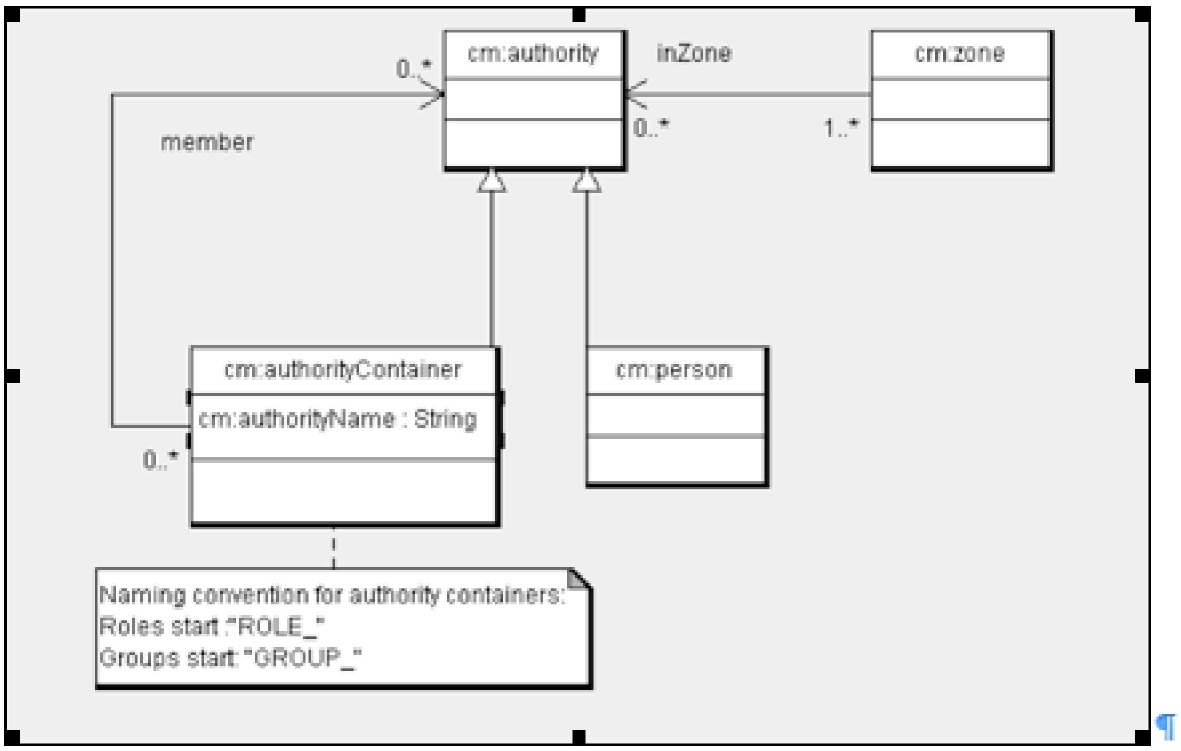
Zones

All person and group nodes are in one or more zones. You can use zones for any partitioning of authorities. For example, Alfresco synchronization uses zones to record from which LDAP server users and groups have been synchronized. Zones are used to hide some groups that provide Role Based Access Control (RBAC) role-like functionality from the administration pages of the Alfresco Explorer and Alfresco Share web clients. Examples of hidden groups are the roles used in Alfresco Share and Records Management (RM). Only users and groups in the default zone are shown for normal group and user selection on the group administration pages. Zones cannot be managed from the administration pages of Alfresco Explorer and Alfresco Share.

Zones are intended to have a tree structure defined by naming convention. Zones are grouped into two areas: Application-related zones and authentication-related zones.

Within a zone, a group is considered to be a root group if it is not contained by another group in the same zone.

Alfresco uses a model for persisting people, groups, and zones. A Person node represents each person, and an AuthorityContainer represents groups, which can be used for other authority groupings such as roles. AuthorityContainer and Person are sub-classes of Authority and as such can be in any number of Zones.



Application-related zones

Application-related zones, other than the default, hide groups that implement RBAC like roles. Application zones, by convention, start APP. and include:

- APP.DEFAULT is for person and group nodes to be found by a normal search. If no zone is specified for a person or group node, they will be a member of this default zone.
- APP.SHARE is for hidden authorities related to Alfresco Share.
- APP.RM will be added for authorities related to RM.

Authorization-related zones

Zones are also used to record the primary source of person and group information. They may be held within Alfresco or some external source. While authorities can be in many zones, it makes sense for an authority to be in only one authentication-related zone.

- AUTH.ALF is for authorities defined within Alfresco and not synchronized from an external source. This is the default zone for authentication.
- AUTH.EXT.<ID> is for authorities defined externally, such as in LDAP.

Defining permissions

Permissions and their groupings are defined in an XML configuration file. The default file is found in the distribution configuration directory as <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\model\permissionDefinitions.xml. This configuration can be replaced or extended and has a structure as described in <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\model\permissionSchema.dtd.

The following example uses the permission definitions related to the Ownable aspect.

```
<!-- ============================================ -->
   <!-- Permissions associated with the Ownable aspect -->
   <!-- ============================================ -->
   <permissionSet type="cm:ownable" expose="selected">

      <!-- Permission control to allow ownership of the node to be taken from
 others -->
      <permissionGroup name="TakeOwnership" requiresType="false"
 expose="false">
        <includePermissionGroup permissionGroup="SetOwner" type="cm:ownable" />
      </permissionGroup>

      <permissionGroup name="SetOwner" requiresType="false" expose="false"/>

      <!-- The low level permission to control setting the owner of a node -->
      <permission name="_SetOwner" expose="false" requiresType="false">
        <grantedToGroup permissionGroup="SetOwner" />
        <requiredPermission on="node" type="sys:base" name="_WriteProperties" /
>
      </permission>

</permissionSet>
```

Permissions and permission groups are defined in a permission set, which is a sub-element of the permissions root element. A permission set is associated with a type or aspect and applies only to that type and sub-types, or aspect and sub-aspects.

A permission has a name. By convention, the names of permissions start with an underscore character. They may be exposed in the administration pages of the Alfresco Explorer and Alfresco Share web clients but, usually, are not. A permission, in its definition, may be granted to any number of permission groups. This means that those permission groups will include the permission. The permission may require that the type or aspect specified on the permission set be present on the node. If a permission is associated with an aspect and the requiresType property is set to true then if that aspect is not applied to a node, the permission does not apply to that node either. If an aspect-related permission definition has the requiresType property set to false, the permission applies to any node, even if the aspect has not been applied to the node.

An aspect can be applied at any time and there are no restrictions as to which aspects can be applied to a type. A permission may also require other permissions be tested on the same node, its children, or its parent. In the example, _SetOwner requires _WriteProperties. This means you cannot set ownership on a node if you are not allowed to write to its properties. You can also use this to check that all children can be deleted before deleting a folder, or to enforce that you can only read nodes for which you can read all the parents; neither are normally required in Alfresco. The configuration to do this is present in the standard configuration file but is commented out. The _DeleteNode permission definition (as shown in the following code snippet) is an example. If permission A requires permission B and this requirement is implied (by setting the implies attribute of the requiredPermission element to true), assigning an authority permission A will also give them permission B (as opposed to checking they have permission B).

```
<permission name="_DeleteNode" expose="false" >
    <grantedToGroup permissionGroup="DeleteNode" />
    <!-- Commented out parent permission check ...
    <requiredPermission on="parent" name="_ReadChildren" implies="false"/>
    <requiredPermission on="parent" name="_DeleteChildren" implies="false"/>
    <requiredPermission on="node" name="_DeleteChildren" implies="false"/>
     -->
    <!-- Recursive delete check on children -->
    <!--  <requiredPermission on="children" name="_DeleteNode" implies="false"/
>  -->
</permission>
```

Permissions are normally hidden inside permission groups. Permission groups are made up of permissions and other permission groups. By convention, each permission has a related permission group. Permission groups can then be combined to make other permission groups. As for permissions, a permission group may be exposed by the administration pages of Alfresco

Explorer and Alfresco Share and may require the presence of a type or aspect to apply to a particular node. In addition, a permission group may allow full control, which grants all permissions and permission groups. As a type or aspect may extend another, a permission group defined for a type or aspect can extend one defined for one of its parent types and be assigned more permissions, include more permission groups, or change what is exposed in the administration pages of the Alfresco Explorer and Alfresco Share web clients.

It is unusual to extend or change the default permission model unless you are adding your own types, aspects, and related public services or you wish to make minor modifications to the existing behavior. The following code snippets show how to extend and replace the default permission model.

```
<bean id='permissionsModelDAO'
class="org.alfresco.repo.security.permissions.impl.model.PermissionModel">
        <property name="model">
<-- <value>alfresco/model/permissionDefinitions.xml</value> -->
<value>alfresco/extension/permissionDefinitions.xml</value>
        </property>
        <property name="nodeService">
            <ref bean="nodeService" />
        </property>
        <property name="dictionaryService">
            <ref bean="dictionaryService" />
        </property>
</bean>
```

The preceding code example shows how to replace the default permission model with one located in the alfresco/extension directory. The following code snippet shows how to extend the existing model.

```
<bean id="extendPermissionModel" parent="permissionModelBootstrap">
   <property name="model" value="alfresco/extension/
permissionModelExtension.xml" />
</bean>
```

Access Control Lists

An Access Control List (ACL) is an ordered list of Access Control Entries (ACEs). An ACE associates a single authority to a single permission group or permission, and states whether the permission is to be allowed or denied. All nodes have an associated ACL. There is one special, context-free, ACL defined in the XML configuration to support global permissions. An ACL specifies if it should inherit ACEs from a parent ACL. The parent ACL is associated with the primary parent node. When a new node is created it automatically inherits all ACEs defined on the parent within which it is created. Linking a node to a secondary parent has no effect on ACE inheritance; the node will continue to inherit permission changes from its primary parent (defined when it was first created).

By default, ACL inheritance is always from the primary parent. The underlying design and implementation does not mandate this. ACL inheritance does not have to follow the parent child relationship. It is possible to change this through the Java API but not via the administration pages of Alfresco Explorer and Alfresco Share.

There are several types of ACL defined in ACLType. The main types are:

- DEFINING
- SHARED
- FIXED
- GLOBAL

A node will be associated with an ACL. It will have a DEFINING ACL if any ACE has been set on the node. DEFINING ACLs include any ACEs inherited from the node’s primary parent and above, if inheritance is enabled. All DEFINING ACLs are associated with one SHARED ACL. This SHARED ACL includes all the ACEs that are inherited from the DEFINING ACL. If the primary children of a node with a DEFINING ACL do not themselves have any specific ACEs defined then they can be assigned the related SHARED ACL. For the primary children of a node with a SHARED ACL that also have no specific ACEs set they can use the same SHARED ACL. A single SHARED ACL can be associated with many nodes. When a DEFINING ACL is updated, it will cascade update any related ACLs via the ACL relationships rather than walk the node structure. If a DEFINING ACL inherits ACEs, then these will come from the SHARED ACL related to another DEFINING ACL.

ACLs and nodes have two linked tree structures.

FIXED ACLs are not associated with a node but found by name. A node ACL could be defined to inherit from a fixed ACL. A GLOBAL ACL is a special case of a FIXED ACL with a well known name. It will be used to hold the global ACE currently defined in XML.

ACEs comprise an authority, a permission, and a deny/allow flag. They are ordered in an ACL.

ACL ordering and evaluation

The ACEs within an ACL are ordered and contain positional information reflecting how an ACE was inherited. DEFINING ACLs have entries at even positions; SHARED ACLs have entries at odd positions. For a DEFINING ACL, any ACEs defined for that ACL have position 0, any inherited from the parent ACL have position two, and so on. For a SHARED ACL, ACEs defined on the ACL from which it inherits will have position one.

When Alfresco makes permission checks, ACEs are considered in order with the lowest position first. Deny entries take precedence over allow entries at the same position. The default configuration is that “any allow allows”. Once a deny entry is found for a specific authority and permission combination, any matching ACE, at a higher position from further up the inheritance chain, is denied. A deny for one authority does not deny an assignment for a different authority. If a group is denied Read permission, a person who is a member of that group can still be assigned Read permission using another group or directly with their person userName. However, if an authority is granted Read (made up of ReadContent and ReadProperties) and the same authority denied ReadContent, they will just be granted ReadProperties permission. The administration pages of Alfresco Explorer and Alfresco Share do not expose deny.

You can alter the configuration to support “any deny denies”.

An ACL example

This example relates a tree of nodes to two corresponding trees of ACLs. The nodes in the node tree are identified by number and are shown filled in black if they have any ACEs set, or white/ clear if not. Primary child relationships are drawn as black lines and secondary child relationships as dashed lines. ACLs in the ACL trees are identified by letter, DEFINING ACLs are shown filled in black, and SHARED ALCs are shown as clear. Under each node on the node tree the related ACL is referenced.

The table describes the ACEs in each ACL and their position.

Table 1: ACL formats

ACL format	Authority	Permission	Allow/Deny	Position
ACL A (Defining, no inheritance)	All	Read	Allow	0
ACL B (Shared, inherits from ACL B)	All	Read	Allow	1
ACL C (Defining, inherits from ACL B)	All	Read	Allow	2
	ROLE_OWNER	All	Allow	0

ACL format	Authority	Permission	Allow/Deny	Position
	GROUP_A	Write	Allow	0
	GROUP_A	CreateChildren	Allow	0
ACL D (Shared, inherits from ACL C)	ALL	Read	Allow	3
	ROLE_OWNER	All	Allow	1
	GROUP_A	Write	Allow	1
	GROUP_A	CreateChildren	Allow	1
ACL E (Defining, inherits from ACL B)	All	Read	Allow	2
	Andy	All	Allow	0
	Bob	Write	Allow	0
	Bob	WriteContent	Deny	0
ACL F (Shared, inherits from ACL E)	All	Read	Allow	3
	Andy	All	Allow	1
	Bob	Write	Allow	1
	Bob	WriteContent	Deny	1
ACL G (Defining, no inheritance)	Bob	All	Allow	0
ACL H (Shared, inherits from ACL G)	Bob	All	Allow	1

ACL A, and any ACL that inherits from it, allows Read for everyone (All) unless permissions are subsequently denied for everyone (All). If ACL A is changed, all the ACLs that inherit from ACL A in the ACL tree will reflect this change. In the example, nodes 1-12 would be affected by such a change. Nodes 13 and 14 would not inherit the change due to the definition of ACL G.

ACL C adds Contributor and Editor permissions for any authority in GROUP_A.

The GROUP_ prefix is normally hidden by the administration pages of Alfresco Explorer and Alfresco Share.

Anyone in GROUP_A can edit existing content or create new content. The owner ACE means that anyone who creates content then has full rights to it. The ACE assignment for owner is not normally required as all rights are given to node owners in the context-free ACL defined in the default permission configuration.

ACL E adds some specific user ACEs in addition to those defined in ACL A. As an example, it allows Bob Write but also denies WriteContent. Write is made up of WriteContent and WriteProperties. Bob will only be allowed WriteProperties.

ACL G does not inherit and starts a new ACL tree unaffected by any other ACL tree unless an inheritance link is subsequently made.

If a new node was created beneath node 13 or 14 it would inherit ACL H. If a new node was created beneath nodes 1, 6, 7, or 8 it would inherit ACL B.

If a node that has a shared ACL has an ACE set, a new defining ACL and a related shared ACL are inserted in the ACL tree. If a defining ACL has all its position 0 ACEs removed, it still remains a defining ACL: There is no automatic clean up of no-op defining ACLs.

Modifying access control

Modifying access control may involve:

- Changing the definition of existing security interceptors to check for different conditions
- Adding new public services and related security interceptors

- Defining new types and aspects and their related permissions
- Adding new definitions to the security interceptor by implementing an ACEGI AccessDecisionVoter and/or AfterInvocationProvider (in extreme cases)

A few constraints and design patterns should be observed when modifying access control. Permissions apply to the node as whole. In particular, the same Read rights apply to all properties and content. You should check that methods can be executed and not that a user has a particular permission. The access control restrictions for a public service method may change. Follow the design pattern to implement RBAC roles.

When modifying access control, do not try to split ReadProperties and ReadContent. This does not make sense for search. A node and all of its properties, including content, are indexed as one entity. Splitting the evaluation of access for content and properties is not possible. Search would have to apply both criteria so as to not leak information. Other services, such as copy, may not behave as expected or may produce nodes in an odd state.

Permissions are assigned at the node level, not at the attribute level. Again, this makes sense with the search capabilities. Search results need to reflect what the user performing the search can see. It makes sense that all properties have the same Read access as the node, as nodes are indexed for searching and not individual properties. Applying Read ACLs at the property level would require a change to the indexing implementation or a complex post analysis to work out how nodes were found by the search. If not, the values of properties could be deduced by how a readable node was found from a search on restricted properties.

Fine grain attribute permissions could be implemented by using children nodes to partition metadata. Queries would have to be done in parts and joined by hand, as there is no native support for SQL-like join.

Check that method execution is allowed and not that the user has a fixed permission. Rather than checking for Read permission in code, check that the appropriate method can be called using the PublicServiceAccessService bean. This avoids hard coding to a specific permission implementation and is essential if you intend to mix records management and the content repository. In any case, the access restrictions for public service methods may change. The PublicServiceAccessService bean allows you to test if any public service method can be invoked successfully with a given set of arguments. It checks all the entry criteria for the method and, assuming these have not changed, the method can be called successfully. The method call may still fail if the conditions for the returned object are not met or some security configuration has changed, such as an ACE is removed, a user is removed from a group, or the method fails for a non-authorization reason.

For those coming from an RBAC background, Alfresco has roles in the RBAC sense only for limited internal use. To implement RBAC in Alfresco, use zoned groups. These groups will not appear in the administration pages of the Alfresco Explorer and Alfresco Share web clients as normal groups (unless you also add them to the APP.DEFAULT zone) but can be used to assign users and groups to roles. This approach has been taken in Alfresco to support roles in Alfresco Share and records management. To map RBAC terminology to Alfresco: operations map to method calls on public service beans, objects map to method arguments including nodes (folders, documents, and so on). Users and permissions/privileges map directly. Alfresco allows the assignment of permissions to users or groups.

By default, the owner of an object can manage any aspect of its ACL. Users with ChangePermissions rights for a node can also change its ACL. If users have the ability to alter the ACL associated with an object, they can allow other users to do the same. There is no restriction on the permissions they may assign. The Alfresco model supports liberal discretionary access control with multi-level grant. A user who can grant access can pass on this right without any restriction. In addition, anyone who can change permissions can carry out the revocation of rights: it is not restricted to the original granter. Normally, when someone can perform an operation you would not expect it is because they own the node and therefore have all permissions for that node.

Access Control Extension

The Access Control model is used for all nodes in the content repository except those related to the Records Management extension. Records Management is used as an example here to outline how to extend access control.

The Records Management authorization is based around a fixed set of capabilities that are part of the DOD 5015.2 specification. These capabilities describe records management operations for which there is not a direct mapping to an Alfresco public service method call. There are separate Records Management implementations of the ACEGI AccessDecisionVoter and AfterInvocationProvider interfaces to support this mapping. The AccessDecisionVoter allows or denies access on method entry. The AfterInvocationProvider allows or denies access based on the method return value; it can also alter the return value. All Records Management nodes carry a marker aspect (an aspect that defines no properties or associations). If this marker is present, the default voter will abstain; if this marker is absent, the Records Management voter will abstain.

Public services are protected for Records Management in the same manner as already described but with two sets of configuration: one for each of the two different implementations. It is more complex to map the Records Management capabilities and caveats (for example, security clearance) to public service method calls and to enforce the restrictions. For example, the node service updateProperties method has to incorporate the idea of updating declared and undeclared records, allow updates to selected properties, and to restrict access to some properties that should only be updated as part of state management. The Records Management voter has additional Records Management hard-coded policies to protect the public services in order to encapsulate the logic for this and related use cases.

In Records Management, normal users cannot pass on their rights to other users.

Public services

Security is enforced around public services. Web services, web scripts, Alfresco Explorer and Alfresco Share, CIFS, WebDAV, FTP, CMIS, and more, all use public services, and therefore include security enforcement. Public services are defined in <installLocation>\tomcat\webapps \alfresco\WEB-INF\classes\alfresco\public-services-context.xml.

Access control allows or prevents users or processes acting on behalf of a user, from executing service methods on a particular object by checking if the current user, or any of the authorities granted to the current user, has a particular permission or permission group, or that the user has a particular authority.

For example, on the NodeService bean, the `readProperties` method checks that the current user has Read permission for the node before invoking the method and returning the node’s properties. On the SearchService query method, the results are restricted to return only the nodes for which a user has Read permission.

Public services configuration

Security is enforced in the Spring configuration by defining proxies for each internal service implementation and adding a method interceptor to enforce security for each public service proxy.

These interceptors also have other roles. When a method is called on a public service, the security interceptor is called before the method it wraps. At this stage, the interceptor can examine the function arguments to the method and check that the user has the appropriate rights for each argument in order to invoke the method. For example, a method delete(NodeRef nodeRef) exists on the node service. The security interceptor can see the nodeRef argument before the underlying delete(...) method is called. If configured correctly, the interceptor could check that the current user has "Delete" permission for the node. If they do not have the permission, a security exception is raised. If all the entry criteria are met, the method goes ahead.

In a similar manner, after a method has executed the interceptor can examine the returned object and decide if it should return it to the caller. For example, a search method could return a list of nodes. The security interceptor could filter this list for only those nodes for which the current user has Read permission.

It is also possible to configure a method so that it can be called by all users, only by users with the admin role, or only by specific users or groups. This can also be enforced by the security method interceptor.

Access control interceptor definitions for public services are included in <installLocation>\tomcat \webapps\alfresco\WEB-INF\classes\alfresco\public-services-security-context.xml along with any other supporting beans. This configuration file also defines the location from which the permission model is loaded. The interceptors are wired up to the public services in <installLocation>\tomcat \webapps\alfresco\WEB-INF\classes\alfresco\public-services-context.xml. The public services are the only Spring beans to have access control.

Method-level security definition

The beans required to support Spring ACEGI-based security around method invocation are defined in <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\public-services-security-context.xml. This configures two Alfresco-specific beans: A voter that can authorize method execution based on the permissions granted to the current user for specific arguments to the method, and an after invocation provider to apply security to objects returned by methods.

Method access is defined in the normal ACEGI manner with some additions.

For the following information detailing preconditions and postconditions, these factors are all relevant:

<authority>
Represents an authority (user name or group).

<#>
Represents a method argument index.

<permission>
Represents the string representation of a permission.

Preconditions take one of the following forms:

ACL_METHOD.<authority>
Restricts access to the method to those with the given authority in Alfresco. This could be a user name or group. Dynamic authorities are not supported.

ACL_NODE.<#>.<permission>
Restricts access control to users who have the specified permission for the node at the identified argument. If the argument is a NodeRef, it will be used; if it is a StoreRef, the root node for the store will be used; if it is a ChildAssociationRef, the child node will be used.

ACL_PARENT.<#>.<permission>
Restricts access control to users who have the specified permission for the parent of the node on the identified argument. If the argument is a NodeRef, the parent of the node will be used; if it is a ChildAssociationRef, the parent node will be used.

ROLE
Checks for an authority starting with ROLE_.

GROUP
Checks for an authority starting with GROUP_.

If more than one ACL_NODE.<#>.<permission> , ACL_PARENT.<#>.<permission>, or ACL_METHOD.<permission> entry is present, then all of the ACL_NODE and ACL_PARENT permissions must be present and any one of the ACL_METHOD restrictions, if present, for the method to execute.

Post-conditions take the forms:

AFTER_ACL_NODE.<permission>
Similar to ACL_NODE.<#>.<permission> but the restriction applies to the return argument.

AFTER_ACL_PARENT.<permission>
Similar to ACL_PARENT.<#>.<permission> but the restriction applies to the return argument.

The support return types are:

- StoreRef
- ChildAssociationRef
- Collections of StoreRef, NodeRef, ChildAssociationRef, and FileInfo
- FileInfo
- NodeRef
- Arrays of StoreRef, NodeRef, ChildAssociationRef, and FileInfo
- PagingLuceneResultSet
- QueryEngineResults
- ResultSet

The post-conditions will create access denied exceptions for return types such as NodeRef, StoreRef, ChildAssociationRef, and FileInfo. For collections, arrays, and result sets, their members will be filtered based on the access conditions applied to each member.

Continuing the example from the permissions defined for the Ownable aspect, the definition for the security interceptor for the related OwnableService is shown in the following code snippet.

```
<bean id="OwnableService_security"

 class="org.alfresco.repo.security.permissions.impl.acegi.MethodSecurityInterceptor">
   <property name="authenticationManager"><ref bean="authenticationManager"/></
property>
   <property name="accessDecisionManager"><ref local="accessDecisionManager"/
></property>
   <property name="afterInvocationManager"><ref local="afterInvocationManager"/
></property>
   <property name="objectDefinitionSource">
     <value>

 org.alfresco.service.cmr.security.OwnableService.getOwner=ACL_NODE.0.sys:base.ReadPrope

 org.alfresco.service.cmr.security.OwnableService.setOwner=ACL_NODE.0.cm:ownable.SetOwne

 org.alfresco.service.cmr.security.OwnableService.takeOwnership=ACL_NODE.0.cm:ownable.Ta

 org.alfresco.service.cmr.security.OwnableService.hasOwner=ACL_NODE.0.sys:base.ReadPrope
      org.alfresco.service.cmr.security.OwnableService.*=ACL_DENY
      </value>
    </property>
</bean>
```

Security for the four methods on the OwnableService is defined. To invoke the OwnableService getOwner() method on a node, the invoker must have permission to read the properties of the target node. To set the owner of a node, a user must have been explicitly assigned the SetOwner permission or have all rights to the node. A user may have all rights to a node via the context-free ACL or be assigned a permission, which grants all permission or includes SetOwner. With the default configuration, a user will own any node they create and therefore be able to give ownership to anyone else and possibly not have the right to take ownership back.

The last entry catches and denies access for any other method calls other than those listed. If any additional methods were added to this service and no security configuration explicitly defined for the new methods, these methods would always deny access.

Implementation and services

The following key services are involved in access control:

- PersonService
- AuthorityService
- PermissionService
- OwnableService

The PersonService and the AuthorityService are responsible for managing authorities. The PermissionService is responsible for managing ACLs and ACEs and for checking if a user has been assigned a permission for a particular node. The OwnableService manages object ownership and is used in evaluation the dynamic ROLE_OWNER authority.

The protection of public services methods is implemented using Spring method interceptors defined as part of the related ACEGI 0.8.2 security package. The Alfresco implementation adds new implementations of the ACEGI interfaces AccessDecisionVoter and AfterInvocationProvider, which support the configuration elements that have already been described (for example, ACL_NODE.<#>.<permission>). These extension classes make use of the key services.

Person service

The PersonService interface is the API by which nodes of the person type, as defined in <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\model\contentModel.xml, should be accessed.

The PersonService is responsible for all of the following:

- Obtaining a reference to the Person node for a given user name
- Determining if a person entry exists for a user
- Potentially creating missing people entries with default settings on demand
- Supplying a list of mutable properties for each person
- Creating, deleting, and altering personal information

The beans to support the PersonService and its configuration can be found in <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\authentication-services-context.xml. The principle configuration options are around how people are created on demand if users are managed via NTLM or some other external user repository.

Authority service

The AuthorityService is responsible for:

- Creating and deleting authorities
- Querying for authorities
- Structuring authorities into hierarchies

- Supporting queries for membership
- Finding all the authorities that apply to the current authenticated user
- Determining if the current authenticated user has admin rights
- Managing zones and the assignment of authorities to zones

The authority service does not support user authentication or user management. This is done by the AuthenticationService. Person nodes are managed via the PersonService.

The default implementation allows a list of group names to define both administration groups and guest groups. Each authentication component defines its own default administrative user(s), which can also be set explicitly. The default service is defined in <installLocation>\tomcat \webapps\alfresco\WEB-INF\classes\alfresco\authority-services-context.xml.

Permission service

The PermissionService is responsible for:

- Providing well known permissions and authorities
- Providing an API to read, set, and delete permissions for a node
- Providing an API to query, enable, and disable permission inheritance for a node
- Determining if the current, authenticated user has a permission for a node

The PermissionService interface defines constants for well-known permissions and authorities.

The default implementation coordinates implementations of two service provider interfaces: a ModelDAO and a PermissionsDAO. A permission is simply a name scoped by the fully qualified name of the type or aspect to which it applies. The beans are defined and configured in <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\public-services-security-context.xml. This file also contains the configuration for security enforcement.

The ModelDAO interface defines an API to access a permissions model. The default permission model is in XML and defines permission sets, and their related permission groups and permissions. Global permissions are part of the permission model. There may be more than one permission model defined in XML; they are in practice merged into one permission model. A module can extend the permission model.

The available permissions are defined in the permission model. This is defined in <installLocation>\tomcat\webapps\alfresco\WEB-INF\classes\alfresco\model \permissionDefinitions.xml. This configuration is loaded in a bean definition in <installLocation> \tomcat\webapps\alfresco\WEB-INF\classes\alfresco\public-services-security-context.xml. This file also defines global permissions. The definition file is read once at application start-up. If you make changes to this file, you will have to restart the repository in order to apply the changes.

Ownable service

The idea of file ownership is present in both UNIX and Windows. In Alfresco, the repository has the concept of node ownership. This ownership is optional and is implemented as an aspect.

The owner of a node may have specific ACLs granted to them. Ownership is implemented as the dynamic authority, ROLE_OWNER, and is evaluated in the context of each node for which an authorization request is made. The Ownable aspect, if present, defines a node’s owner by storing a userName; if the Ownable aspect is not present, the creator is used as the default owner. If the userName of the current user matches, including case, the userName stored as the owner of the node, the current user will be granted all permissions assigned to the authority ROLE_OWNER.

The OwnableService is responsible for all of the following:

- Determining the owner of a node

- Setting the owner of a node
- Determining if a node has an owner
- Allowing the current user to take ownership of a node

The OwnableService is supported by an Ownable aspect defined in <installLocation>\tomcat \webapps\alfresco\WEB-INF\classes\alfresco\model\contentModel.xml.

There are permissions and permission groups associated with the Ownable aspect in the permission model and related access controls applied to the methods on the public OwnableService.

Setting up high availability systems

This section describes how to implement multiple Alfresco instances in a high availability configuration.

In a clustered installation, concurrent writes to the same documents using file server protocols (CIFS, FTP, or NFS) are not currently recommended.

High Availability (HA) clusters are implemented in Alfresco to improve the availability of services and to improve performance of these services. Availability is enhanced through redundant nodes that provide services when other nodes fail. When integrated with a load balancer, performance is enhanced by distributing, or balancing, server workload across a collection of nodes.

A cluster represents a collection of nodes. For example, a set up of two tomcat nodes on two separate machines, talking to shared content store, shared database, but each with their own indexes. This is the simplest cluster to set up, gives redundancy due to the two machines, and can load-balance for performance or use the second node as a "hot spare" for fail over.

High availability components

To ensure redundancy during runtime, the following components of the Alfresco system must be replicated and/or synchronized across each cluster:

- Content store
- Indexes
- Database
- Level 2 cache

Content store replication

The underlying content binaries are distributed by either sharing a common content store between all machines in a cluster or by replicating content between the clustered machines and a shared store(s). The common store is simpler and more prevalent.

When using multiple content stores, each cluster stores content and retrieves content from its primary content store. Both content stores share a replicated content store. Content placed in a primary content store is copied to the replicated content store in a process known as outbound replication. The effect is that two copies of the content exist, one in the primary content store and another in the replicated content store.

If a request for that content occurs on another node, the application first looks for the content item in the primary content store of that node. If it is not there, the application looks to the replicated content store.

If inbound replication is configured, the replicated content store copy is then copied to the requesting node’s primary content store.

Index synchronization

Indexes provide searchable references to all nodes in Alfresco. The index store cannot be shared between servers. To keep the indexes up to date, a timed thread updates each index directly from the database when running in a cluster.

When a node is created (this may be a user node, content node, or space node), metadata is indexed and the transaction information is persisted in the database. When the synchronization thread runs on the other nodes in the cluster, the indexes on those nodes are updated using the transaction information stored in the database.

The tables that contain the index tracking information are:

Table	Description
`alf_server`	Each committing server has an entry in this table.
`alf_transaction`	Each write operation to nodes in Alfresco generates a unique transaction ID. The transaction is attached to the entry in the server table. The column `commit_time_ms` ensures that the transactions can be ordered by commit time. A unique GUID (due to historical reasons) is also attached here.
`alf_node`	An entry is created here for each node, including nodes that have been deleted. With each modification, the status is updated to refer to the transaction entry for the committing transaction.

When indexes are updated on a machine (for rebuilding or tracking) the transactions are time-ordered. The server can then determine which nodes have been modified or deleted in a particular transaction.

Database synchronization

It is possible to have co-located databases which synchronize with each other. To use co-located databases, refer to your database vendor documentation.

Level 2 cache replication

The Level 2 (L2) cache provides out-of-transaction caching of Java objects inside the Alfresco system. Alfresco provides support for EHCache. Using EHCache does not restrict the Alfresco system to any particular application server, so it is completely portable.

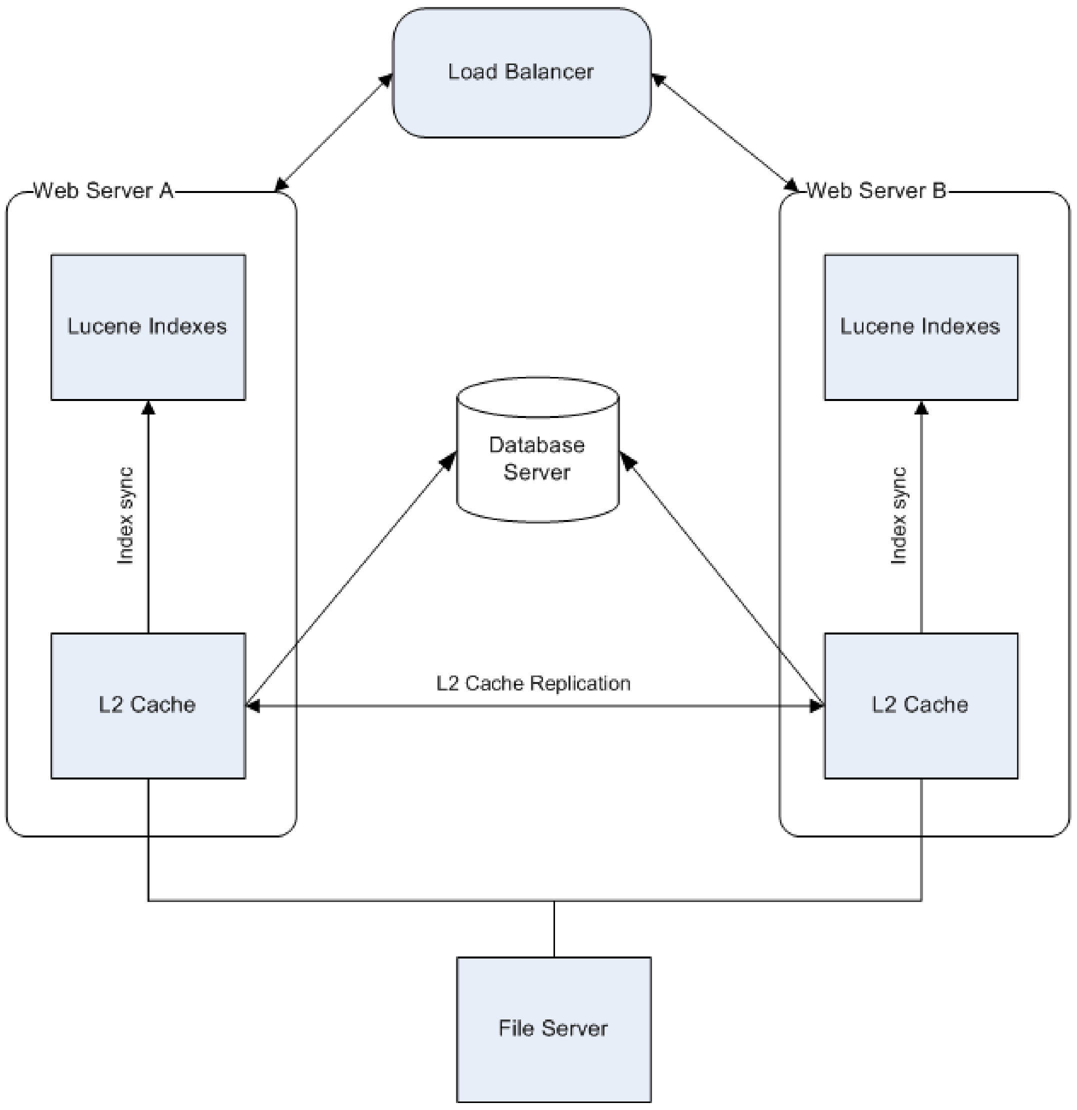
The L2 cache objects are stored in memory attached to the application scope of the server. Sticky sessions must be used to keep a user that has already established a session on one server for the entire session. By default, the cache replication makes use of RMI to replicate changes to all nodes in the cluster using the Peer Cache Replicator. Each replicated cache member notifies all other cache instances when its content has changed.

Level 2 cache is a technology to speed up Hibernate. When the application makes a Hibernate query, it does not have to do a (costly) SQL request if the object is already present in the Level 2 cache. For debugging purposes, you can disable the L2 cache. Hibernate will keep working, but at a slower rate. If you have an issue with EHCache, that is, the cache cluster test fails, you may want to confirm this by disabling the L2 cache setting in the `custom-hibernate-dialect.properties` file. For example:

```
hibernate.cache.use_second_level_cache=false
```

High availability scenario

This scenario shows a single repository database and file system (for the content store) and multiple web application servers accessing the content simultaneously. The configuration does not guard against repository file system or database failure, but allows multiple web servers to share the web load, and provides redundancy in case of a web server failure. Each web server has local indexes (on the local file system).



A hardware load balancer balances the web requests among multiple web servers. The load balancer must support 'sticky' sessions so that each client always connects to the same server during the session. The file system and database will reside on separate servers, which allows us to use alternative means for file system and database replication. The configuration in this case will consist of L2 Cache replication, and index synchronization.

Initiating clustering

Alfresco uses JGroups to send the initial broadcast messages announcing a server's availability. After initial setup, it is possible for a server to enter a cluster by setting the `alfresco.cluster.name` property.

1. Locate the `ehcache-custom.xml.sample.cluster` file.
2. Copy the file, and then name it `ehcache-custom.xml`.
3. Set the required properties using global property overrides (`alfresco-global.properties` file) or system properties (Java command line -D options)
   a. `alfresco.cluster.name`: The name of the cluster.

      This property is mandatory. Without it, neither JGroups nor index tracking will be enabled.

b. Any JGroups properties, especially if the TCP stack is required.
c. `index.recovery.mode`: Set this to AUTO to ensure indexes are refreshed properly on startup.
d. `index.tracking.cronExpression`: This does not need to be set and is 0/5 * * * * ? by default. The index tracking code will not activate unless the cluster name has been set.

4. Configure the content stores.

Additional steps for initiating clustering

These additional steps are required for cluster initiation on Solaris environments and other environments with restricted TCP port ranges and multiple network adapters.

1. Open the `ehcache-custom.xml` file.
2. Remove the following default definition of `cacheManagerPeerListenerFactory`:

```
 <cacheManagerPeerListenerFactory

 class="net.sf.ehcache.distribution.RMICacheManagerPeerListenerFactory"
            properties="socketTimeoutMillis=10000"
            />
```

3. Uncomment the extended definition by removing the comment lines `<!--` and `--!>` before and after the following section:

```
<cacheManagerPeerListenerFactory

 class="net.sf.ehcache.distribution.RMICacheManagerPeerListenerFactory"
            properties="hostName=${alfresco.ehcache.rmi.hostname},
            port=${alfresco.ehcache.rmi.port},

          remoteObjectPort=${alfresco.ehcache.rmi.remoteObjectPort},
          socketTimeoutMillis=
${alfresco.ehcache.rmi.socketTimeoutMillis}" />
```

4. Save the `ehcache-custom.xml` file.
5. Set the following parameters in the `alfresco-global.properties` file:

Parameter	Description
`alfresco.ehcache.rmi.hostname`	The IP address of the network adapter to listen on for the cache invalidation messages.
`alfresco.ehcache.rmi.port`	The fixed port number to which to bind the ehcache RMI registry.
`alfresco.ehcache.rmi.remoteObjectPort`	The fixed port number through which to receive cache invalidation messages.

For example:

```
alfresco.ehcache.rmi.hostname=192.168.40.114
alfresco.ehcache.rmi.port=40001
alfresco.ehcache.rmi.remoteObjectPort=45001
```

Configuring JGroups and Alfresco clustering

This section describes the options available for configuring JGroups and other Alfresco-specific cluster options.

When setting up cluster communications, Alfresco requires servers to discover other instances of Alfresco on a network. In older Alfresco releases, this discovery process used a UDP multicast message (provided by EHCache). Servers in the cluster picked up the message and used the information to set up inter-server communication for inter-cache communication.

To provide a more flexible cluster discovery process, JGroups is integrated into the repository. JGroups is a toolkit for multicast communication between servers. It allows inter-server communication using a highly configurable transport stack, which includes UDP and TCP protocols. Additionally, JGroups manages the underlying communication channels, and cluster entry and exit.

Configuring JGroups

This section describes how to initialize clustering with JGroups. The configuration settings for JGroups clustering are set in a file called`<configRoot>/alfresco/jgroups/alfresco-jgroups-XYZ.xml`, where `XYZ` is the name of the protocol being used.

To initialize JGroups clustering, you must set the following property:

```
alfresco.cluster.name=<mycluster>
```

Where `<mycluster>` is the name used by JGroups to distinguish unique inter-server communication. This allows machines to use the same protocol stacks, but to ignore broadcasts from different clusters.

You can also create a cluster from the Java command line option:

```
-Dalfresco.cluster.name=mycluster
```

1. Open the `alfresco-global.properties` file.
2. Set the general properties for the required protocol stack.

   The general properties for both protocol stacks are:

General property	Description
`alfresco.jgroups.bind_address`	The address to which you bind local sockets.
`alfresco.jgroups.bind_interface`	The interface to which you bind local sockets.

   The default is UDP and is specified in the system `repository.properties` file. The JGroups configuration file is built using the protocol string `alfresco.jgroups.defaultProtocol=UDP`.
3. To select the TCP communication method, add the following property:

   `alfresco.jgroups.defaultProtocol=TCP`
4. Set the property definitions for the chosen stack.

   The default JGroups configuration will probably be adequate. However, the protocol stacks can be redefined completely using any of the standard JGroups transport protocols.

   The properties for the TCP stack are:

TCP property	Description
`alfresco.tcp.start_port`	The port that the server will start listening on. The default is 7800.
`alfresco.tcp.initial_hosts`	A list of hosts and start ports that must be pinged. This can call potential members of the cluster, including the current server and servers that might not be available. The port listed in square brackets is the port to start pinging. The default is `localhost[7800]`. For example: `HOST_A[7800],HOST_B[7800]`

TCP property	Description
`alfresco.tcp.port_range`	The number of increments to make to each host's port number during scanning. Each host has a port number in square brackets, for example, 7800. If the host does not respond to the ping message, the port number will be increased and another attempt made.

The properties for the UDP stack are:

UDP property	Description
`alfresco.udp.mcast_addr`	The multicast address to broadcast on. The default is 230.0.0.1.
`alfresco.udp.mcast_port`	The port to use for UDP multicast broadcasts. The default is 4446.
`alfresco.udp.ip_ttl`	The multicast "time to live" to control the packet scope. The default is 2.

5. (Optional) To specify your own JGroups configuration file, add the following properties:

   ```
   alfresco.jgroups.configLocation=classpath:some-classpath.xml
   alfresco.jgroups.configLocation=file:some-file-path.xml
   ```

   Where `some-file-path` is the name of your configuration file.
6. Save the `alfresco-global.properties` file.

Clustering through shared content stores

This section describes how to configure clustering through shared content stores.

1. Ensure the following stores exist on a shared file system:
   a. Content Store
   b. Audit Content Store
   c. Deleted Content Store
2. Open the `<ClasspathRoot>/alfresco-global.properties` file.
3. Add the following properties:

   ```
   dir.contentstore=<new_location>/contentstore
   dir.contentstore.deleted=<new_location>/contentstore.deleted
   dir.auditcontentstore=<new_location>/audit.contentstore
   ```
4. Save the file.

Using EHCache multicast discovery

This section describes how to configure cluster discovery to use the EHCache multicast. Use this if you do not wish to use JGroups.

1. Open the `<extension>/ehcache-custom.xml` file.
2. Replace the `cacheManagerPeerProviderFactory` with the following:

   ```
   <cacheManagerPeerProviderFactory

    class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFactory"
               properties="peerDiscovery=automatic,
                           multicastGroupAddress=230.0.0.1,
                           multicastGroupPort=4446"/>
   ```

   You must also set the `alfresco.cluster.name` property in order to activate index tracking.

If you have several alfresco clusters on the same network, ensure that the addresses and ports used for Ehcache UDP broadcasts (using the `multicastGroupAddress` and `multicastGroupPort` parameters) are unique to each cluster. If you use the same parameters for all the clusters, each cluster will try to communicate with the other clusters, leading to potential issues.

For example, you may have a testing or validation Alfresco cluster environment and a production Alfresco cluster environment on the same network. When you copy or transfer your testing configuration files to the production environment, you must change the parameters.

3. Save the file.

Verifying the cluster

This section describes how to verify that clustering is working for the various components involved. You will need direct Explorer access to each of the machines in the cluster. The operation is done on machine one (M1) and verified on the other machines (Mx). The process can be switched around with any machine being chosen as M1.

Testing cache clustering

This section describes the steps used to test cache clustering.

1. On M1, login as user `admin`.
2. Browse to the Guest Home space, locate the tutorial PDF document and view the document properties.
3. On Mx, login as `admin`.
4. Browse to the Guest Home space, locate the tutorial PDF document and view the document properties.
5. On M1, modify the tutorial PDF description field, and add `abcdef`.
6. On Mx, refresh the document properties view of the tutorial PDF document.
7. The description field must have changed to include `abcdef`.

Index clustering

This section describes the steps used to test index clustering.

1. Repeat the steps for testing cache clustering.
2. On M1, perform an advanced search of the description field for `abcdef` and verify that the tutorial document is returned.
3. On Mx, search the description field for `abcdef`. Allow time for index tracking (10s or so), and the document will show up in the search results.

Testing content replication and sharing

This section describes the steps used to test content replication and sharing.

1. On M1, add a text file to Guest Home containing `abcdef`.
2. Refresh the view of Guest Home and verify that the document is visible.
3. On Mx, perform a simple search for `abcdef` and ensure that the new document is retrieved.

   This relies on index tracking, so it may take a few seconds for the document to be visible.
4. Open the document and ensure that the correct text is visible.

Testing WCM clustering

This section contains the topics that describes how to test WCM clustering.

Testing web project creation

This section describes the steps used to test the a web project once it is created successfully in the cluster and that any edits are updated.

1. On M1, create a web project, and add only the **Name** and **DNS Name** fields.
2. On M2, verify that the web project is created on M2.
3. On M1, edit the web project by adding values in the **Title** and **Description** fields.
4. On M2, verify the web project title and descriptions.

Testing web project data node synchronization

This section describes the steps used to test the synchronization between web project data nodes.

1. On M2, stop the Alfresco server.
2. On M1, import the sample website `alfresco-sample-website.war` into the `admin` user sandbox.
3. On M2, start the Alfresco server.
4. On M2, after synchronization time, browse the web project through the `admin` user sandbox and open `robots.txt` from the website root.

Testing web project user invite

This section describes the steps used to test the creation of a user on one machine and the invitation of that user to a web project on another machine.

1. On M1, create a new user.
2. On M2, invite the new user to a web project.
3. On M1, show all sandboxes and observe the new user's sandbox.

Configuring the cache peer URLs

This section describes how to control the cache peer URLs.

If the cache clustering tests fail, enable debug so that you can track the issues. Refer to Tracking clustering issues on page 199.

If the cache peer URLs generated do not contain the correct host name or IP address of the sending server, then other machines will not be able to connect back. This occurs when the JVM call to get the current host name produces an incorrect result. That is, a host name that is not recognized in the cluster (this is typically `localhost`). This can be resolved at a system level, but can also be changed for the Alfresco cluster.

To change the host name and/or port values that the caches broadcast to the cluster:

1. Open the `ehcache-custom-xml` file.

   This file is created when initiating the cluster by making a copy of the `ehcache-custom.xml.sample.cluster` file and calling it `ehcache-custom-xml`.
2. Locate the cacheManagerPeerProviderFactory definition.
3. Comment out the `cacheManagerPeerListenerFactory` definition, and uncomment the second `cacheManagerPeerListenerFactory` definition.

   This extended definition allows additional properties to be set.

4. Set the additional properties in the `alfresco-global.properties` file.

   For example, set the host name of the current server using the following property setting:

   ```
   alfresco.ehcache.rmi.hostname=1.2.3.4
   ```

   This should be set to the IP address that other cluster members should use to communicate with this node.

   The other properties available are:

   remoteObjectPort

   This is the port number on which the remote nodes registry receive messages. The default is 0 (zero) which will select a free port.

   port

   The port that this node listens on. The default is 0 (zero) which will select a free port.

   socketTimeoutMillis

   The number of ms client sockets will stay open when sending messages to remote nodes. The default is 5 seconds, which should be long enough.

5. If the debug logging shows that the IP address or host name being sent or received by JGroups is wrong, set the JGroups bind address to the address that other members of the cluster should use to communicate with this node (`alfresco.jgroups.bind_address`). Refer to Configuring JGroups on page 195.

Tracking clustering issues

This section describes how to track issues with clustering in a high availability environment.

1. Enable the following log categories:

   - `log4j.logger.net.sf.ehcache.distribution=DEBUG`

     Check that heartbeats are received from from live machines.

   - `log4j.logger.org.alfresco.repo.node.index.IndexTransactionTracker=DEBUG`

     Remote index tracking for Alfresco DM.

   - `log4j.logger.org.alfresco.repo.node.index.AVMRemoteSnapshotTracker=DEBUG`

     Remote index tracking for AVM.

2. Enable the following JGroups logs:

   - `log4j.logger.org.alfresco.repo.jgroups=debug`

     `log4j.logger.org.alfresco.enterprise.repo.cache.jgroups=debug`

     Checks heartbeat messages sent and received by machines in the cluster, and watches the entry and exit of cluster members.

3. If cache clustering is not working, the EHCache website describes some common problems. The remote debugger can be downloaded as part of the EHCache distribution files and executed:

   ```
   > java -jar ehcache-1.3.0-remote-debugger.jar
   Command line to list caches to monitor: java -jar ehcache-remote-
   debugger.jar path_to_ehcache.xml
   Command line to monitor a specific cache: java -jar ehcache-remote-
   debugger.jar path_to_ehcache.xml cacheName
   ```

Backing up and restoring

This section describes the process for backing up the Alfresco content repository. It assumes that the various binaries (operating system, database, JDK, application server, and so on.) and configuration files (operating system, database, JDK, application server, Alfresco, and so on) are being backed up independently.

Your backup strategy must be tested end-to-end, including restoration of backups that were taken previously. Ensure that you have adequately tested your backup scripts prior to deploying Alfresco to production.

Backing up and restoring the repository

Backing up an Alfresco repository involves backing up the following:

- The directory pointed to by the `dir.root` setting
- The database Alfresco is configured to use

To restore the backup successfully, the directory and database must be backed up as a single unit. When you restore an Alfresco backup, you must restore both the `dir.root` directory and the Alfresco database from the same backup set. Otherwise, the repository will be corrupted.

The `dir.root` directory is defined in the `alfresco-global.properties` file. By default, this directory is named `alf_data` and is located within the directory where Alfresco is installed.

Performing a cold backup

By default, the `dir.root` contains both the content and indexes. For a cold backup, you can back up just the content and perform a full reindex when a backup is restored. A full reindex can be a time consuming process, so the steps include the indexes in the backup.

1. Stop Alfresco.
2. Back up the database Alfresco is configured to use, using your database vendor's backup tools.
3. In parallel, back up the `dir.root` directory in its entirety.
4. Store both the database and `dir.root` backups together as a single unit.

   For example, store the backups in the same directory or compressed file.
5. Start Alfresco.

Performing a hot backup

This section describes the procedure for performing at hot backup.

The high-level procedure for a hot backup is:

1. Back up Lucene.
2. Back up SQL.
3. Back up files.

Lucene indexes have to be backed up first and before SQL because if new rows are added in SQL after the lucene backup is done, a lucene reindex (AUTO) can regenerate the missing Lucene indexes from the SQL transaction data.

SQL has to be done before backing up the files because if you have a SQL node pointing to a missing file, then that node will be orphan. Also, if you have a file without SQL node data, this just means that the user has added the file too late to be included in a backup.

It is critical to perform hot backups in the following order of steps:

1. Ensure that you have a `backup-lucene-indexes` directory under `dir.root`.
2. Backup the database Alfresco is configured to use, using your database vendor's backup tools

3. As soon as the database backup completes, backup specific subdirectories in the file system Alfresco `dir.root`
4. Store both the database and Alfresco `dir.root` backups together as a single unit.

   For example, store the backups in the same directory or in a single compressed file. Do not store the database and `dir.root` backups independently, as that makes it difficult to reconstruct a valid backup set, if restoration becomes necessary.
5. Store both the database and `dir.root` backups together as a single unit.

   Ensure that the cron generated in the `backup-lucene-indexes` does not run while you do the SQL backup. The `backup-lucene-indexes` generation should be finished when you start the SQL backup.

Alfresco includes a background job responsible for backing up the Lucene indexes that (by default) is configured to run at 3am each night. The hot backup process must not run concurrently with this background job, so you should either ensure that the hot backup completes by 3am, or wait until the index backup job has completed before initiating a hot backup.

Refreshing the backup Lucene indexes (optional)

This is an optional step before initiating a hot backup.

1. Trigger a Lucene index backup using JMX, and it can be done several ways, including using:

   The backup can be done in several ways, including:

   - VisualVM
   - JConsole (MBeans tab `-gt Alfresco/Schedule/DEFAULT/MonitoredCronTrigger/indexBackupTrigger/Operations` - **executeNow** button)
   - Command line

   During the creation of the backup Lucene indexes, the system is placed in read-only mode, which could last several minutes depending on the size of the Lucene indexes.
2. After completing this operation, the `backup-lucene-indexes` directory contains an up-to-date cold copy of the Lucene indexes, ready to be backed up.

Backing up the database

In an Alfresco system, the ability to support hot backup is dependent on the hot backup capabilities of the database product Alfresco is configured to use.

Database hot backup requires a tool that can "snapshot" a consistent version of the Alfresco database (that is, it must capture a transactionally-consistent copy of all the tables in the Alfresco database). In addition, to avoid serious performance problems in the running Alfresco system while the backup is in progress, this "snapshot" operation should either operate without taking out locks in the Alfresco database or it should complete quickly (within seconds).

Backup capabilities vary widely between relational database products, and you should ensure that any backup procedures that are instituted are validated by a qualified, experienced database administrator before being put into a production environment.

Backing up the file system

This section describes the process for backing up the file system.

1. Backup the following subdirectories of the Alfresco `dir.root` directory using whatever tools you are comfortable with (`rsync`, `xcopy`):

    - `contentstore`
    - `contentstore.deleted`
    - `audit.contentstore`
    - `backup-lucene-indexes`

    Do not attempt to backup the `lucene-indexes` subdirectory while Alfresco is running. This will cause Lucene index corruption. Use `backup-lucene-indexes` instead.

Backing up and restoring Lucene indexes

This section describes how to back up and restore the Lucene indexes.

Lucene is a text search engine library written entirely in Java. It is used within Alfresco for full-text search.

Changing the scheduled Lucene back up time

This section describes how to set the time that the scheduled backup of the Lucene indexes occurs.

1. Copy the following file:

    `<configRoot>/alfresco/scheduled-jobs-context.xml`
2. Locate the `<extension>` directory, and paste the copied file into this location.
3. Rename the file to `custom-scheduled-jobs-context.xml`.

    As your override file ends with `-context.xml`, you do not need to point to your file.
4. Delete each pair of `<bean> </bean>` tags (excluding the pair containing the `indexBackupTrigger` bean).

    This bean contains the following properties:

```
<!-- trigger at 3am each day -->
        <property name="cronExpression">
            <value>0 0 3 * * ?</value>
        </property>
```

    The default is to run the job at 3am every day.
5. Modify the `cronExpression` values, if required

    The value `0 0 3 * * ?` specifies the backup is triggered at 3am every day.

    After each backup scheduled in the `indexBackupTrigger` bean, perform your normal backup of this directory.

    Each backup will overwrite the existing backup.

Specifying the Lucene backup directory

This section describes how to specify the Lucene backup directory.

The Lucene directories are backed up under the default `dir.root` directory.

1. Browse to the following file:

    `<configRoot>/alfresco/core-services-context.xml`
2. Locate the `<extension>` directory, and paste the copied file into this location.

3. Open the `core-services-context.xml` file, and then locate the following bean:

   `luceneIndexBackupComponent`

   The `targetLocation` property contains the backup location, with the default value `<dir.root>/backup-lucene-indexes`.

Restoring the Lucene indexes

In addition to full restorations, you can also use the backup sets created through either the cold or hot backup procedures to restore just the Lucene indexes. This is useful where the repository itself does not need to be restored but for some reason the Lucene indexes are stale and rebuilding them from scratch is undesirable.

1. Stop the Alfresco server.
2. Move the existing `dir.root/lucene-indexes` directory to another location.
3. Perform the following, depending on whether you are doing a hot or cold backup:
   - For cold backups, restore `dir.root/lucene-indexes` from the most recent backup step.
   - For hot backups, restore `dir.root/backup-lucene-indexes` from the most recent backup step and rename it to `dir.root/lucene-indexes`.
4. Restart the Alfresco server.

   Upon restarting, Alfresco will detect that the indexes are stale, and incrementally reindex just the content that has changed since the last backup. As the size of your content set grows, the time savings from performing incremental reindexing rather than full reindexing will become greater and greater. Incremental reindexing is typically measured in minutes, whereas full reindexing can take hours for large content sets.

   For incremental reindexing to occur properly, leave the `index.recovery.mode` property at its default value of `AUTO` to ensure that the restored Lucene indexes are incrementally built with any newer transactions in the database and contentstore. Setting this property to `FULL` forces a full reindex, even if incremental reindexing is possible, negating any benefits from this procedure. If a full rebuild is required, it is quicker to delete the existing index.

Exporting and importing

This section describes how to export and import information from a repository, and then import that information into either the same or another repository.

Export and import is useful for:

- Bulk extraction and loading of personal or team information from one location to another
- Integration with third party systems

- You can only perform an export/import between compatible versions of Alfresco, which generally means the same version
- You should not perform an upgrade (Versions 2.x-3.x) using export/import
- It is not recommended that you backup and restore personal, team, or complete repository scope

The export procedure produces one or more Alfresco Content Package (ACP) files, which hold the exported information. As with all files, you can place them somewhere secure, or transfer them using methods, such as email, FTP, and so on. The scope of information to export is configurable, but typically involves specifying the location within the repository to export. The hierarchical nature of the repository means that every item within that location is exported. For example, exporting the folder **My Documents** will export the folder, its contents, and all sub-folders. Security settings allow the export of only those items that are readable by the user performing the export.

Import of an ACP file is the reverse of an export. The information held in the ACP file is placed into the repository location chosen at import time. By default, the import process creates a copy of the ACP held information.

Alfresco Content Package files

An Alfresco Content Package (ACP) is a single file (with an extension of `.acp`) that bundles together the metadata and content files for the information to be transported.

An ACP file is a ZIP archive whose structure is as follows:

```
/<packagename>.xml
/<packagename>/
   contentNNN.pdf
   contentNNN.txt
   ...
```

The `packagename` is assigned on export.

`<packagename>.xml` contains an XML rendition of the transported information in the form of repository nodes. There is no restriction on the information types that can be transported but typically a bundle contains folders and files. Other information types may include forums, rules, preferences, tasks, or anything that is described by a repository content model.

The XML conforms to the export and import view schema, which describes the transported nodes in terms of their types, aspects, properties, associations, and permissions. Content properties are handled specifically where the binary content of the property is held in a separate file under the `packagename` directory of the ZIP archive, and the XML contains a reference to the file.

Although the repository provides different ways to create an ACP file (that is, to export), it is also possible to manually create one using any means. This is very useful for system to system integration.

Exporting spaces in Explorer

You can export any spaces and content in Alfresco Explorer to which you have access. However, you can only import and export from the same version.

1. In Alfresco Explorer, browse to the space you want to export.
2. To export the space, either:
   - Click the **Administration Console** icon, and then click **Export**, or
   - Click **View Details**, and in the **Actions** list, click **Export**
3. In Package Name, specify a name for the file.
4. Choose **Click here to select the destination**.
5. Navigate the spaces to select a destination space for your file.
6. Select the **Current space** option.
7. Check at least one of the boxes for **Include Children** and **Include this Space**.

   Children means everything that you see in the Browse Spaces and Content Items panes.
8. Optionally, check **Run export in background**.
9. Click **OK**.
10. Click **Close**.

    Browse to the space that you specified as the destination to see the `.acp` export file.

After exporting an ACP file, you should move it to a secure location.

Importing spaces in Explorer

You can import to any spaces and content in Alfresco Explorer to which you have access.

1. In Alfresco Explorer, browse to the space into which you want to import.
2. To import a space, either:
   - Click the **Administration Console** icon, and then click **Import**, or
   - Click **View Details**, and in the **Actions** list, click **Import**
3. In the Import pane, browse to the location of the `ACP` file you want to import.
4. Click **Upload**.
5. Optionally, check **Run import in background**.
6. Click **OK**.
7. Click **Close**.

The information from the ACP file now resides in the destination space.

Using rules to import to a space

You can use a rule in a space to import a file to the same space or to another space in which you have permissions.

1. Browse to the space into which you want to import.
2. Click **More Actions**.
3. In the menu, click **Manage Content Rules**.
4. Click **Create Rule** to open the Create Rule Wizard.
5. In the Select Condition menu, click **Items which contain a specific value in its name**.
6. Click **Set Values and Add**.
7. In File name pattern, type `*.acp`.
8. Click **OK**, and then click **Next**.
9. In Select Action, click **Import an Alfresco content package**.
10. Click **Set Values and Add**.
11. In Import To, click the space to which you want to import.
12. Click **OK** twice, and then click **Next** to open the Enter Details pane.
13. In the Type menu, click **Inbound**.
14. In Title, type a meaningful name for the rule to identify the rule from any other rules that might apply in the space.
15. In Description, type a meaningful description that allows other users to understand what the rule does.
16. Deselect **Apply rule to sub spaces**.
17. Check **Run rule in background**.
18. Click **Next**, and then click **Finish**.

Test the rule by inserting an `ACP` file in the space that corresponds to space containing the import rule. The import process starts and places the items held in the ACP file into the destination folder specified with "Import To".

The import will be initiated regardless of how the ACP file was placed into the folder. For example, the import will initiate if the ACP file was placed there using CIFS, FTP, WebDAV, Explorer, or API. This is particularly powerful for system to system data integration.

Creating and managing workflows

This section contains steps for creating a workflow process definition and task model.

What is workflow?

A workflow is a work procedure and workflow steps that represent the activities users must follow in Alfresco to achieve a desired outcome. You can define your own content-oriented workflows. Alfresco provides two different types of workflow: simple workflow and advanced workflow.

Simple workflow

Simple workflow defines content rules for a space. The content rule dictates how the content entering, leaving, or currently residing in the space is managed. Each workflow definition is restricted to a single state.

Advanced workflow

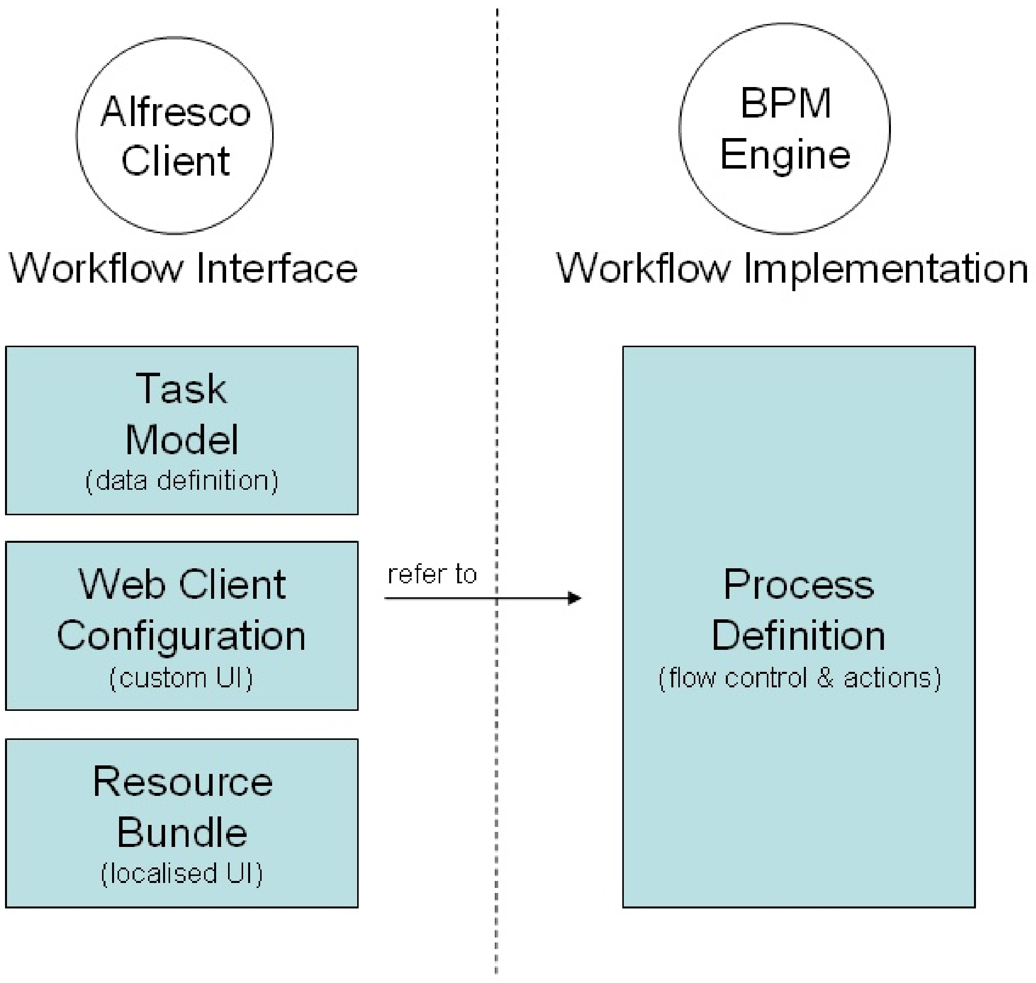
Advanced workflow is any workflow constructed using the Alfresco embedded workflow engine. Alfresco includes two out-of-the-box workflows, which are both basic examples of advanced workflows:

- Adhoc Task (for assigning a task to a colleague)
- Review & Approve (for setting up review and approval of content)

In both examples, the content items are attached to the workflow.

Advanced workflow artifacts

An Alfresco "advanced" workflow comprises the following artifacts.


Alfresco Client
Workflow Interface
Task Model (data definition)
Web Client Configuration (custom UI)
Resource Bundle (localised UI)
refer to
BPM Engine
Workflow Implementation
Process Definition (flow control & actions)

Administration features

Three workflow administration features are available.

These are:

- Workflow Definition Language
- Workflow Interfaces
- Workflow Tools

Implementation

This section describes the way that workflow is implemented in Alfresco.

- Workflows are defined using jPDL process language.
- You can create process definitions manually in XML files or you can create the definitions graphically using the JBoss jBPM Process Designer. These definitions are automatically saved in XML files.
- You can specify the content of the workflow task dialogs that will be displayed in the UI.
- Workflow definitions are easily localizable.
- Optionally, you can use Process Designer to deploy the process definitions to the Alfresco server in real time.

Creating a process definition

The process definition allows you to do the following:

- Group tasks into task nodes
- Assign task nodes to people using swimlanes (example)
- Define system actions that can occur during the transition from one task node to the next

Process definition methods

A process definition can be either an XML file or a process archive. Both of these can be created using jBPM Process Designer. You can also create the XML file manually.

The Process Designer allows you to switch between diagram mode and XML editor mode. This means that you can initially create a file using diagram mode, then switch to editor mode for viewing and fine tuning.

When you redeploy updated process definitions, you can do so manually or using the Process Designer. In either case, the previously deployed process definition is versioned and kept alive to allow existing “in-progress” workflows to continue executing.

Creating a skeleton process definition manually

The high-level parts of the process definition are shown in the Adhoc task example. The complete process definition is shown in the Process definition for an ad hoc task.

Assume that the person who starts the workflow is **initiator**, and the person who is assigned the workflow is **assignee**.

The initiator can specify the following information through the UI:

- Task description
- Due date (optional)
- Priority
- Request for email notification of task completion (optional)

Setting up JBoss jBPM Process Designer

This section describes the two ways to set up Process Designer.

- Download and install a single zipped file from the Alfresco website. This will install a new, standalone Process Designer.

or

- Do the steps manually. You might do this if you want to embed jBPM Process Designer in your own Eclipse. In this case, you need Eclipse 3.2 (or later).

Installing the Process Designer package

The Process Designer is a zipped file that contains the following:

- Eclipse 3.2.1
- jBPM 3.1.2
- jBPM Process Designer 3.0.11
- Eclipse projects for the following workflows: Review & Approve; Ad hoc Task

Unzip the file to any `<install>` folder. There is a ReadMe file in the root of the `<install>` folder with installation and configuration instructions.

Deploying Eclipse

This task describes how to download and install Eclipse.

1. Download **Eclipse SDK 3.2** from http://www.eclipse.org/downloads.
2. Unzip the downloaded file in the required directory.
3. To run Eclipse, follow the advice in the release notes, `readme_eclipse.html`.

The following are good sources for Eclipse information:

- http://www.cs.laurentian.ca/badams/c1047/eclipse-tutorials/index.html
- http://eclipse-tutorial.dev.java.net/http://eclipse-tutorial.dev.java.net/
- http://wiki.eclipse.org/index.php/Eclipse_FAQs

Deploying JBoss jBPM 3.1.2

This task describes how to download and install JBoss jBPM.

Documentation for JBoss jBPM is located at:

- http://docs.jboss.com/jbpm/v3/userguide/
- http://docs/jboss/com/jbpm/v3/gpd/

1. Download JBoss jBPM 3.1.2 from:

   http://www.jboss.com/products/jbpm/downloads
2. Unzip the downloaded file in the required directory.
3. Start Eclipse.
4. Ensure you are in the correct workspace.
5. Click **File** > **Import**.
6. In the Select dialog box, click **General > Existing projects into workspace**.
7. Click **Next**.
8. In the Import Projects dialog box, enable **Select root directory**.
9. Browse to the jBPM root directory, for example, `jbpm-3.1.2`.
10. Enable **Copy projects into workspace**.

Creating a task model

Perform this task to create a task model, which is similar to a content model.

1. Derive your model from the base task model:
   - `<import uri="http://www.alfresco.org/model/bpm/1.0" prefix="bpm"/>`
2. For each `<task>` in the process definition, create a `<type>` in the task model. `<type name>` must be identical to `<task name>`:
   - `<type name="wf:submitAdhocTask">`
   - `<type name="wf:adhocTask">`
   - `<type name="wf:completedAdhocTask">`
3. For each type, describe the properties:
   - `<property name="wf:notifyMe">`
4. For each type, define aspects:
   - `<aspect>bpm:assignee</aspect>`

You do not need to create an association for `initiator`. `initiator` is a process instance variable that is available in any workflow. `initiator` is a repository node (cm:person) that represents the person who initiated the workflow.

5. Add the details for properties and associations.

Deploying the task model

This section describes the methods to deploy a task model.

You can deploy a task model in two ways:

- Using the workflowDeployer bean
- Deploying as a content model

Using the workflowDeployer bean

A workflow task model may be deployed using the workflowDeployer bean.

```
<bean id="myworkflows.workflowBootstrap" parent="workflowDeployer">
   <property name="workflowDefinitions">
      ...
   </property>
   <property name="models">
      <list>
         <-- Task Model associated with above process definition -->
         <value>alfresco/workflow/adhocModel.xml</value>
      </list>
   </property>
</bean>
```

Deploying as a content model

The task model is a content model, so it may be deployed like any other content model.

An example configuration snippet follows:

```
<bean id="adhocWorkflow.dictionaryBootstrap" parent="dictionaryModelBootstrap"
 depends-on="dictionaryBootstrap">
   <property name="models">
      <list>
         <value>alfresco/model/adhocTaskModel.xml</value>
      </list>
   </property>
</bean>
```

Adding behavior to a process definition

You can add behavior to a process definition to describe the data flow, task assignments, and repository actions.

Based on the task model, the complete process definition is shown in the following code snippet.

Note:

- The swimlane assignee is mapped to the process variable `bpm_assignee`.
- A task-create event is used to initialize the due date and priority of the ad hoc task.
- The ad hoc task completed transition event is used to call Alfresco JavaScript that sends an email.

  If you have a JavaScript that returns details of the host, for example, the protocol, the host name, and the port, use the sysAdmin subsystem properties to specify these values.

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  ```

```
<process-definition xmlns="urn:jbpm.org:jpdl-3.1" name="wf:adhoc">

  <swimlane name="initiator"/>

  <start-state name="start">
    <task name="wf:submitAdhocTask" swimlane="initiator"/>
    <transition name="" to="adhoc"/>
  </start-state>

  <swimlane name="assignee">
    <assignment actor-id="#{bpm_assignee.properties['cm:userName']}"/>
  </swimlane>

  <task-node name="adhoc">
    <task name="wf:adhocTask" swimlane="assignee">
      <event type="task-create">
        <script>
          if (bpm_workflowDueDate != void)
          {
            taskInstance.dueDate = bpm_workflowDueDate;
          }
          if (bpm_workflowPriority != void)
          {
            taskInstance.priority = bpm_workflowPriority;
          }
        </script>
      </event>
    </task>
    <transition name="" to="completed">
      <action class="org.alfresco.repo.workflow.jbpm.AlfrescoJavaScript">
        <script>
          if (wf_notifyMe)
          {
            var mail = actions.create("mail");
            mail.parameters.to = initiator.properties["cm:email"];
            mail.parameters.subject = "Adhoc Task " +
 bpm_workflowDescription;
            mail.parameters.from = bpm_assignee.properties["cm:email"];
            mail.parameters.text = "It's done";
            mail.execute(bpm_package);
          }
        </script>
      </action>
    </transition>
  </task-node>

  <task-node name="completed">
    <task name="wf:completedAdhocTask" swimlane="initiator"/>
    <transition name="" to="end"/>
  </task-node>

  <end-state name="end"/>

  <event type="process-end">
     <action class="org.alfresco.repo.workflow.jbpm.AlfrescoJavaScript">
        <script>
           if (logger.isLoggingEnabled())
              logger.log("End of process.  Cancelled: " + cancelled);
        </script>
     </action>
  </event>


</process-definition>
```

Notes about the code snippet:

- The swimlane `assignee` is mapped to the process variable `bpm_assignee`

- A task-create event is used to initialize the due date and priority of the ad-hoc task
- The adhoc task completed transition event is used to call Alfresco JavaScript that sends an email
- A process-end event is used to log the end of the workflow

Configuring UI workflow dialogs

Dialogs are used in Explorer to present tasks to users.

You can modify default dialogs to:

- Control which task properties display.
- Control which task properties are read-only and mandatory.
- Control how each task property is rendered in the dialog.
- Present a custom dialog for each kind of task in the workflow.

Alfresco Explorer already provides a sophisticated configuration mechanism for controlling dialogs. This same mechanism extends to workflow tasks.

Process definition deployment

You can deploy a process definition manually or use the Process Designer.

For manual deployment, the Alfresco server must be shut down. Process definitions are deployed when Alfresco starts.

Deploying a process definition manually

You can use the `workflowDeployer` bean to deploy process definitions (refer to the following code snippet).

The bean must be in a file in the `<extension>` directory.

```
<bean id="myworkflows.workflowBootstrap" parent="workflowDeployer">
  <property name="workflowDefinitions">
    <list>
      <props>
        <prop key="engineId">jbpm</prop>
        <prop key="location">alfresco/workflow/adhoc_processdefinition.xml</
prop>
        <prop key="mimetype">text/xml</prop>
      </props>
    </list>
  </property>
</bean>
```

Deploying a process definition

Use the JBoss jBPM Process Designer to save a process definition to a process archive file or to deploy directly to an existing server. Alfresco supports deployment directly to Alfresco.

1. Enable the jBPM Deploy Process Servlet by adding the following setting to the `alfresco-global.properties` file:

   `system.workflow.deployservlet.enabled=true`

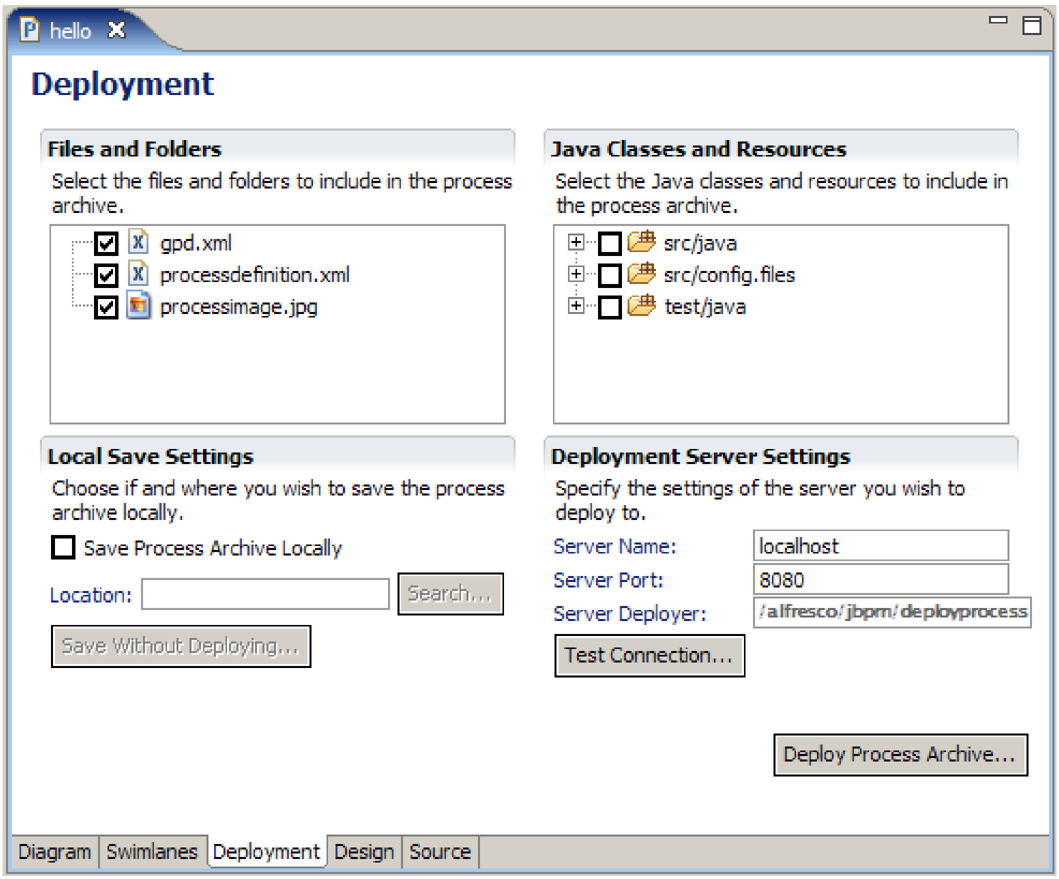
   This allows you to upload workflows directly into Alfresco; however, this setting is not recommended in a production environment because it allows unauthenticated deployment of new workflows.
2. Restart the Alfresco server.

3. At the bottom of the Process Designer window, click the **Deployment** tab.
4. In the **Deployment Server Settings** block in the **Server Name** field, enter the name of the machine where Alfresco is installed.
5. In the **Server Port** field, enter the port number assigned to Alfresco (default: 8080).
6. In the **Server Deployer** field, enter `/alfresco/jbpm/deployprocess`.
7. Click **Test Connection**.
8. If the test is successful, click **Deploy Process Archive**.

   You do not need to restart the Alfresco server to activate the newly deployed process definition. Using the jBPM Process Designer allows quick turnaround while testing new process definitions.

The process definition is now available for use by Alfresco.

The following image shows using the Process Designer to deploy a process definition.



hello

Deployment

Files and Folders

Select the files and folders to include in the process archive.

- [✓] gpd.xml
- [✓] processdefinition.xml
- [✓] processimage.jpg

Java Classes and Resources

Select the Java classes and resources to include in the process archive.

- [ ] src/java
- [ ] src/config.files
- [ ] test/java

Local Save Settings

Choose if and where you wish to save the process archive locally.

[ ] Save Process Archive Locally

Location:

Search... | Save Without Deploying...

Deployment Server Settings

Specify the settings of the server you wish to deploy to.

Server Name:	localhost
Server Port:	8080
Server Deployer:	/alfresco/jbpm/deployprocess

Test Connection... | Deploy Process Archive...

Diagram | Swimlanes | Deployment | Design | Source

Managing the content store

The Content Store Selector provides a mechanism to control the store used for the content file associated with a particular content item.

By applying the `cm:storeSelector` aspect and setting its `cm:storeName` property to the name of a selectable store, the content will be automatically moved from its current location to the new store. The store does not, therefore, store content itself, it defines and manages those stores that are available for selection.

This allows storage polices to be implemented to control which underlying physical storage is used, based on your applications needs or business policies. For example, if you have a fast (and expensive) local disk, you can use this to store the files that you want to ensure are served for best performance; however, infrequently used files may be stored on lower cost, slower storage.

Content store selector configuration example

The following example defines two file stores, in addition to the standard default file store. By setting the `cm:storeName` property to either of these new stores or the default store, the content is automatically moved from its existing store to the relevant new store.

A summary of the procedure is as follows:

1. Create a file called `sample-content-store-selector-context.xml` in the `extension` directory.
2. Define two new file stores.
3. Declare a `storeSelectorContentStore` to be the system's primary content store.
4. Declare the mapping between the store name and store instances.
5. Add the extra stores to the list to be handled by the `eagerContentStoreCleaner`.

1. Open the `sample-content-store-selector-context.xml` file.
2. Define the new file stores by adding the following bean definitions:

   ```
   <bean id="firstSharedFileContentStore"
    class="org.alfresco.repo.content.filestore.FileContentStore">
      <constructor-arg>
         <value>${dir.root}/storeA</value>
      </constructor-arg>
   </bean>

   <bean id="secondSharedFileContentStore"
    class="org.alfresco.repo.content.filestore.FileContentStore">
      <constructor-arg>
         <value>${dir.root}/storeB</value>
      </constructor-arg>
   </bean>
   ```

   This configuration snippet defines two new stores. The physical location is relative to the `dir.root` property defined in the `alfresco-global.properties` file.
3. Declare the `storeSelectorContentStore` to be the primary content store by adding the following bean definition:

   ```
   <bean id="contentService" parent="baseContentService">
      <property name="store">
          <ref bean="storeSelectorContentStore" />
      </property>
   </bean>
   ```
4. Declare the mapping between store names and store instances.

   ```
   <bean id="storeSelectorContentStore"
    parent="storeSelectorContentStoreBase">
          <property name="defaultStoreName">
               <value>default</value>
          </property>
          <property name="storesByName">
              <map>
                  <entry key="default">
                      <ref bean="fileContentStore" />
                  </entry>
                  <entry key="storeA">
                      <ref bean="firstSharedFileContentStore" />
                  </entry>
                  <entry key="storeB">
                      <ref bean="secondSharedFileContentStore" />
                  </entry>
   ```

```
            </map>
         </property>
     </bean>
```

The list of stores is defined by the `<property name="storesByName">` property. Any stores you want to be available to the `storeSelectorContentStore` should be listed under this property.

Using the new content store

The new content store is set using the `cm:storeName` property.

The `cm:storeName` property can be set in number of ways:

- Manually, by exposing this property so its value can be set by either Explorer or Share
- Running a script action that sets the `cm:storeName` property value within the script
- Using a rule that runs a script action to set the property

The expected behavior is as follows:

- When the `cm:storeSelector` aspect is not present or is removed, the content is copied to a new location in the 'default' store
- When the `cm:storeSelector` aspect is added or changed, the content is copied to the named store
- Under normal circumstances, a trail of content will be left in the stores, just as it would be if the content were being modified. The normal processes to clean up the orphaned content will be followed.

Content Store Selector full configuration example

The following example shows the full definition of creating new stores using the Content Store Selector.

This configuration must be saved an a extension, for example, `<extension>\sample-content-store-selector-context.xml`.

The list of stores available can be set by updating the list under the `<property name="storesByName">` property.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE beans PUBLIC '-//SPRING//DTD BEAN//EN' 'http://
www.springframework.org/dtd/spring-beans.dtd'>

<beans>

   <bean id="firstSharedFileContentStore"
 class="org.alfresco.repo.content.filestore.FileContentStore">
      <constructor-arg>
         <value>${dir.root}/storeA</value>
      </constructor-arg>
   </bean>

   <bean id="secondSharedFileContentStore"
 class="org.alfresco.repo.content.filestore.FileContentStore">
      <constructor-arg>
         <value>${dir.root}/storeB</value>
      </constructor-arg>
   </bean>

   <bean id="storeSelectorContentStore" parent="storeSelectorContentStoreBase">
       <property name="defaultStoreName">
```

```
            <value>default</value>
       </property>
       <property name="storesByName">
           <map>
               <entry key="default">
                   <ref bean="fileContentStore" />
               </entry>
               <entry key="storeA">
                   <ref bean="firstSharedFileContentStore" />
               </entry>
               <entry key="storeB">
                   <ref bean="secondSharedFileContentStore" />
               </entry>
          </map>
       </property>
   </bean>

<!-- Point the ContentService to the 'selector' store -->
   <bean id="contentService" parent="baseContentService">
      <property name="store">
         <ref bean="storeSelectorContentStore" />
      </property>
   </bean>

   <!-- Add the other stores to the list of stores for cleaning -->
   <bean id="eagerContentStoreCleaner"
 class="org.alfresco.repo.content.cleanup.EagerContentStoreCleaner" init-
method="init">
      <property name="eagerOrphanCleanup" >
         <value>${system.content.eagerOrphanCleanup}</value>
      </property>
      <property name="stores" >
         <list>
            <ref bean="fileContentStore" />
            <ref bean="firstSharedFileContentStore" />
            <ref bean="secondSharedFileContentStore" />
         </list>
      </property>
      <property name="listeners" >
         <ref bean="deletedContentBackupListeners" />
      </property>
   </bean>

</beans>
```

The following example shows the web-client-config-custom.xml file:

```
 <!-- Configuring in the cm:storeSelector aspect -->
   <config evaluator="aspect-name" condition="cm:storeSelector">
      <property-sheet>
         <show-property name="cm:storeName" />
      </property-sheet>
   </config>
   <config evaluator="string-compare" condition="Action Wizards">
      <aspects>
         <aspect name="cm:storeSelector"/>
      </aspects>
   </config>
   ...
```

Migrating

This section describes how to perform various migration procedures for Alfresco servers and databases.

Migrating servers

The process of migrating an instance of Alfresco running on one server to another server follows a similar pattern to the backup process, with additional steps to ensure any configuration is also copied over.

The `dir.root` property is usually defined in the `alfresco-global.properties` file.

The `dir.root` is often a directory named `alf_data` within the directory where Alfresco is installed, and will hold both content and full text indexes by default. The `dir.root` location is also reported in the Alfresco logs when the server is started.

Backing up Alfresco Server 1

This task describes how to back up the first server for migration.

1. Stop the application server to ensure that no changes can be made while backing up or restoring.
2. Export the database to `dir.root` (same location as content and indexes).
3. Copy the `configuration` directory to `dir.root`.

   For example:

   ```
   cp -r tomcat/shared/classes/alfresco/extension alf_data
   ```
4. Back up `dir.root`.

Restoring to Server 2

This task describes how to restore a back up of a server to another server.

1. Install a compatible Alfresco server. This is typically an identical version to server 1.

   Do not start the new Alfresco server.
2. Restore `dir.root`. If the path is different on server 2, change the `dir.root` configuration.
3. Rename the new server's configuration directory.

   For example:

   ```
   mv tomcat/shared/classes/alfresco/extension new_ext
   ```
4. Move the configuration directory from `dir.root` to the appropriate location

   For example:

   ```
   mv alf_data/extension tomcat/shared/classes/alfresco
   ```
5. If any configuration references server 1 explicitly, change these references to server 2.
6. Import the database from `dir.root`.
7. Start the Alfresco server.

You should now have a new instance of Alfresco on a second server with identical data. If you wish to migrate the data from one type of database to another, see Migrating from the default database to another database.

Monitoring Alfresco

This section describes the various methods for monitoring Alfresco.

JMX monitoring and management extensions

This section describes the JMX-based monitoring and management functionality.

The monitoring and management extensions can be subdivided into three categories:

Read-only monitoring beans
Expose a variety of real-time metrics for monitoring health and throughput of your Alfresco server.

Configuration beans
Provide an easily navigable view of key system configuration for support and diagnostic purposes.

Management beans
Allow control over various subsystems.

For more information on these categories of bean, refer to the reference section JMX bean categories reference on page 291.

Coexistence with other MBeans

If there is an MBean server already running on the Java Virtual Machine (JVM) that Alfresco is running on, Alfresco will export its MBeans to that server. Otherwise, Alfresco will start up its own MBean server. This means that, for example, on Tomcat or WebLogic, the Alfresco beans will compliment those provided by the application server and will be navigable in the same context with a suitable JMX client.

Activating the Sun JMX agent and local JMX connectivity

Using Tomcat and a Sun JVM for the richest possible monitoring experience, you can get Alfresco and Tomcat to share the JVM's own platform MBean server, whose pre-registered MXBeans give a detailed view of the JVM's health, usage and throughput, in areas including class loading, Hotspot compilation, garbage collection and thread activity.

Sun's MBean server also provides a convenient 'local' connection method, allowing the Alfresco process to be automatically 'discovered' by a JMX client such as JConsole or Hyperic agent without manual configuration of connection details. For more information on using Hyperic with Alfresco, refer to Installing Alfresco Enterprise plug in for Hyperic on page 218

The Sun JMX agent can also be activated in 'remote' mode (where a connection is made through an RMI lookup). However, since Alfresco is always preconfigured to allow a secure remote JMX connection on any JVM, it is most likely that you will choose to activate the Sun JMX agent in local mode. This will mean the platform MBean Server will be shared by Alfresco and still be available for remote connections through the RMI connector.

- To activate the Sun JMX agent in local mode, you simply need to ensure that the following system property is set:

  ```
  com.sun.management.jmxremote
  ```

  For example, in your Tomcat startup script, you could use the following line:

  ```
  export JAVA_OPTS="${JAVA_OPTS} -Dcom.sun.management.jmxremote"
  ```
- Refer to the Sun documentation for more information on all the possible configuration options.

Installing Alfresco Enterprise plug in for Hyperic

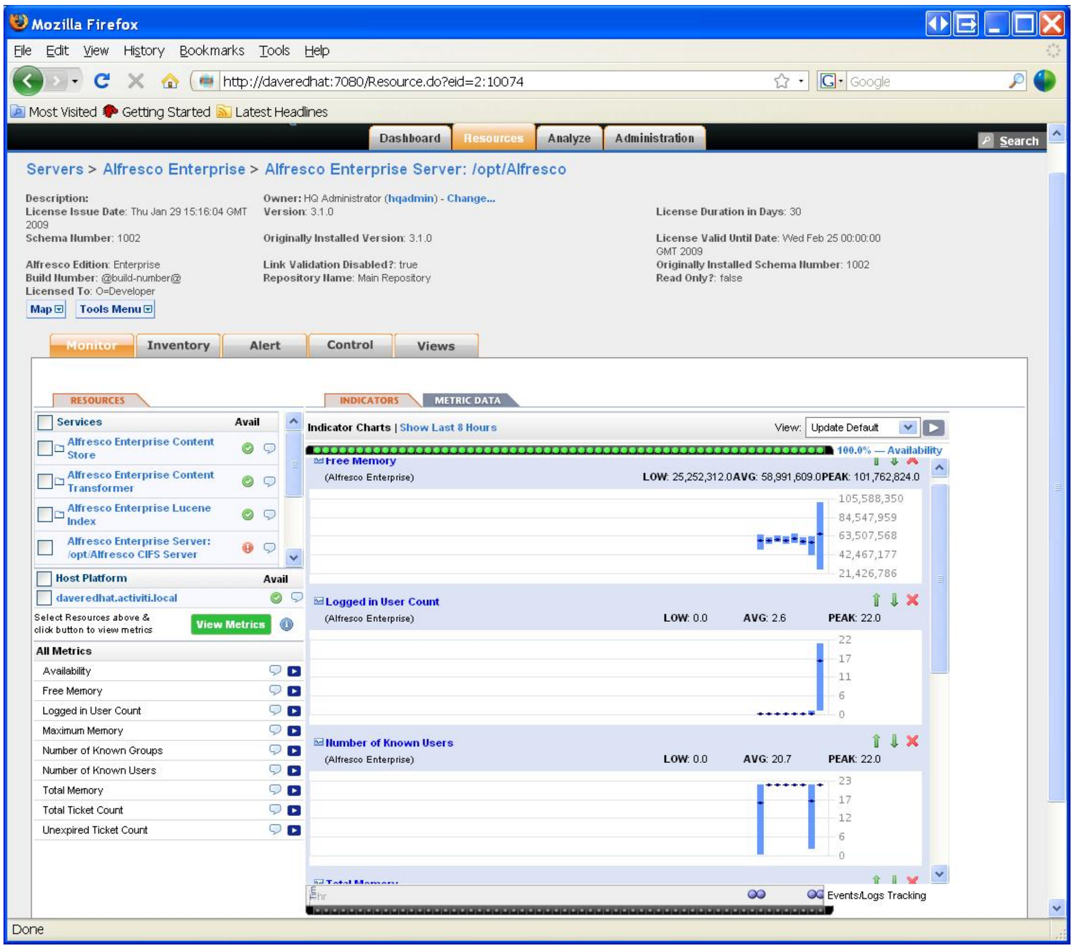
Hyperic provides auto-discovery, monitoring of system resources, alerts, charting, and event correlation for problem identification and resolution. The Alfresco Enterprise plug in for Hyperic allows you to auto-discover all Alfresco components and to monitor usage and performance using the Hyperic HQ interface.

Before you install the Alfresco Enterprise plug in for Hyperic, ensure the following:

- Hyperic HQ 4.0 Server is installed and running on your system
- Hyperic HQ Agent is installed on the same machine as Alfresco

- The operating system user running the Hyperic agent and the operating system user running Alfresco both have permissions to read and write each other's file. For example, both users must be running as root, or alternatively, both users must be in the same group, with `umask` set to 2.

The Hyperic installation consists of a server and one or more agents. A Hyperic agent running on the same machine as your Alfresco server can use the Alfresco Enterprise plug in to detect running Alfresco servers on the machine, collecting metrics on availability, performance, and use. The agent sends the inventory and metric data to the Hyperic HQ server, which can be managed using the Hyperic portal.


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Most Visited Getting Started Latest Headlines
Dashboard Resources Analyze Administration
Search
Map
Tools Menu
Monitor Inventory Alert Control Views
RESOURCES
INDICATORS METRIC DATA
View Metrics
Events/Logs Tracking
Done

http://daveredhat:7080/Resource.do?eid=2:10074

Servers > Alfresco Enterprise > Alfresco Enterprise Server: /opt/Alfresco

Description:
License Issue Date: Thu Jan 29 15:16:04 GMT 2009
Schema Number: 1002
Alfresco Edition: Enterprise
Build Number: @build-number@
Licensed To: O=Developer

Owner: HQ Administrator (hqadmin) - Change...
Version: 3.1.0
Originally Installed Version: 3.1.0
Link Validation Disabled?: true
Repository Name: Main Repository

License Duration in Days: 30
License Valid Until Date: Wed Feb 25 00:00:00 GMT 2009
Originally Installed Schema Number: 1002
Read Only?: false

Services	Avail
Alfresco Enterprise Content Store	✓
Alfresco Enterprise Content Transformer	✓
Alfresco Enterprise Lucene Index	✓
Alfresco Enterprise Server: /opt/Alfresco CIFS Server	!

Host Platform	Avail
daveredhat.activiti.local	✓

Select Resources above & click button to view metrics

All Metrics
- Availability
- Free Memory
- Logged in User Count
- Maximum Memory
- Number of Known Groups
- Number of Known Users
- Total Memory
- Total Ticket Count
- Unexpired Ticket Count

Indicator Charts | Show Last 8 Hours   View: Update Default

100.0% — Availability

Free Memory (Alfresco Enterprise) LOW: 25,252,312.0 AVG: 58,991,609.0 PEAK: 101,762,824.0

Logged in User Count (Alfresco Enterprise) LOW: 0.0 AVG: 2.6 PEAK: 22.0

Number of Known Users (Alfresco Enterprise) LOW: 0.0 AVG: 20.7 PEAK: 22.0

1. Browse to Alfresco Alfresco Support Portal.
2. Log in using your user name and password.
3. Click **Online Resources > Downloads**.
4. Search for and download the following Alfresco installation file:

   `hyperic-plugin.zip`
5. Copy the downloaded file to the `hq-plugins` directory in your Hyperic installation.
6. Open your Alfresco startup script.
7. Append the following to the JAVA_OPTS setting:

   (Windows) `-Dalfresco.home=%ALF_HOME% -Dcom.sun.management.jmxremote`

   (Linux) `-Dalfresco.home=${ALF_HOME} -Dcom.sun.management.jmxremote`
8. Save your start up script.
9. Restart the Hyperic agent using the following command:

(Linux) `/etc/init.d/hyperic-hq-agent restart`

10. Restart the Alfresco server.
11. In the Hyperic Portal, schedule an auto-discovery. Refer to the Hyperic documentation for details on how to set up auto-discovery.

    The **Alfresco Enterprise Server** is discovered, in addition to all the system resources on the machine.
12. To enable log tracking, click **Resources**, then navigate to the Alfresco Server and select **Inventory**.
13. Under **Configuration Properties**, click **Edit**.
14. Set `server.log_track.enable` to true.
15. Set the `server.log_track.level`, if required.

    Log entries will then be indicated by a blue light at the bottom of the **Monitor** tab.

Scheduled jobs

Alfresco runs a number of scheduled jobs that assist in the maintenance of a production environment. These jobs are defined in the `<configRoot>/scheduled-jobs-context.xml` file.

Scheduled job	Description
`ftsIndexerTrigger`	Triggers the full text indexing of uploaded or modified documents.
`contentStoreCleanerTrigger`	Launches the `contentStoreCleaner` bean, which identifies, and deletes or purges orphaned content from the content store while the system is running. Content is said to be orphaned when all references to a content binary have been removed from the metadata. By default, this job is triggered at 4:00 am each day. In a clustered environment, this job could be enabled on a headless (non-public) node only, which will improve efficiently.
`nodeServiceCleanupTrigger`	Performs cleanup operations on DM node data, including old deleted nodes and old transactions. In a clustered environment, this job could be enabled on a headless (non-public) node only, which will improve efficiently.
`openOfficeConnectionTesterTrigger`	Maintains the connection with OpenOffice.
`indexBackupTrigger`	Creates a safe backup of the Lucene directories.
`tempFileCleanerTrigger`	Cleans up all Alfresco temporary files that are older than the given number of hours. Subdirectories are also emptied and all directories below the primary temporary subdirectory are removed. The job data must include the `protectHours` property, which is the number of hours to protect a temporary file from deletion since its last modification.
`avmOrphanReaperJob`	Quartz wrapper for OrphanReaper, which is a background thread for reaping nodes that are no longer referenced in the AVM repository. These orphans arise from purge operations.
`avmExpiredContentTrigger`	Searches for expired content in the web project staging area and prompts the last modifier of the content to review it.

Scheduled job	Description
`ehCacheTracerJob`	Collects detailed cache usage statistics and outputs them to the console, depending on how logging has been configured for the server. By default, his job is not activated. To activate this job, uncomment the `scheduler` property.

Setting up Alfresco multi-tenancy

Alfresco supports a single-instance, single-tenant (ST) environment where each tenant (for example, customer, company, or organization) runs a single instance that is installed on one server or across a cluster of servers. You can also run multiple instances of Alfresco on the same server by configuring separate database schemas, separate content stores, separate (non-conflicting) ports, and so on. However, this adds additional complexity in terms of configuration and upgrades.

The multi-tenancy (MT) features enable Alfresco to be configured as a true single-instance, multi-tenant environment. This enables multiple independent tenants to be hosted on a single instance, which can be installed either on a single server or across a cluster of servers. The Alfresco instance is logically partitioned such that it will appear to each tenant that they are accessing a completely separate instance of Alfresco.

Enabling multi-tenancy

You can configure a multi-tenant (MT) environment by renaming three sample MT extension files, and then restarting Alfresco.

1. Locate the following directory:

   `<extension>\mt\`
2. Remove the `.sample` extension from the following MT files:
   a. `mt-admin-context.xml.sample`
   b. `mt-contentstore-context.xml.sample`
   c. `mt-context.xml.sample`

   All three files must be renamed to enable MT.
3. Restart the Alfresco server.

Managing tenants

The default Alfresco administrator user has access to the default environment and can be considered to be a "super tenant". The administrator can manage tenants using the Tenant Administration Console.

1. Log in to Alfresco as the `admin` user and access: `http://localhost:8080/alfresco/faces/jsp/admin/tenantadmin-console.jsp`
2. Perform the following as required:
   a. To list all tenants and show their details, type `show tenants`.
   b. To show details for a single tenant, type `show tenant <tenant domain>`.

   This shows the status (for example, whether it is enabled or disabled) and the root content store directory.
   c. To create a tenant, type `create <tenant domain> <tenant admin password> [<root contentstore dir>]`.

For example, `create zzz.com l3tm31n /usr/tenantstores/zzz`

This creates an empty tenant. By default the tenant will be enabled. It will have an administrator user called `admin@<tenant domain>` with the supplied password. All users that the administrator creates can login using `<username>@<tenant domain>`. The root of the content store directory can be optionally specified, otherwise it defaults to the repository default root content store (as specified by the `dir.contentstore` property). The default workflows are also be bootstrapped.

d. To enable a tenant, type `enable <tenant domain>`.

   This enables the tenant so that it is active and available for new logins.

e. To disable a tenant, type `disable <tenant domain>`.

   This disables the tenant so that it is inactive and prevents tenant login.

Multi-tenancy administration

Once a tenant is created and enabled, the tenant administrator can log into Explorer and access the Administration Console within the context of their tenant domain.

For example, if a tenant/organization called `acme` is created, the tenant administrator can log in as `admin@acme` and create users such as `alice@acme`, and `bob@acme`.

The administration features currently available to the tenant administrator include:

- Manage system users (including user Usages and Quotas)
- Manage user groups
- Category management
- Export and import
- System information
- Node browser

Multi-tenancy export and import

This section describes how a tenant administrator can export and import spaces and tenants using the Tenant Administration Console.

Repository export does not apply to certain areas, such as in-flight workflows. A repository import must be into the same version of Alfresco from which the export was performed.

1. Log in to Alfresco as the `admin` user and access: `http://localhost:8080/alfresco/faces/jsp/admin/tenantadmin-console.jsp`
2. Use the export feature to export a tenant:

   ```
   export <tenant domain> <destination directory>
   ```

   This exports the tenant to a set of repository export files in a given destination directory. Export file names will be suffixed with `<tenant domain>_`.
3. Use the import feature to import a tenant:

   ```
   import <tenant domain> <source directory> [<root contentstore dir>]
   ```

   This creates a tenant by importing the tenant files from the given source directory. The import file names must be suffixed with `<tenant domain>_`.

   If an existing tenant needs to be re-imported, the tenant must be deleted first. To cleanly delete a tenant, the server must be restarted to clear the index threads. The tenant-specific index directories and tenant-specific content directories must also be manually deleted before starting the import.

Multi-tenancy implementation

To implement multi-tenancy, Alfresco has been logically partitioned such that each tenant has access to their own set of tenant-specific stores. These stores are typically routed to their own physical root directory. This also means that indexes are partitioned, since Alfresco maintains an index per store.

All Alfresco-related services are partitioned including node services, security services, workflow services, search and index services, and dictionary services. To support Alfresco Share in a multi-tenant environment, additional partitioned services include site services, activity services, invite services, and AVM services.

The metadata is logically partitioned within the database schema.

Logging enables nested diagnostic context (NDC). For a single tenant environment, the log output will show the user name context. For a multi-tenant environment, the log output also shows the tenant context.

Clustering

The MT features have been designed and implemented to work in a clustered configuration.

Cache size

If you wish to support a large number of tenants (for example, greater than 99), then must review and increase the cache size for all of the tenant caches. The cache sizes are by default configured to 100 (including the default domain) in the `<configRoot>/cache-context.xml` file. Change the cache size in the `ehcache-custom-cluster.xml.sample.cluster` file.

Tenant-based caches currently include:

- `webScriptsRegistryCache (RepositoryContainer)`
- `prefixesCache (NamespaceDAOImpl)`
- `urisCache (NamespaceDAOImpl)`
- `compiledModelsCache (DictionaryDAOImpl)`
- `uriToModelsCache (DictionaryDAOImpl)`
- `messagesCache (MessageServiceImpl)`
- `loadedResourceBundlesCache (MessageServiceImpl)`
- `resourceBundleBaseNamesCache (MessageServiceImpl)`

Modules

Alfresco supports the ability to pre-package AMPs (Alfresco Module Packages) into the Alfresco WAR, which are installed into the default domain on start up. In a multi-tenant environment, the module is also installed into each tenant domain when the tenant is created or imported.

Features not currently supported in a multi-tenant environment

The following features and components are not supported in a multi-tenant production environment:

- CIFS
- WCM
- Portlets
- Delete tenant (pending Delete Store)
- LDAP, NTLM and authentication methods other than `alfresco`
- Inbound email
- Content replication

- IMAP
- SharePoint Protocol
- Alfresco Share (for versions prior to Alfresco 3.2)

Setting up replication jobs

The replication service provides control for replicating content between different Alfresco repositories.

The replication service is responsible for persisting replication jobs that specify what is to be replicated, to where, and when. In addition, it monitors the status of currently executing replication jobs and enables replications to be canceled.

The replication service finds the nodes that need to be transferred, and then it delegates to the transfer service.

Alfresco Share provides the user interface for the replication service, which is available through the administration tools menu. The methods are exposed by Java-based replication web scripts.

Configuring Share to open locked content in the source repository

For replication jobs, you must configure Alfresco Share to open a locked node in the source repository, where it can be edited. This is configured by mapping the remote repository identifier (`repositoryId`) and the URL, which gives access the remote repository.

1. Locate the `repositoryId` by browsing to the remote server's CMIS landing page using the following URL:

   ```
   http://{server}:{port}/alfresco/service/cmis/index.html
   ```

   The `repositoryId` field is displayed in the **CMIS Repository Information** panel.
2. Open the `<web-extension>\share-config-custom.xml.sample` file.
3. Locate the following example configuration:

   ```
    <config evaluator="string-compare" condition="Replication">
         <share-urls>
            <!--
               To discover a Repository Id, browse to the remote server's
    CMIS landing page at:
                 http://{server}:{port}/alfresco/service/cmis/index.html
               The Repository Id field is found under the "CMIS Repository
    Information" expandable panel.

               Example config entry:
                 <share-url repositoryId="622f9533-2a1e-48fe-af4e-
   ee9e41667ea4">http://new-york-office:8080/share/</share-url>
            -->
         </share-urls>
      </config>
   ```
4. Modify the `repositoryId` in the following line:

   ```
   <share-url repositoryId="622f9533-2a1e-48fe-af4e-ee9e41667ea4">http://
   new-york-office:8080/share/</share-url>
   ```
5. Copy this configuration setting to your `share-config-custom.xml` file or save the sample file without the `.sample` extension.

Creating a new transfer target for replication jobs

The transfer service stores files that control and monitor the operation of the transfer service in the **Transfer** space in the Data Dictionary.

The **Transfer Target** groups space contains the transfer target definitions that specify where transfers go to. There is a group level below the folder which is used to classify different sets of transfer targets. There is only a single group called **Default Group**.

You can add transfer targets by creating a folder in Alfresco Explorer or Alfresco Share.

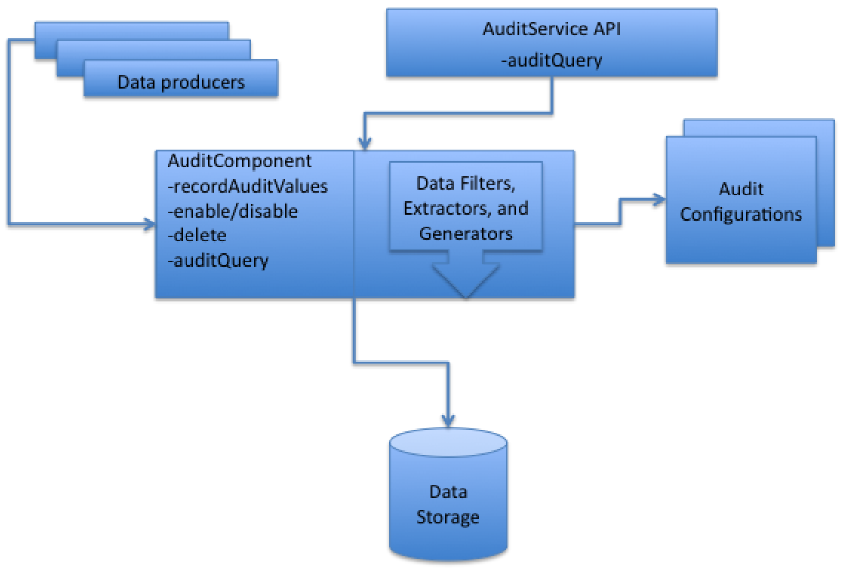
1. Create a folder in **Company_Home > Data_Dictionary > Transfer > Transfer Targets > Default Group**.
2. A rule defined on the **Default Group** folder specializes the type of any folder created within it. The type is set to `trx:transferTarget`, which you can then complete through the user interface.

Auditing Alfresco

Alfresco provides the ability to audit activity. This section describes how Alfresco generates, stores, and retrieves auditing information.

Version 3.4.0 has a new default implementation of auditing. The mechanism prior to Version 3.4.0 has been removed but the old tables remain in the system. You can access the previous audit data but any new audit data will be directed to the new tables. Any customizations of the auditing feature must be rewritten using the new configuration files. All SQL-based queries used previously must be replaced bu calls to the supplied APIs. The use of low-level SQL statements to retrieve data is not supported.

The architecture of the auditing features comprises the following components:



Data Producers defines the components that produce data that might be audited. Data producers do not need to know anything about how the data is stored. Data is generated and sent to the `AuditComponent.recordAuditValues` component. The only requirement is that each packet of data is a *Map* of data keyed by logical path names, which are specific to the producers.

The **AuditService** search should be used for data retrieval; however, for completeness, the following tables are used:

- Tables exclusive to the new audit (*AlfrescoPostCreate-3.2-AuditTables.sql*)
  - `alf_audit_model`: Contains the record of the audit configuration files.
  - `alf_audit_application`: Contains an entry for each logical application. There may be several audit applications defined in a single audit model.
  - `alf_audit_entry`: Contains an entry for aach call to `AuditComponent.recordAuditValues`. There is a reference to a property.
- Shared tables (*AlfrescoPostCreate-3.2-PropertyValueTables.sql*)
  - `alf_prop_root`: Entry point for properties: shared values are fully indexed; arbitrarily-deep collections; quick data query and reconstruction.

Audit configuration and environment

This section describes the configuration and environment settings for auditing.

Configuration and environment	Details
Tomcat environment	• Set the configuration properties in the `alfresco-global.properties` file. • Log4J settings can be added in a file `<tomcat>/shared/classes/alfresco/extension/audit-log.properties`.
View the available web scripts and details	Use the following scripts: • Script index: http://localhost:8080/alfresco/service/ • Audit scripts: http://localhost:8080/alfresco/service/index/package/org/alfresco/repository/audit
HTTP client	• *curl* will be used as the HTTP client

Check the state of auditing on the server:

```
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/
control"
{
   "enabled" : false,
   "applications":
   [
   ]
}
```

Sample files

Audit sample files are distributed in the `<TOMCAT_HOME>/classes/alfresco/extension/audit` directory.

Samples can also be downloaded directly from the following location in svn:

`http://svn.alfresco.com/repos/alfresco-open-mirror/alfresco/HEAD/root/projects/repository/config/alfresco/extension/audit/`

When using a sample file, remove the `.sample` extension.

Enabling auditing

Auditing is disabled by default. To enable auditing permanently, set auditing in the global properties file.

1. Auditing can be globally enabled using the control web script, but will reset when the server restarts.

   ```
   % curl -u admin:admin -d "" "http://localhost:8080/alfresco/service/api/
   audit/control?enable=true"
   {
      "enabled" : true
   }
   ```

2. To enable auditing permanently, add the following setting to the `alfresco-global.properties` file:

   ```
     audit.enabled=true
   ```

3. Save the file, and then restart the Alfresco server.

Use the JMX client to modify the Audit subsystem. Changes to the Audit subsystem will be preserved across server restarts.

Audit sample files are distributed in the `<extension>/audit` directory. Activate the sample files by removing the `.sample` extension.

Auditing examples

This section describes some auditing examples.

Audit data passed to recordAuditValues():

```
Root path:
   /alfresco-api/post/NodeService/createStore
Map:
   args/protocol = "workspace"
   args/identifier = "SpacesStore"
   result = StoreRef[workspace://SpacesStore]
```

If the root path passes the initial filtration phase - there is at least one component interested in auditing the information - then the map is expanded.

Expanded audit data:

```
Map:
   /alfresco-api/post/NodeService/createStore/args/protocol = "workspace"
   /alfresco-api/post/NodeService/createStore/args/identifier =
 "SpacesStore"
   /alfresco-api/post/NodeService/createStore/result = StoreRef[workspace://
SpacesStore]
```

The filtered data is then passed through the path mappings, generating a new "Map" of data for each application.

Path-mapped audit data:

```
Map:
   /MyApp/createStore = StoreRef[workspace://SpacesStore]
```

This data is then passed to any extractors and generators to produce a final "Map" of data that will be persisted.

Persisted audit data:

```
Map:
   /MyApp/createStore/value = StoreRef[workspace://SpacesStore]
   /MyApp/createStore/rootNode = NodeRef[workspace://SpacesStore/fd123...]
```

Audit configuration files

This section describes the location and basic structure of the audit configuration files.

Audit configuration files are picked up automatically using the following search paths.

- `classpath*:alfresco/audit/*.xml`
- `classpath*:alfresco/enterprise/audit/*.xml`
- `classpath*:alfresco/module/*/audit/*.xml`
- `classpath*:alfresco/extension/audit/*.xml`

The XML schema is located at `<configRoot>/classes/alfresco/audit/alfresco-audit-3.2.xsd`.

The configuration file structure is divided into four basic sections:

<DataExtractors>

In this section, DataExtractors are declared for use in the `<Application>` sections of the configuration files. A DataExtractor is a component that uses input data to produce some output, either transforming the data or outputting the data verbatim. The simplest extractor is the `SimpleValueDataExtractor`, which returns whatever data is passed in. A more complex extractor is the `NodeNameDataExtractor`, which is able to produce the `cm:name` value of a node, assuming the data passed in is a NodeRef. For the complete set of built-in generators, see the `org.alfresco.repo.audit.extractor` package, or the `auditModel.extractor.*` beans, which are declared in `alfresco/audit-services-context.xml`.

The extractors can be declared in-line, for example:

```
    <DataExtractors>
       <DataExtractor name="simpleValue"
class="org.alfresco.repo.audit.extractor.SimpleValueDataExtractor"/>
       ...
    </DataExtractors>
```

Or they can be declared in Spring configuration and referenced in the audit configuration (see the `alfresco/audit-services-context.xml` file), for example:

```
    <DataExtractors>
       <DataExtractor name="simpleValue"
registeredName="auditModel.extractor.simpleValue"/>
       ...
    </DataExtractors>
```

<DataGenerators>

In this section, DataGenerators are declared for use in the `<Application>` sections of the configuration files. A DataGenerator is a component that produces data without any input, that is, data is produced when a data path is active, but is independent of the values at that path. Examples of generators are the `AuthenticatedUserDataGenerator` component, which produces the name of the currently-authenticated user (user in context) and the `AuthenticatedPersonDataGenerator` component, which produces the full name of the currently-authenticated user (person in context). For the complete set of built-in generators, see the `org.alfresco.repo.audit.generator` package or the `auditModel.generator.*` beans, which are declared in the `alfresco/audit-services-context.xml` file.

The generators can be declared in-line, for example:

```
    <DataGenerators>
       <DataGenerator name="currentUser"
 class="org.alfresco.repo.audit.generator.AuthenticatedUserDataGenerator"/>
       <DataGenerator name="personFullName"
 class="org.alfresco.repo.audit.generator.AuthenticatedPersonDataGenerator"/
>
    </DataGenerators>
```

Or they can be declared in Spring configuration and referenced in the audit configuration (see the `alfresco/audit-services-context.xml` file), for example:

```
    <DataGenerators>
       <DataGenerator name="currentUser"
 registeredName="auditModel.generator.user"/>
       <DataGenerator name="personFullName"
 registeredName="auditModel.generator.personFullName"/>
    </DataGenerators>
```

<PathMappings>

The expanded map coming from the Data Producers is passed through the path mappings. This is a raw remapping of the input data based on the path names in the data map.

```
    <PathMappings>
        <PathMap source="/DOD5015" target="/DOD5015"/>
        <!-- Force the fullName generator to trigger -->
        <PathMap source="/DOD5015/event/node" target="/DOD5015/event/
person"/>
        <PathMap source="/alfresco-api/post/AuthenticationService/
authenticate" target="/DOD5015/login"/>
    </PathMappings>
```

In this example, all paths starting with `/DOD5015` are mapped verbatim, but without the declaration, the data paths starting with `/DOD5015` are discarded. A small subset of the Alfresco API data is used (only the `AuthenticationService.authenticate` call) by mapping all values starting with that path to `/DOD5015/login`.

<Application>

This section defines how the mapped data is to be used by DataGenerators or by DataExtractors.

```
    <Application name="DOD5015" key="DOD5015">
        <AuditPath key="login">
            <AuditPath key="args">
                <AuditPath key="userName">
                    <RecordValue key="value" dataExtractor="simpleValue"/>
                </AuditPath>
            </AuditPath>
            <AuditPath key="no-error">
                <GenerateValue key="fullName"
 dataGenerator="personFullName"/>
            </AuditPath>
            <AuditPath key="error">
                <RecordValue key="value" dataExtractor="nullValue"/>
            </AuditPath>
        </AuditPath>
    </Application>
```

Built-in data producers

The following are built-in data producers.

- `org.alfresco.repo.audit.AuditMethodInterceptor`: Generates audit data for all public service API calls. Refer to the javadocs for the data structure.
- `org.alfresco.repo.node.NodeAuditor`: Generates audit data for `beforeDeleteNode`

It is possible for any server-side component to pass data to the `auditComponent` bean.

To see what information is available to audit, enable the following logging:

```
log4j.logger.org.alfresco.repo.audit.inbound=DEBUG
```

The following is an example of output generated when a node is deleted from Alfresco Explorer:

```
15:55:26,590 User:admin DEBUG [repo.audit.inbound]
Inbound audit values:
 /alfresco-node/beforeDeleteNode/node=workspace://SpacesStore/
c4728f24-4a11-40f7-9062-315edf959d79
15:55:26,748 User:admin DEBUG [repo.audit.inbound]
Inbound audit values:
 /alfresco-api/post/NodeService/deleteNode/no-error=null
 /alfresco-api/post/NodeService/deleteNode/args/nodeRef=workspace://
SpacesStore/c4728f24-4a11-40f7-9062-315edf959d79
```

DataExtractors and DataGenerators

This section provides a description of DataExtractors and DataGenerators.

It is possible for any server-side component to pass data to the `auditComponent` bean.

DataExtractor

Uses an inbound mapped value as the source of the data. *AuditExampleLogin1* records values quite literally using the *simpleValue* data extractor.

DataGenerator

Activates when an inbound mapped path is present, but is not dependent on the value on that path. *AuditExampleLogin2* triggers the *personFullName* generator when the *authenticate/no-error* path is present; this records the full name of the currently-authenticated user even though the inbound data for *authenticate/no-error* is *null*.

Look at the data recorded for the two sample applications:

```
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/query/
AuditExampleLogin1?verbose=true&forward=false&limit=1"
```

```
{
   "count":1,
   "entries":
   [
      {
         "id":137,
         "application":AuditExampleLogin1,
         "user":admin,
         "time":"2010-09-20T17:37:14.699+01:00",
         "values":
         {
                     "\/auditexamplelogin1\/login\/no-error\/user":"admin"
         }

      }
   ]
}
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/query/
AuditExampleLogin2?verbose=true&forward=false&limit=1"
{
   "count":1,
   "entries":
   [
      {
         "id":138,
         "application":AuditExampleLogin2,
         "user":admin,
         "time":"2010-09-20T17:37:23.101+01:00",
         "values":
         {
                     "\/auditexamplelogin2\/login\/user":"Administrator"
         }

      }
   ]
}
```

Locating the audit code

This section describes the location of audit code.

1. For DEBUG logging, to see which data is being produced, rejected, or recorded, enable DEBUG for:

   ```
   log4j.logger.org.alfresco.repo.audit.AuditComponentImpl=DEBUG
   ```

2. For JUnit code, the unit test code demonstrates use of the Audit APIs and configuration:

   ```
   org.alfresco.repo.audit.AuditComponentTest
   ```

   - `alfresco-audit-test-authenticationservice.xml`: This is used by the test to capture both successful and unsuccessful login attempts in the audit data.
   - `testAuditAuthenticationService`: This demonstrates the use of the `auditSearch` method.

3. For Records Management (DOD5015) and auditing, the module pulls in audit data from the '`AuthenticationService`' but adds more data around the individual actions that take place during Records Management processes.

   ```
   org.alfresco.module.org_alfresco_module_dod5015.audit.*
   ```

   - `RecordsManagementAuditServiceImpl$RMAuditTxnListener`: This transaction listener generates Records Management-specific data for events (it is a `Data Producer`). It generates node property deltas.
   - `config/alfresco/module/org_alfresco_module_dod5015/audit/rm-audit.xml`: This defines how the data produced by the `AuthenticationService`

and the Records Management module is persisted. There are some custom `DataGenerators` and `DataRecorders`.

- `RecordsManagementAuditServiceImpl.getAuditTrailImpl`: This method demonstrates how the Records Management use-case searches the audit data. Further query extensions are required to extend the search filters available using the `auditQuery` API.

Defining the audit application

This section describes the audit applications.

Data producers have no knowledge of how or whether data will be stored. Different use cases need to store or modify inbound data independently, therefore the use cases are separated into audit applications. Each application defines how data is mapped, extracted, and recorded without affecting data required by other applications.

For example, the Records Management module records before and after values when specific nodes are modified, whereas the CMIS standard requires a slightly different set of data to be recorded. Additionally, each of the audit logs can be enabled and disabled independently within the same server. Usually, each audit application is defined in its own configuration file, but for demonstration purposes, multiple application definitions can be defined in one configuration file.

1. Enable the sample file by removing the `.sample` extension.

   `alfresco/extensions/audit/alfresco-audit-example-login.xml.sample`
2. Restart the Alfresco server.
3. Ensure that the applications have been registered properly and are enabled:

```
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/
control"
{
   "enabled" : true,
   "applications":
   [
      {
         "name": "AuditExampleLogin1",
         "path" : "/auditexamplelogin1",
         "enabled" : true
      }
         ,
      {
         "name": "AuditExampleLogin2",
         "path" : "/auditexamplelogin2",
         "enabled" : true
      }
         ,
      {
         "name": "CMISChangeLog",
         "path" : "/CMISChangeLog",
         "enabled" : true
      }

   ]
}
```

4. At an application level, auditing is enabled or disabled for specific paths; changes made to an application's audit state are persisted. To disable all auditing for an application, disable the root path; in this case, disable the root path for the `CMISChangeLog` application. If you restart the server you will see that the application remains disabled.

```
% curl -u admin:admin -d "" "http://localhost:8080/alfresco/service/api/
audit/control/CMISChangeLog/CMISChangeLog?enable=false"
{
   "enabled" : false
}
```

Simple audit query

This section describes the a simple audit query example.

1. Generate some auditing data for the sample applications.
2. Connect to the Alfresco Explorer client.
3. Login as the `admin` user.
4. Logout of Alfresco.
5. Login as the `admin` user but use an illegal password.

   The following examples are two queries to return results: without and with full-audited values respectively. Some entries have been replaced with a (**...**) for brevity.

```
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/
query/AuditExampleLogin1"
{
   "count":4,
   "entries":
   [
      {
         "id":69,
         "application":AuditExampleLogin1,
         "user":admin,
         "time":"2010-09-20T14:45:28.998+01:00",
         "values":
null
      },
      ...
   ]
}
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/
query/AuditExampleLogin1?verbose=true"
{
   "count":5,
   "entries":
   [
      ...
      {
         "id":72,
         "application":AuditExampleLogin1,
         "user":null,
         "time":"2010-09-20T14:45:43.884+01:00",
         "values":
         {
                     "\/auditexamplelogin1\/login\/error\/user":"admin"
         }

      },
      ...
      {
         "id":76,
         "application":AuditExampleLogin1,
         "user":admin,
         "time":"2010-09-20T14:46:23.319+01:00",
         "values":
         {
                     "\/auditexamplelogin1\/login\/no-error\/
user":"admin"
         }

      }
   ]
}
```

There is no count function in the search API. This is by design; use the `limit` parameter instead.

6. Assume that a client wants to see the details of the latest two results but knows of the existence of the next eight results. In this case, it would be pointless pulling back full (`verbose=true`) results for the latest 10 entries. Instead, pull back the last two results with values and then pull back the next eight results without values.

   Notice that the response contains a count of the number of entries returned; the individual entries are provided so that the entry IDs can be used for further result retrieval.

```
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/
query/AuditExampleLogin1?verbose=true&limit=2&forward=false"
{
   "count":2,
   "entries":
   [
      {
         "id":98,
         "application":AuditExampleLogin1,
         "user":admin,
         "time":"2010-09-20T15:10:04.043+01:00",
         "values":
         {
                     "\/auditexamplelogin1\/login\/no-error\/
user":"admin"
         }

      },
      {
         "id":96,
         "application":AuditExampleLogin1,
         "user":admin,
         "time":"2010-09-20T15:09:50.117+01:00",
         "values":
         {
                     "\/auditexamplelogin1\/login\/no-error\/
user":"admin"
         }

      }
   ]
}
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/
query/AuditExampleLogin1?verbose=false&limit=8&forward=false&toId=96"
{
   "count":8,
   "entries":
   [
      {
         "id":94,
         "application":AuditExampleLogin1,
         "user":admin,
         "time":"2010-09-20T15:09:47.606+01:00",
         "values":
null
      },
      ...
      {
         "id":80,
         "application":AuditExampleLogin1,
         "user":admin,
         "time":"2010-09-20T14:58:34.305+01:00",
         "values":
null
      }
   ]
}
```

Advanced audit query

This section describes the a advanced audit query example.

This type of query URL makes use of a data path within the audit application. This allows entries to be found that match specific audited values. By default, query values are treated as case-sensitive string types, but it is possible to specify the type to query against.

1. Generate some audit data.
2. Connect to the Alfresco Explorer client.
3. Attempt a filed login as `joe`.

```
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/
audit/query/AuditExampleLogin1/auditexamplelogin1/login/error/user?
verbose=true&value=joe"
{
   "count":1,
   "entries":
   [
      {
         "id":101,
         "application":AuditExampleLogin1,
         "user":null,
         "time":"2010-09-20T15:13:57.947+01:00",
         "values":
         {
                     "\/auditexamplelogin1\/login\/error\/user":"joe"
         }

      }
   ]
}
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/
audit/query/AuditExampleLogin1/auditexamplelogin1/login/error/user?
verbose=true&value=JOE"
{
   "count":0,
   "entries":
   [
   ]
}
```

Understanding PathMappings

To create an audit configuration file, it is necessary to know which data can be audited and how the data is mapped onto your application.

1. Turn on debugging for the inbound data. For a better understanding, you can turn on debug logging for the mapping components as well, although this is more verbose.

```
% cat <tomcatgt/shared/classes/alfresco/extension/audit-log4j.properties
log4j.logger.org.alfresco.repo.audit.AuditComponentImpl=DEBUG
log4j.logger.org.alfresco.repo.audit.inbound=DEBUG
```

2. Tail the log file and watch the output.

   a. Login as admin.

```
16:47:37,434  DEBUG [repo.audit.inbound]
Inbound audit values:
 /alfresco-api/pre/AuthenticationService/authenticate/args/
userName=admin
16:47:37,443 User:admin DEBUG [repo.audit.inbound]
Inbound audit values:
 /alfresco-api/post/AuthenticationService/authenticate/no-error=null
 /alfresco-api/post/AuthenticationService/authenticate/args/
userName=admin
```

b. From the inbound values (and if you have the `AuthComponentImpl` debugging on):

```
16:47:37,445 User:System DEBUG [repo.audit.AuditComponentImpl]
 Extracted audit data:
   Application: AuditApplication[ name=AuditExampleLogin2, id=7,
 disabledPathsId=7]
   Raw values:  {/auditexamplelogin2/login=null}
   Extracted:   {}
16:47:37,447 User:admin DEBUG [repo.audit.AuditComponentImpl] New
 audit entry:
   Application ID: 7
   Entry ID:       130
   Values:         {/auditexamplelogin2/login=null}
   Audit Data:     {/auditexamplelogin2/login/user=Administrator}
16:47:37,447 User:System DEBUG [repo.audit.AuditComponentImpl]
 Extracted audit data:
   Application: AuditApplication[ name=AuditExampleLogin1, id=6,
 disabledPathsId=6]
   Raw values:  {/auditexamplelogin1/login/no-error=null, /
auditexamplelogin1/login/args/userName=admin}
   Extracted:   {/auditexamplelogin1/login/no-error/user=admin}
16:47:37,449 User:admin DEBUG [repo.audit.AuditComponentImpl] New
 audit entry:
   Application ID: 6
   Entry ID:       131
   Values:         {/auditexamplelogin1/login/no-error=null, /
auditexamplelogin1/login/args/userName=admin}
   Audit Data:     {/auditexamplelogin1/login/no-error/user=admin}
```

You can see that the `AuthenticationService.authenticate` method generate two sets of "inbound" data: the `/alfresco-api/pre/AuthenticationService/authenticate` data is passed through before the service call is processed; the `/alfresco-api/post/AuthenticationService/authenticate` data is passed through after the service call has been processed. When logging in successfully, the post-call data is generated with a `no-error` path.

c. Perform a failed login with user joe.

```
17:02:09,697  DEBUG [repo.audit.inbound]
Inbound audit values:
 /alfresco-api/pre/AuthenticationService/authenticate/args/
userName=joe
17:02:09,704  DEBUG [repo.audit.inbound]
Inbound audit values:
 /alfresco-api/post/AuthenticationService/authenticate/error=08200014
 Failed to authenticate
   Started at:

 org.alfresco.repo.security.authentication.AbstractChainingAuthenticationServi
      ...
```

This is translated and recorded:

```
17:02:09,704 User:System DEBUG [repo.audit.AuditComponentImpl]
 Extracted audit data:
   Application: AuditApplication[ name=AuditExampleLogin1, id=6,
 disabledPathsId=6]
   Raw values:  {/auditexamplelogin1/login/error=08200014 Failed to
 authenticate
   Started at:

 org.alfresco.repo.security.authentication.AbstractChainingAuthenticationServi
      ...
17:02:09,704  DEBUG [repo.audit.AuditComponentImpl] New audit entry:
   Application ID: 6
   E6try ID:       135
   Values:         {/auditexamplelogin1/login/error=08200016 Failed to
 authenticate
   Started at:

 org.alfresco.repo.security.authentication.AbstractChainingAuthenticationServi
      ...
   Audit Data:     {/auditexamplelogin1/login/error/user=joe}
```

d. Notice that the failed login did not generate any data for audit application `AuditExampleLogin2`. To understand this, look at the `PathMappings` section of the example:

```
<PathMappings>
        <PathMap source="/alfresco-api/post/AuthenticationService/
authenticate" target="/auditexamplelogin1/login"/>
        <PathMap source="/alfresco-api/post/AuthenticationService/
authenticate/no-error" target="/auditexamplelogin2/login"/>
    </PathMappings>
```

Before any data is considered for persistence, the inbound data paths are remapped using the `PathMappings` configuration. The `/auditexamplelogin2/login` path is mapped onto `.../no-error` only, so failed logins were not recorded for the `AuditExampleLogin2` audit application, while the `AuditExampleLogin1` application recorded both successful and failed logins.

Audit recording values

The `RecordValue` element makes use of the `DataExtractor` definitions, but specifies when to be activated (`dataTrigger`) and where to get the data from (`dataSource`). Both the `dataTrigger` and `dataSource` attributes default to the path of the `RecordValue` element. Data is always written to the path where the `RecordValue` is declared. So, it is possible to trigger the `RecordValue` when a data path is present (such as a `null` value) and then to read a value from a completely different location.

1. Activate sample `/audit/alfresco-audit-example-extractors.xml` file.
2. Restart Alfresco (or restart the Audit subsystem).
3. Tail the log to capture `createNode` calls:

```
tail -f ../logs/catalina.out | grep -G "createNode" -A 200 -B 20
```

4. Login to explorer and add some content under **Company Home**.

```
20:18:52,817 User:admin DEBUG [repo.audit.AuditComponentImpl]
New audit entry:
 Application ID: 8
 Entry ID:       177
 Values:
  /auditexampleextractors/args/properties=...
  /auditexampleextractors/args/assocQName={http://www.alfresco.org/model/
content/1.0}alfresco.log
  /auditexampleextractors/args/parentRef=workspace://
SpacesStore/37884669-0607-4527-940d-cb34b4f07d75
  /auditexampleextractors/no-error=null
  /auditexampleextractors/args/assocTypeQName={http://www.alfresco.org/
model/content/1.0}contains
  /auditexampleextractors/args/nodeTypeQName={http://www.alfresco.org/
model/content/1.0}content
  /auditexampleextractors/result=workspace://
SpacesStore/37884669-0607-4527-940d-cb34b4f07d75|workspace://SpacesStore/
c0fabc6d-903f-4317-87d1-ec62de37089c|...
 Audit Data:
  /auditexampleextractors/create/out/a=workspace://
SpacesStore/37884669-0607-4527-940d-cb34b4f07d75|workspace://SpacesStore/
c0fabc6d-903f-4317-87d1-ec62de37089c|...
  /auditexampleextractors/create/derived/parent-node-name=Company Home
  /auditexampleextractors/create/derived/parent-node-null=null
  /auditexampleextractors/create/in/c={http://www.alfresco.org/model/
content/1.0}contains
  /auditexampleextractors/create/in/d={http://www.alfresco.org/model/
content/1.0}alfresco.log
  /auditexampleextractors/create/in/a=workspace://
SpacesStore/37884669-0607-4527-940d-cb34b4f07d75
  /auditexampleextractors/create/derived/parent-node-type={http://
www.alfresco.org/model/content/1.0}folder
  /auditexampleextractors/create/in/b={http://www.alfresco.org/model/
content/1.0}content
```

5. View the audited data using the query API:

```
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/
query/AuditExampleExtractors?limit=1&forward=false&verbose=true"
{
   "count":1,
   "entries":
   [
      {
         "id":177,
         "application":AuditExampleExtractors,
         "user":admin,
         "time":"2010-09-20T20:18:52.761+01:00",
         "values":
         {
                     "\/auditexampleextractors\/create\/out\/
a":"workspace:\/\/SpacesStore\/37884669-0607-4527-940d-cb34b4f07d75|
workspace:\/\/SpacesStore\/c0fabc6d-903f-4317-87d1-ec62de37089c|...
                     ,"\/auditexampleextractors\/create\/derived\/parent-
node-name":"Company Home"
                     ,"\/auditexampleextractors\/create\/in\/c":"{http:\/
\/www.alfresco.org\/model\/content\/1.0}contains"
                     ,"\/auditexampleextractors\/create\/in\/d":"{http:\/
\/www.alfresco.org\/model\/content\/1.0}alfresco.log"
                     ,"\/auditexampleextractors\/create\/in\/
a":"workspace:\/\/SpacesStore\/37884669-0607-4527-940d-cb34b4f07d75"
                     ,"\/auditexampleextractors\/create\/derived\/parent-
node-type":"{http:\/\/www.alfresco.org\/model\/content\/1.0}folder"
                     ,"\/auditexampleextractors\/create\/in\/b":"{http:\/
\/www.alfresco.org\/model\/content\/1.0}content"
         }

      }
   ]
}
```

The `/no-error` path was used as the `dataTrigger` to activate all the `RecordValue` elements, that is, the presence of the path triggered the data rather than any specific value. `/create/derived/...` audit values show how the parent node reference was used to record values that were not part of the inbound data set.

Using the example, to search for values that are not strings, use the following:

```
% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/query/
AuditExampleExtractors/ \
                 auditexampleextractors/create/derived/parent-node-type?
                       \
                 valueType=org.alfresco.service.namespace.QName&
                       \
                 value=%7Bhttp://www.alfresco.org/model/content/1.0%7Dfolder"
{
   "count":1,
   "entries":
   [
      {
         "id":177,
         "application":AuditExampleExtractors,
         "user":admin,
         "time":"2010-09-20T20:18:52.761+01:00",
         "values":
null
      }
   ]
}

% curl -u admin:admin "http://localhost:8080/alfresco/service/api/audit/query/
AuditExampleExtractors/ \
                 auditexampleextractors/create/in/a?
                       \
                 valueType=org.alfresco.service.cmr.repository.NodeRef&
                       \
                 value=workspace://SpacesStore/37884669-0607-4527-940d-
cb34b4f07d75"
{
   "count":1,
   "entries":
   [
      {
         "id":177,
         "application":AuditExampleExtractors,
         "user":admin,
         "time":"2010-09-20T20:18:52.761+01:00",
         "values":
null
      }
   ]
}
```

It is not possible to restrict results to a specific value path. The path AND the value are enough to return a result. This does not usually yield duplicate results but it is not as restrictive as it should be. For example, generate the audit data and query for verbose output. Choose to search based on a path and a value and check that you get the correct number of results. Now choose a different path in the value list and query with that, that is, use a path and value that are not related.

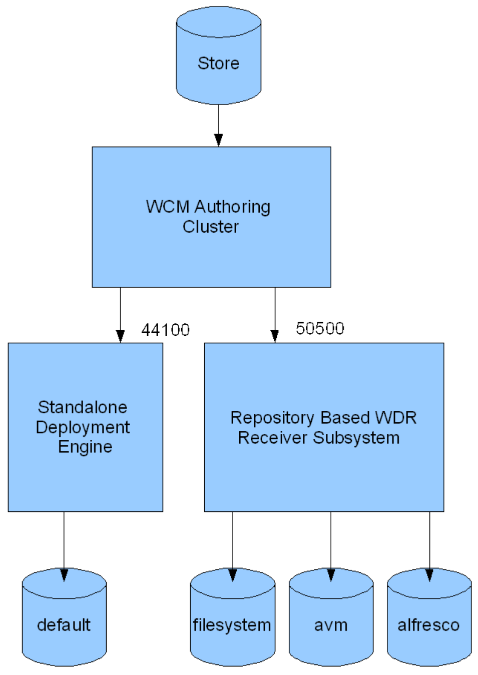
Deploying from AVM

Deployment provides a framework for pushing content from an AVM authoring environment into another environment. For example you can push out content to a flat file system, to be served up by Apache or IIS, or to another instance of Alfresco.

The AVM authoring environment provides the facilities to produce an approved and consistent view of a web project called a snapshot. Deployment takes those snapshots and pushes them out to either live or test servers. The Deployment Engine receives deployments from an AVM authoring environment and delegates the contents of the deployment to the appropriate deployment receiver target. The deployment process may be automated so that it happens automatically when content is approved for publishing.

There are two implementations of the Deployment Engine:

- Standalone deployment engine, which is a small lightweight framework that is independent of the Alfresco repository
- Deployment engine, which is a subsystem within the Alfresco repository


Store
WCM Authoring Cluster
44100
50500
Standalone Deployment Engine
Repository Based WDR Receiver Subsystem
default
filesystem
avm
alfresco

Deployments are sent to the Deployment Engine, which delegates the deployment to the registered deployment targets. Deployment targets are registered using the Web Project wizard.

Deployment targets

A deployment target is a named destination for a deployment. Alfresco deploys content through a deployment engine to a deployment target.

There are four deployment targets defined.

default
The file system deployment target for the Standalone Deployment Engine.

filesystem
The file system (`filesystem`) deployment target for the Web Delivery Runtime (WDR) Deployment Engine.

AVM
The AVM (`avm`) deployment target for the WDR Deployment Engine.

DM
The DM deployment target (`alfresco`) for the WDR Deployment Engine.

You also can add your own deployment targets.

Deployment servers are considered to be either live servers or test servers. This is used to prevent content being deployed to the wrong server. Deployments from the staging sandbox go to live servers, and from authoring and workflow sandboxes to test servers.

A contributor can deploy the state of their sandbox to a test server and preview their site. Similarly, reviewers in a workflow can deploy and preview the change set they are approving (or rejecting).

Once a test server has been deployed to, it is allocated to the user or workflow that performed the deploy. Once the user or workflow has finished with the test server it is released and returned to the pool of test servers. This happens automatically in the case of a workflow sandbox, and manually ising a user interface action for user sandboxes.

Filesystem deployment target

The file system deployment target deploys web content to a local file system. By default, there is a file system deployment target built into the standalone WCM_Deployment_Engine called `default` and also one included in the web delivery runtime subsystem called `filesystem`.

There are two methods that are important: from where you are deploying; and, to where you are deploying.

The Alfresco user interface stores content in an AVM store with a prefix of `ProjectName://www/avm_webapps`, and by default, this is followed by another folder called a `webapp`. By default, when you create a web project there will be a single `webapp` called `ROOT`. The path for `ROOT` will be `ProjectName:/www/avm_webapps/ROOT`. A file in `ROOT` will have a path like `ProjectName:/www/avm_webapps/ROOT/index.htm`.

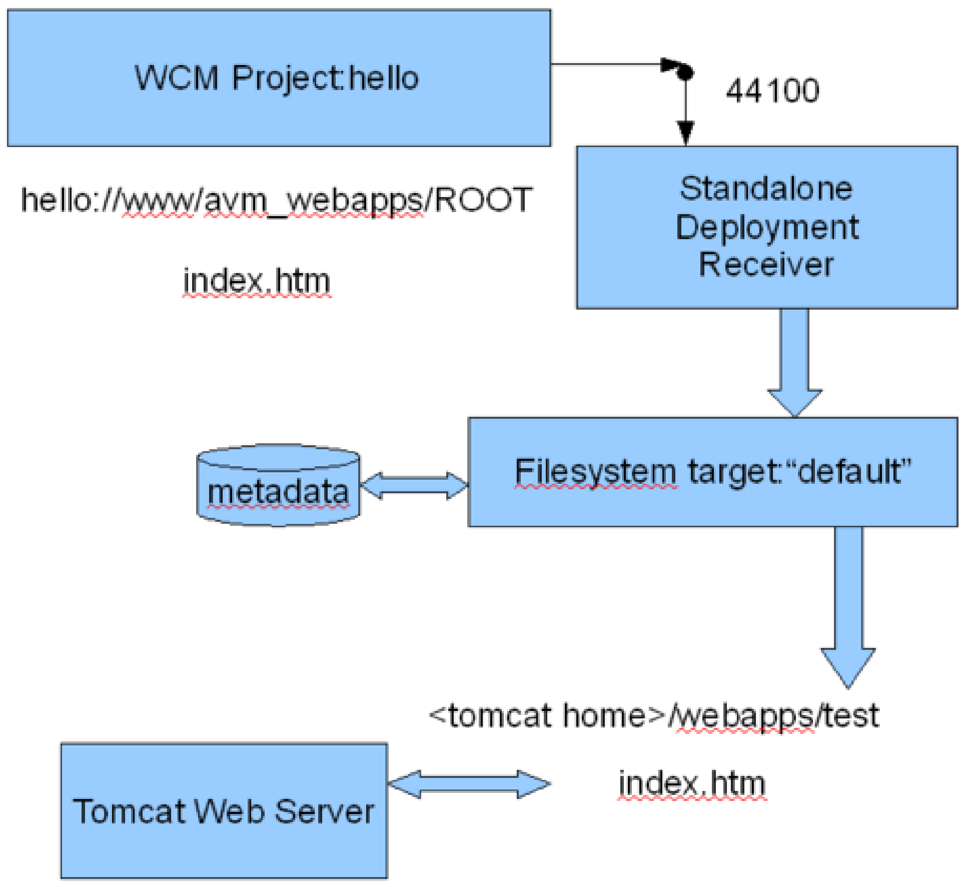
The second method is to specify where you want your files to go. For example if you are using a web server like Tomcat, then your files go into `<TOMCAT_HOME>/webapps/<webappName>`. You can then deploy all or part of this content to a file system location.

Single web project deployed to Tomcat

This is an example of how to deploy content to a separate instance of Tomcat to receive your deployment.

This example installs a test server which can be used to receive the contents of your authoring sandbox. It also sets `SourcePath` to just deploy the contents of the ROOT folder into the "hello" webapp and not the root folder itself.

The files to be deployed need to be placed in `<tomcat home>/webapps/hello`.


WCM Project:hello
44100
Standalone Deployment Receiver
hello://www/avm_webapps/ROOT
index.htm
metadata
Filesystem target:"default"
<tomcat home>/webapps/test
Tomcat Web Server
index.htm

1. Install a standalone deployment receiver on the machine with your instance of Tomcat.
2. Configure the file system deployment target that comes with the standalone deployment receiver.
3. Open the `deployment.properties` file and set the `deployment.filesystem.datadir` property to where you want your content to go.

   For example, in this case `c:/tomcat/webapps/hello`.
4. In Alfresco Explorer, create a Web Project called "hello".
5. On the Web Project Details window:
   a. Set a name of `hello`.
   b. Set the DNS Name to `hello`,
   c. Leave the default webapp as `ROOT`.
6. On the Configure Deployment Receivers window:
   a. Add Deployment Receiver.
   b. In the **Display Name** field, type `hello`.
   c. In the **Display Group** field, type `demo`.
   d. In the **Type** field, type `Test Server`.
   e. In the **Host** field, type the host name or IP address of your standalone deployment receiver.

   f. In the **Port** field, type `44100`.
   g. In the **Username** field, type `admin`, and the **Password**, type `admin`.
   h. In the **Source Path** field, type `ROOT`.
   i. In the **Target Name** field, type `default`.
7. Add a file called `index.htm` containing `hello world`.
8. Deploy your web project to your test server.

Now you should be able to open `<your tomcat webserver>/hello` and see `hello world`.

Single web project deployed to two Tomcat webapps

This example describes how to install a test server that can be used to receive the contents of your authoring sandbox.

Install a separate instance of Tomcat to receive your deployment. The files to be deployed need to be placed in `<tomcat home>/webapps/red` and `<tomcat home>webapps/blue`.

1. Install a standalone deployment receiver on the machine with your instance of Tomcat.
2. Configure the file system deployment target that comes with the standalone deployment receiver.
3. Open the `deployment.properties` file and set the `deployment.filesystem.datadir` property to where you want your content to go.

   For example, in this case `c:/tomcat/webapps`.
4. In Alfresco Explorer, create a Web Project called "colors".
5. On the Web Project Details window:
   a. Set a name of `colors`.
   b. Set the DNS Name to `colors`,
   c. Create a webapp called `red`.
   d. Create a webapp called `blue`.
   e. Change the default webapp to `red`.
6. On the Configure Deployment Receivers window:
   a. Add Deployment Receiver.
   b. In the **Display Name** field, type `colors`.
   c. In the **Display Group** field, type `demo`.
   d. In the **Type** field, type `Test Server`.
   e. In the **Host** field, type the host name or IP address of your standalone deployment receiver.
   f. In the **Port** field, type `44100`.
   g. In the **Username** field, type `admin`, and the **Password**, type `admin`.
   h. Leave the **Source Path** field blank.
   i. In the **Target Name** field, type `default`.
7. Add a file called `index.htm` containing "hello world red" to the red webapp.
8. Add a file called `index.htm` containing "hello world blue" to the blue webapp.
9. Deploy your web project to your test server.

You should be able to open `<your tomcat webserver>/red` and see `hello world red` and then open `<your tomcat webserver>/blue` and see `hello world blue`.

Filesystem deployment target properties and metadata

The following table shows the properties that can be configured on the file system deployment target.

Property	Description
`name`	This is the target name. To select this deployment target, the value of this property should be entered in the "Target Name" box of the UI. (string)
`autoFix`	The flag controlling the automatic repair of metadata. (boolean)
`rootDirectory`	The directory on the filesystem which will receive files deployed to this target. Note: this directory must be be unique to each target. At this time it is not possible to configure multiple targets that deploy to a single shared directory. (string)
`metaDataDirectory`	The directory on the filesystem which stores information relating to the current contents of this target's rootDirectory. (string)
`fileSystemReceiverService`	Indicates the File System Receiver Service bean which is associated with this deployment target. (bean reference or declaration)
`authenticator`	A link to an implementation of the DeploymentReceiverAuthenticator interface. May be either DeploymentReceiverAuthenticatorSimple (preconfigured username/password) or DeploymentReceiverAuthenticatorAuthenticationService (full Alfresco authentication.) (bean reference or declaration)

The File System Deployment Target has a simple repository of metadata to track which files, directories and versions are on the target file system. This data is maintained automatically by the File System Deployment Target. It reduces the amount of files that need to be deployed.

To force a full redeploy, you can safely delete the contents of the metadata directory, but you must ensure that a deployment is not already in progress.

The location of the metadata is configured for each target through the `metaDataDirectory` property.

If there are multiple file system targets on the same deployment engine, consider whether any of the targets share metadata or have one set of metadata per target. The simplest configuration is to use a separate folder for each target's metadata with a folder structure like `<receieverRoot>/<metadata>/<targetName>`.

File System Deployment Targets have functionality to validate that the metadata and the target deployment are consistent. Validation occurs after the deployment engine starts and after detecting an inconsistency. For example trying to delete a file that does not exist or overwriting a file that was outside the control of the File System Deployment Target.

The File System Deployment Target can either issue an error upon detecting a problem or automatically fix the problem. The autoFix parameter in the definition of the Target controls whether the File System Deployment Target will attempt to fix the metadata itself or just issue a warning. Set the value to true to fix or false to not fix.

Filesystem deployment target configuration

The following example shows a target definition for the standalone deployment engine.

```
<!--
```

```
  Define and register the deployment target called "sampleTarget which
  is used for unit tests"
 -->
 <bean
  class="org.alfresco.deployment.impl.server.DeploymentTargetRegistrationBean"
  init-method="register">

  <!-- What's the name of your target? -->
  <property name="name">
   <value>sampleTarget</value>
  </property>

  <!--  Register with the deploymentReceiverEngine -->
  <property name="registry">
   <ref bean="deploymentReceiverEngine" />
  </property>

  <property name="target">

   <!-- This is the definition of the target - you could also add a reference
 to a bean which already exists -->
   <bean
    class="org.alfresco.deployment.impl.fsr.FileSystemDeploymentTarget"
    init-method="init">

    <!--  Where to store the deployed content -->
    <property name="rootDirectory">
     <value>sampleTarget</value>
    </property>

    <!--  where to store meta data for sampleTarget-->
          <property name="metaDataDirectory">
              <value>${deployment.filesystem.metadatadir}/sampleTarget</value>
          </property>
    <property name="autoFix">
     <value>${deployment.filesystem.autofix}</value>
    </property>
    <property name="postCommit">
     <list>
      <bean class="org.alfresco.deployment.SampleRunnable" />
     </list>
    </property>
    <property name="fileSystemReceiverService">
     <ref bean="fileSystemReceiverService" />
    </property>
    <property name="name"><value>sampleTarget</value></property>
    <property name="authenticator">
     <bean

 class="org.alfresco.deployment.impl.server.DeploymentReceiverAuthenticatorSimple">
      <property name="user">
       <value>Giles</value>
      </property>
      <property name="password">
       <value>Watcher</value>
      </property>
     </bean>
    </property>
   </bean>
  </property>
 </bean>
```

avm deployment target

The AVM Deployment Target is a target which is registered with the repository-based Deployment Engine. By default its target name is `avm` although this can be changed through configuration. The AVM Deployment Target receives a deployment from an AVM authoring environment and puts the content into an AVM store where it can be used to support a dynamic web site.

AVM deployment target properties

The following properties can be configured on the AVM deployment target.

store naming pattern

The pattern for creating the live store name. By default, this is `%storeName%-live`.

root Path

The Alfresco explorer authoring environment creates assets with the path `/www/avm_webapps`. So the ROOT folder is deployed to `/www/avm_webapps/ROOT`.

The `rootPath` property allows you to specify the root of your live store. So if you do not want `/www/avm_webapps`, set it to `/`. If you want `/banana/custard/ROOT` set it to `/banana/custard`.

DM deployment target

The DM Deployment Target receives a deployment from an AVM authoring environment and puts the content into the workspace spaces store where it can be used to support a dynamic website.

The DM Deployment Target is a target which is registered with the repository based Deployment Engine. By default its target name is `alfresco` although this can be changed through configuration.

DM deployment target properties

The following properties can be configured for the DM Deployment Target.

Store name mapping

The authoring environment for a WCM Web Project consists of a set of related AVM stores. There is a staging store, one or more author stores and possibly workflow stores. The different stores have a naming convention for their store names.

The consolidate flag says deploy all these related stores to the same location. If it is turned off by setting deployment.dmr.consolidate to false there will be a separate paths for each store and content will be duplicated in the DM store. For example, set the following in the `alfresco.global.properties` file:

```
deployment.dmr.consolidate= true | false
deployment.dmr.name=alfresco
```

You can use spring to plug in your own implementation of the StoreNameMapper interface to control your project name mappings.

Root location mapping

The default implementation of `RootMapper`, the `RootMapperImpl` class, allows you to specify a default location for all web projects and also a map of mappings, one for each web project. By default, the web projects are deployed to `/app:company_home/app:wcm_deployed`.

Standalone deployment receiver

The Standalone Deployment Engine consists of a small server that receives updates from an Alfresco repository and publishes them to its deployment targets. It does not have the benefits of a full repository but is a small and tightly focused server.

It is configured with a single file system deployment target, which places the contents of the deployment onto a flat file system, and is typically served up by a web or application server. For performance reasons, only the difference between the old version and the new version is sent.

The destination file server receiver has to be running with its RMI registry port and service port (by default, 44100 and 44101, respectively) accessible, unless you have configured it to run over another transport.

Configuring the standalone deployment receiver

This section describes how to configure the standalone deployment receiver. The configuration files needed for configuration are the `deployment.properties` file and the `application-context.xml` file.

Ensure that you have installed the standalone deployment receiver. See Installing the standalone deployment receiver on page 59.

1. Locate the `deployment` installation directory, for example:

   - (Windows) `c:/Alfresco/Deployment`
   - (Linux) `/opt/alfresco/deployment`

   This directory contains deployment target definitions and plug in definitions. The spring definitions of the deployment targets are read from this directory. All files matching the pattern `deployment/*-context.xml` and `deployment/*-target.xml` are loaded by the deployment engine. Targets are loaded after the context files, so each target has all spring beans available when it is defined.
2. Open the `deployment.properties` file.

   The `deployment.properties` file contains a simple configuration for the standalone deployment receiver. The file is created by the deployment project **deployer**.
3. The file shows the following properties:

   ```
   ; Stand alone deployment receiver properties

   ; filesystem receiver configuration
   deployment.filesystem.datadir=/opt/alfresco/deployment/depdata
   deployment.filesystem.logdir=/opt/alfresco/deployment/deplog
   deployment.filesystem.metadatadir=/opt/alfresco/deployment/depmetadata
   deployment.filesystem.autofix=true
   deployment.filesystem.errorOnOverwrite=false

   ; default filesystem target configuration
   deployment.filesystem.default.metadatadir=
   ${deployment.filesystem.metadatadir}/default
   deployment.filesystem.default.rootdir=target
   deployment.filesystem.default.name=default
   deployment.filesystem.default.user=admin
   deployment.filesystem.default.password=admin

   ; Deployment Engine configuration
   deployment.rmi.port=44100
   deployment.rmi.service.port=44101

   ; Stand alone deployment server specific properties
   deployment.user=admin
   deployment.password=admin
   ```

   The default target set in this file is a working example.
4. Modify the properties to reflect the relevant settings for your system.

   For Windows directory locations, the backslashes need to be escaped. For example, use `C:\\directory1\\directory2`. Alternatively, you can use the slash character as a separator, for example, `C:/directory1/directory2`.

a. Ensure that the following properties point to the locations for the deployment files and metadata:

```
deployment.filesystem.datadir=/opt/alfresco/deployment/depdata
deployment.filesystem.metadatadir=/opt/alfresco/deployment/
depmetadata
```

b. Modify the following properties when using the “default” target.

```
deployment.filesystem.default.rootdir={deployment.filesystem.datadir}/
default

deployment.filesystem.default.metadatadir=
${deployment.filesystem.metadatadir}/default

deployment.filesystem.default.user=admin
deployment.filesystem.default.password=admin
```

c. Add any further targets to the file. For example, for a target called "foo":

```
deployment.filesystem.foo.rootdir= {deployment.filesystem.datadir}/foo

deployment.filesystem.foo.metadatadir=
${deployment.filesystem.metadatadir}/foo

deployment.filesystem.foo.user=admin
deployment.filesystem.foo.password=admin
```

d. Modify the following properties to specify the user who can shut down the standalone deployment server.

```
deployment.user=admin
deployment.password=admin
```

5. Save your file.
6. Restart the deployment engine.

The following is a sample `application-context.xml` file and it shows how the `deployment.properties`, context files and the targets are read.

```
<beans>
   <bean id="properties"

 class="org.springframework.beans.factory.config.PropertyPlaceholderConfigurer">
     <property name="ignoreUnresolvablePlaceholders">
          <value>true</value>
     </property>
        <property name="locations">
           <list>
              <value>classpath:deployment.properties</value>
           </list>
       </property>
   </bean>

    <import resource="classpath*:deployment/*-context.xml" />
    <import resource="classpath*:deployment/*-target.xml" />

</beans>
```

The standalone deployment engine uses `log4j` for problem determination, and logging for the deployment engine is placed in the `log` directory.

Your spring definitions of the deployment targets are read from this directory. All files matching the pattern `deployment/*-target.xml` are loaded by the deployment engine.

Targets are loaded after the context files. So each target has all spring beans available to it when it is defined

Configuring the standalone deployment receiver as a Windows service

This section describes the steps for configuring the standalone deployment receiver as a Windows service.

1. Download Java Wrapper from following URL.

   `http://wrapper.tanukisoftware.org/doc/e ... wnload.jsp`
2. Unzip the wrapper to a folder.

   For example, `C:\wrapper`.
3. Download the Standalone Deployment Receiver.
4. Copy all the JAR files from the Standalone Deployment Receiver to the `wrapper\lib` directory.
5. Create a empty JAR file called `deployment-config.jar`.
6. Add the `deployment.properties` file and the deployment folder with all of your deployment target XML files from the Standalone Deployment Receiver to the new JAR file.
7. Copy the JAR file to the `wrapper\lib` directory.
8. Copy following files from Standalone Deployment Receiver to the `wrapper\bin` directory.
   a. `application-context.xml`
   b. `shutdown-context.xml`
9. Copy the following files from the `wrapper\src\bin` directory to the `wrapper\bin` directory, and then remove `.in` from file name to make it batch file.
   a. `InstallApp-NT.bat.in` (after rename it will be `InstallApp-NT.bat`)
   b. `UninstallApp-NT.bat.in` (after rename it will be `UninstallApp-NT.bat`
10. Open the `wrapper/conf/wrapper.conf` file and make following changes:
    a. Change `wrapper.java.command` to `%JAVA_HOME%/bin/java`.
    b. Change `wrapper.java.mainclass` to `org.tanukisoftware.wrapper.WrapperStartStopApp`.
11. Add following classpath entries. Remove any default entries for classpath:
    a. `wrapper.java.classpath.1=../lib/wrapper.jar`
    b. `wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar`
    c. `wrapper.java.classpath.4=../lib/alfresco-deployment-3.2.0r.jar`
    d. `wrapper.java.classpath.5=../lib/alfresco-core-3.2.0r.jar`
    e. `wrapper.java.classpath.6=../lib/alfresco-repository-3.2.0r.jar`
    f. `wrapper.java.classpath.7=../lib/commons-logging-1.1.jar`
    g. `wrapper.java.classpath.8=../lib/jug-lgpl-2.0.0.jar`
    h. `wrapper.java.classpath.9=../lib/log4j-1.2.15.jar`
    i. `wrapper.java.classpath.10=../lib/spring-2.0.8.jar`
    j. `wrapper.java.classpath.11=../lib/deployment-config.jar`
    k. `#wrapper.java.classpath.10=../lib/deployment.properties`
    l. `#wrapper.java.classpath.11=../lib/shutdown-context.xml`
    m. `#wrapper.java.classpath.12=../lib/application-context.xml`
12. Add following additions to parameters:
    a. `wrapper.java.additional.2=-Dcatalina.base=..`

   b. `wrapper.java.additional.3=-Dcatalina.home=..`
   c. `wrapper.java.additional.4=-Djava.io.tmpdir=../temp`

13. Add following Application Parameters:
    a. `wrapper.app.parameter.1=org.alfresco.deployment.Main`
    b. `wrapper.app.parameter.2=1`
    c. `wrapper.app.parameter.3=application-context.xml`
    d. `wrapper.app.parameter.4=org.alfresco.deployment.Main`
    e. `wrapper.app.parameter.5=TRUE`
    f. `wrapper.app.parameter.6=1`
    g. `wrapper.app.parameter.7=shutdown-context.xml`
14. Change service name related changes as per below:
    a. `wrapper.name=Alfresco Standalone Deployment Receiver`

       Name of the service.
    b. `wrapper.displayname=Alfresco Standalone Deployment Receiver`

       Display name of the service.
    c. `wrapper.description=Alfresco Standalone Deployment Receiver`

       Description of the service.
15. Click the `wrapper\bin\InstallApp-NT.bat` file. You should be able to see service name **Alfresco Standalone Deployment Receiver**. The first time you start it, you need to start the service manually.

Check the service log in the `wrapper\log\wrapper.log` file.

Administering Explorer from the Administration Console

The Administration Console enables Alfresco administrators to create and manage users and groups, manage categories, import and export spaces and content, and perform other administrative tasks from within Alfresco Explorer.

Managing users

In Alfresco a home space is a place for users to store their items.

By default a user has full control over items in their space and other users are given guest access to that space.

Users can navigate to their home space by clicking **My Home** in the toolbar.

Creating a user

The **New User Wizard** enables you to create a new user, creating the user's home space at the same time.

1. In the toolbar, click **(Administration Console)**.
2. Click **Manage System Users**.
3. In the space header, click **Create User**.
4. In Step One, Person Properties, enter information about the user being created and click **Next**.

5. In Step Two, User Properties, provide user information and click **Next**.

   The password is case sensitive. You must provide a **Home Space Name** to create the user's home space.
6. In Step Three, Summary, check that all information entered is correct and click **Finish**.

   To view the new user, use the search feature in the **Users** pane or click **Show All**.
7. Click **Close** to return to the **Administration Console**.

Editing user details

The **Edit User Wizard** enables you to modify the person and user properties of a user’s account.

1. In the toolbar, click **(Administration Console)**.
2. Click **Manage System Users**.
3. On the **Manage System Users** page, use the search feature to locate the user whose account you wish to edit or click **Show All** to display all users.

   Selecting to display all users may take some time if there are many users in the system.
4. Click **(Modify)** for the user of interest.
5. In the **Edit User Wizard**, modify the person and/or user properties as desired. Click **Next** and **Back** to work through the steps in the **Edit User Wizard**. Make your changes to the appropriate step(s).
6. Click **Finish** to process the changes.
7. Click **Close** to return to the **Administration Console**.

Changing a user's password

You must change a user’s password separately from editing the user account.

It is important to remember that passwords are case sensitive.

1. In the toolbar, click **(Administration Console)**.
2. Click **Manage System Users**.
3. On the **Manage System Users** page, use the search feature to locate the user whose account you wish to edit or click **Show All** to display all users.

   Selecting to display all users may take some time if there are many users in the system.
4. Click **(Change Password)** for the user of interest.
5. On the **Change Password** page, enter and confirm the new password for this user in the **Password** and **Confirm** boxes.

   The password is case sensitive.
6. Click **Finish** to process the change.
7. Click **Close** to return to the **Administration Console**.

Deleting a user

Delete a user to prevent that person from having access to the Alfresco system.

Only an Administrator can delete a user.

1. In the toolbar, click **(Administration Console)**.
2. Click **Manage System Users**.

3. On the **Manage System Users** page, use the search feature to locate the user whose account you wish to edit or click **Show All** to display all users.

   Selecting to display all users may take some time if there are many users in the system.
4. Click **(Delete)** for the user of interest.

   A message prompts you to confirm the deletion of the selected user.
5. Click **Yes**.
6. Click **Close** to return to the **Administration Console**.

Managing user groups

User groups enable you to organize your Alfresco users.

Groups allow you to quickly and easily give all members of a group abilities in a space that are specific to that group. Once you create a group, you manage its membership by inviting and removing users.

By default, all users are members of the group called **Everyone** with guest abilities. Users can belong to more than one group.

To assist with the management of the Alfresco administrative users, a default group, ALFRESCO_ADMINISTRATORS, has been created for you. This group enables you to easily configure the permissions for all Alfresco administrators. The initial administrator (the default "admin" user) can create additional administrative users by adding users to this group.

When a web project is created and users are invited to that project, a user group is created automatically in the Administration Console for the project. However, web project membership must be managed within the web project and not within the Administration Console.

The **Groups Management** page header provides functionality to toggle between the **Groups** view and the **Details** view. To aid navigation, a breadcrumb showing the groups hierarchy appears above the **Groups** list. Click the links in this breadcrumb to navigate the groups hierarchy.

Creating a user group

Create a user group to organize Alfresco users.

Top level groups reside beneath the heading **Root Groups**. A group can contain sub-groups. Only an Administrator can create a user group.

1. In the toolbar, click **(Administration Console)**.
2. Click **Manage User Groups**.
3. On the **Groups Management** page, use the search feature to locate a specific user group or click **Show All** to display the existing root, or top-level, groups.

   If not already displayed, click **Root Groups** beneath the space header to return to the top-level group.
4. Navigate to the user group where you want to create a group.
5. Click **Create Group**. To create a sub-group, click **(Create Sub-Group)** associated with the group you wish to be the parent.
6. On the **Create Group** page, enter the name of the group you are creating in the **Identifier** box.

   Once you provide an **Identifier** for the group, you cannot change it.
7. Click **Create Group**.

An additional viewing option in the space header allows you to view either all groups and sub-groups beneath the currently selected group or only the immediate child groups of the currently selected group. To the right of the icon, select **All** or **Children**, as preferred. Once you set the filter option, click **Show All** to populate the Groups pane.

8. Click **Close** to return to the **Administration Console**.

Deleting a user group

Delete a group to permanently remove it from the system.

Deleting a group also deletes all sub-groups and users associated with it. Only an Administrator can delete a user group.

1. In the toolbar, click **(Administration Console)**.
2. Click **Manage User Groups**.
3. On the **Groups Management** page, use the search feature to locate a specific user group or click **Show All** to display the existing root, or top-level, groups.

   If not already displayed, click **Root Groups** beneath the space header to return to the top-level group.
4. Navigate to the user group you want to delete.

   The page header displays the name of the selected group.
5. In the **More Actions** menu, click **Delete Group**.

   A message prompts you to confirm the deletion of the selected user group.
6. Click **Delete**.
7. Click **Close** to return to the **Administration Console**.

Adding a user to a user group

Add any number of Alfresco users to a user group.

Only an Administrator can add a user to a user group.

1. In the toolbar, click **(Administration Console)**.
2. Click **Manage User Groups**.
3. On the **Groups Management** page, use the search feature to locate a specific user group or click **Show All** to display the existing root, or top-level, groups.

   If not already displayed, click **Root Groups** beneath the space header to return to the top-level group.
4. Navigate to the user group you want to add users to.

   The page header displays the name of the selected group.
5. In the **More Actions** menu, click **Add User**.
6. Use the search feature to locate users.

   You must enter a minimum of one (1) character.
7. Click to select the users you want to add to the group.

   Use SHIFT to select multiple, consecutive users; use CTRL to select multiple, nonconsecutive users.
8. Click **Add** to add the user(s) to the **Selected Users** list.

   Click **(Remove)** to remove a user from this list.

9. Click **OK**.
10. Click **Close** to return to the **Administration Console**.

Removing a user from a user group

A user that has been added to a user group can be removed.

Only an Administrator can remove a user from a user group.

1. In the toolbar, click **(Administration Console)**.
2. Click **Manage User Groups**.
3. On the **Groups Management** page, use the search feature to locate a specific user group or click **Show All** to display the existing root, or top-level, groups.

   If not already displayed, click **Root Groups** beneath the space header to return to the top-level group.
4. Navigate to the user group you want to remove users from.

   The page header displays the name of the selected group.
5. On the **Groups Management** page, click **(Remove)** for the user you want to remove from the group.

   The user is removed without a prompt to confirm the action.
6. Click **Close** to return to the **Administration Console**.

Managing categories

Categories allow users to quickly and easily organize their content by classifying content items.

An Administrator creates and manages the categories, which are organized into related groups to form a hierarchy. Users then link content items to one or more categories to classify the content items.

The **Category Management** page header provides functionality to toggle between the **Categories** view and the **Details** view. To aid navigation, a hierarchy path appears beneath the page header. Click the links in this path to navigate the category hierarchy.

Adding a category

Add a category at the top level or as a sub-category to an existing category.

Only an Administrator can add a category.

1. In the toolbar, click **(Administration Console)**.
2. Click **Category Management**.
3. Click **Add Category** to create a top-level category.

   To create a sub-category, navigate the existing categories, select the category for which you are creating a sub-category, and click **Add Category**.
4. On the **New Category** page, type the relevant information in the **Name** and **Description** boxes.
5. Click **New Category**.
6. Click **Close** to return to the **Administration Console**.

Deleting a category

Delete a category that you no longer want users to be able to access.

Deleting a category deletes its sub-categories and breaks any existing links between content items and the categories being deleted. Only an Administrator can delete a category.

1. In the toolbar, click **(Administration Console)**.
2. Click **Category Management**.
3. Navigate to the category you want to delete.

   The page header displays the name of the selected category.
4. Click **(Delete Category)**.

   Deleting a category also deletes its sub-categories. A message informs you if content is linked to the category you are deleting.

   A message prompts you to confirm the deletion of the selected category.
5. Click **Delete**.
6. Click **Close** to return to the **Administration Console**.

Editing a category

Edit a category to change its name or description.

Changing the name does not break any links between content and the category. Only an Administrator can edit a category.

1. In the toolbar, click **(Administration Console)**.
2. Click **Category Management**.
3. Navigate to the category you want to edit.

   The page header displays the name of the selected category.
4. Click **(Edit Category)**.
5. On the **Edit Category** page, modify the properties as desired.
6. Click **Finish**.
7. Click **Close** to return to the **Administration Console**.

Importing the ACP file into a space

The Import function in the Administration Console enables you to import an exported space to any space within Alfresco or into another Alfresco repository altogether.

An exported space is bundled into an Alfresco Content Package (ACP). Importing the ACP into a new location expands the package to the original structure of the space.

1. Navigate to the space into which you want to import content.

   The space header displays the name and details of the space.
2. In the toolbar, click **(Administration Console)**.
3. Click **Import**.

   The space header indicates the space into which you will import your file.
4. Click **Browse** then locate and select the ACP file you want to import.
5. Check **Run import in background** if you want the import to occur while you are still working.
6. Click **OK**.

The ACP file expands, putting the space, sub spaces, and content in the space.

7. Click **Close** to return to the current space.

Exporting a space and its contents

The Export function in the Administration Console enables you to copy an Alfresco space and its contents.

Exporting a space differs from copying a space in that the export function bundles all rules, workflow, properties, and metadata associated with the space into an Alfresco Content Package (ACP). You can import the ACP to a different space within Alfresco or into another Alfresco repository altogether.

1. Navigate to the space you want to export.

   The space header displays the name and details of the space.
2. In the toolbar, click **(Administration Console)**.
3. Click **Export**.

   The space header indicates the space selected for export.
4. On the **Export** page, type a name for the export package (ACP).
5. Select a destination location to store the resulting ACP file.
6. Select **Current Space** as what you would like to export from.
   a. Check **Include Children** if you want to export sub spaces.
   b. Check **Include this Space** if you want to export the selected space as well as the children.
7. Check **Run export in background** if you want the export to occur while you are still working.
8. Click **OK**.

   The ACP file is created and stored in the destination location.
9. Click **Close** to return to the current space.

Viewing System Information

The System Information feature in the Administration Console displays settings and configuration values used by the environment on which Alfresco runs. The information available is read-only and is useful to Support for checking and diagnosing issues.

1. In the toolbar, click **(Administration Console)**.
2. Click **System Information**.
3. Click ▶ to expand a pane to view its contents; click ▼ to collapse the pane.
4. Click **Close** to return to the **Administration Console**.

Using the Node Browser

The Node Browser is a debugging aid that allows you to browse the raw Alfresco repository structure. This feature is intended for developers responsible for customizing the application.

This is a read-only feature with basic search capability.

1. In the toolbar, click **(Administration Console)**.

2. Click **Node Browser**.
3. On the **Alfresco Node Browser** page, click the store of interest.

   Each store is an area of the repository and within each store, the nodes of that store are organized hierarchically. The node displayed is the root node of the selected store.
4. Search the selected store, as needed:
   a. Select the search type: **noderef**, **xpath**, **lucene**, **selectnodes**.
   b. Enter the search criteria in the field provided.
   c. Click **Search**.
5. Click **Close** to return to the **Administration Console**.

Administering Share from the Admin Console

The Admin Console enables Alfresco Administrators to create and manage both users and groups from within Share. It also provides the functionality for setting application preferences. Only those users who are members of the group ALFRESCO_ADMINISTRATORS have access to the Admin Console.

Specifying application preferences

The Application tool in the Admin Console enables you to set application preferences.

Selecting a theme

The Application tool enables you to select a color scheme for the Share user interface.

The change affects all users of the Share instance from the next time they log in. The selected theme persists across sessions.

1. On the toolbar, expand the **More** menu and click **Application** in the Tools list.

   The **Options** page appears.
2. Select the desired theme from the list provided.
3. Click **Apply**.

The page refreshes to display with the selected theme.

Managing groups

The Groups tool in the Admin Console enables you to create and manage Share user groups.

Browsing the user groups

The Groups page contains a multi-paned panel that allows you to navigate the hierarchy of Share user groups.

1. On the toolbar, expand the **More** menu and click **Groups** in the Tools list.
2. On the **Groups** page, click **Browse**.

   The leftmost pane displays all top-level user groups.
3. Click a group to display its contents in the panel directly to the right.

   The content can be subgroups and/or individual users. Text at the bottom of this panel indicates the number of groups and users that belong to the selected group.

4. As you browse the group structure, a navigation path is displayed at the top of the panel indicating your selections stemming from the initial pane. Click any link in this path to step back to that selection.
5. To browse a different group, click the first link in the navigation path to return to the top-level groups, then select a new group to browse.

Searching for a group

The Search feature enables you to locate any Share user group, regardless of where it exists in the group hierarchy. Once located, you can edit or delete the group.

1. On the toolbar, expand the **More** menu and click **Groups** in the Tools list.
2. In the search box, type the full or partial identifier, not display name, of the desired group.

   You must enter a minimum of one (1) character. The search is not case sensitive.
3. Click **Search**.

   In the results table, click the column headings to sort the results as desired.

Creating a new group

The Admin Console enables you to create both top level user groups and subgroups within existing groups.

1. On the toolbar, expand the **More** menu and click **Groups** in the Tools list.
2. On the **Groups** page, click **Browse**.

   The leftmost pane displays all top-level user groups.
3. Navigate to the user group where you want to create the new group.
   - To create a top-level group, click the **New Group** icon at the top of the initial pane.
   - To create a subgroup, browse the group structure to locate the desired parent group. Select this group and then click the **New Subgroup** icon at the top of the pane immediately to the right.

   The **New Group** page appears. Fields marked with an asterisk (*) are required.
4. Complete the required user details.
5. Click **Create Group**.

   If you intend to immediately create another group at the same level, click **Create and Create Another**. This creates the group specified and clears the fields without returning you to the **Groups** page.

Editing an existing group

Edit a user group to change the group's display name. Once created, you cannot edit the group's Identifier.

1. On the toolbar, expand the **More** menu and click **Groups** in the Tools list.
2. On the **Groups** page, click **Browse**.

   The leftmost pane displays all top-level user groups.
3. Navigate the group structure or use the search feature to locate the user group you want to edit.

   You must enter a minimum of one (1) character. The search is not case sensitive.
4. Position the cursor over the desired group to display its available actions.
5. Click the **Edit Group** icon.
6. Edit the group's **Display Name**.

7. Click **Save Changes**.

Deleting an existing group

Delete a user group to remove it from the system.

1. On the toolbar, expand the **More** menu and click **Groups** in the Tools list.
2. On the **Groups** page, click **Browse**.

   The leftmost pane displays all top-level user groups.
3. Navigate the group structure or use the search feature to locate the user group you want to delete.

   You must enter a minimum of one (1) character. The search is not case sensitive.
4. Position the cursor over the desired group to display its available actions.
5. Click the **Delete Group** icon.

   A message prompts you to confirm the deletion.
6. Click **Delete**.

Managing group membership

To populate a user group, you can add both individual users and existing user groups.

1. On the toolbar, expand the **More** menu and click **Groups** in the Tools list.
2. On the **Groups** page, click **Browse**.

   The leftmost pane displays all top-level user groups.
3. Navigate the group structure to locate the user group you want to work with. Click the desired user group to select it.
4. Using the icons in the pane directly to the right of where you selected the group, perform the desired action:
   a. To add a user, click the **Add User** icon. Using the search feature provided, locate the user you want to add to the selected group. Click **Add** to the right of the desired user.
   b. To add a group, click the **Add Group** icon. Using the search feature provided, locate the group you want to add to the selected group. Click **Add** to the right of the desired user.

   The individual user or group is added as a child to the group selected in the panel.

Managing replication jobs

The Replication Jobs tool in the Admin Console enables you to create and manage replication jobs in Share.

A replication job specifies the content to be replicated; the day and time the job is to be performed; and the target location for the replicated content. The job, which is controlled by the Replication Service, calls the Transfer Service, which allows folders and content to be automatically copied between Alfresco repositories.

A replication job can be run according to a schedule or on-demand.

By default, the replicated content is read-only in the target repository. This ensures the integrity of the content is not compromised by uncontrolled updates.

Viewing a replication job

Select a replication job to view the job details and display the available actions.

1. On the toolbar, expand the **More** menu and click **Replication Jobs** in the Tools list.

The Replication Jobs page displays a summary of recently run jobs and a list of existing replication jobs. In this list, use the menu provided to sort the jobs by Status, Name, and Last Run Date.

2. In the Jobs section, click a job to view its details.

   The job appears highlighted in the list and its details appear on the right side of the page.

Creating a new replication job

You can create any number of replication jobs to suit your needs.

1. On the toolbar, expand the **More** menu and click **Replication Jobs** in the Tools list.
2. In the Jobs section, click **Create Job**.

   The Create New Replication Job page appears. Fields marked with an asterisk (*) are required.
3. Complete the form.
   a. Provide a name and description for the job.

      Only the job name is required.

   b. Select the payload.

      In the Payload section, click **Select**. Navigate the repository and click **Add** to the right of each branch of the repository that you want to include in the payload; this is the content that will be replicated (copied) when the job is run. Click **OK**.

   c. Specify the transfer target.

      In the Transfer Target section, click **Select**. Navigate the Transfer Target Groups and click **Select** to the right of the desired target. Click **OK**.

      Out of the box, one target group, *default group*, is available. Use the Repository Browser to create additional target groups (Data Dictionary > Transfers > Transfer Target Group). A rule defined on the Transfer Groups folder specializes the type of any folder created within it.

   d. Schedule the replication job.

      Select the **Schedule job** check box, then enter the date and time the job is to run. Specify the repeat period for this job.

   e. Enable the job.

      Select the **Enabled** check box.

      You must enable a replication job for it to be run.
4. Click **Create Job**.

   The job created appears highlighted in the Jobs list. The job details appear on the right side of the page.

Managing existing jobs

The Replication Jobs page of the Admin Console displays a list of all existing replication jobs. For each job in this list, you can perform any of the following actions to manage and maintain the jobs:

- Edit a job
- Manually run a job
- Cancel a job
- Delete a job

Editing a replication job

You can easily update existing replication jobs. In addition to changing the job details, you can use this feature to disable a job so that it will not be run.

1. On the toolbar, expand the **More** menu and click **Replication Jobs** in the Tools list.
2. In the Jobs section, click the job you want to edit.

   The job appears highlighted in the list and its details appear on the right side of the page.
3. Click **Edit**.

   The Edit Replication Job page appears.
4. Edit the replication job as necessary. All job details—name, description, payload, transfer target, and schedule—are available for editing.

   Add and remove source items as necessary. Click **Remove** to the right of a single item to remove it. Click **Remove All** beneath the list to remove all items.

   Deselect the **Enabled** check box to prevent the job from being run.
5. Click **Save**.

   The main page displays the updated job details.

Manually running a replication job

The **Run Job** feature enables you to manually run a replication job. You can do this at any time. If a schedule is set for the job, it remains in place and will be run at the appropriate time.

1. On the toolbar, expand the **More** menu and click **Replication Jobs** in the Tools list.
2. In the Jobs section, click the job you want to run.

   The job appears highlighted in the list and its details appear on the right side of the page.

   For a job to be run, it must be enabled.
3. Click **Run Job**.

   The Status section on the right side of the page indicates that the job is running. The date and time the job started is displayed.

Cancelling a replication job

You can cancel a job that is currently running, regardless of whether it was started automatically (that is, it is a scheduled job) or manually.

1. On the toolbar, expand the **More** menu and click **Replication Jobs** in the Tools list.
2. In the Jobs section, click the currently running job that you want to cancel.

   An icon (🔄) to the left of the job name indicates a job is currently running.

   The Status section on the right side of the page indicates the start time of the selected job.

   If the job was already displayed, you may need to click **Refresh** to update the status.
3. Click **Cancel Job**.

   The job is stopped and a report is created.

Deleting a replication job

If you no longer need a replication job, you can delete it from the Jobs list. If there is a chance you might need the job again, you may prefer to edit the job and simply disable it.

1. On the toolbar, expand the **More** menu and click **Replication Jobs** in the Tools list.
2. In the Jobs section, click the job you want to delete.

The job appears highlighted in the list and its details appear on the right side of the page.

3. Click **Delete**.

   A message prompts you to confirm the deletion of the selected job.
4. Click **Delete**.

   The selected job is deleted from the jobs list.

Viewing replication job reports

Two reports—local and remote—are available for each replication job run successfully.

The local report is the transfer report from the sending system, which manages the content being transferred to the receiving system. The local report details the speed at which the files were transferred and other related details.

The remote report is the transfer report from the receiving system. This report indicates whether files were created, updated, modified, or deleted as part of the transfer.

1. On the toolbar, expand the **More** menu and click **Replication Jobs** in the Tools list.
2. In the Jobs section, click the job you want want to view.

   The job appears highlighted in the list and its details appear on the right side of the page.
3. Select the desired report:
   - Click **View Local Report**.
   - Click **View Remote Report**.

   The selected report displays on the details page of the Repository Document Library.

Performing a repository dump

In Share, configuration changes can be made using file changes (`alfresco-global.properties`), properties, and JMX. Regardless of how the changes were made, the JMX interface holds the current values of a running system. When talking to Alfresco Support, it may be convenient to have a dump of these settings.

The **Repository** tool provides a web JMX dumper so you can easily access this information.

1. On the toolbar, expand the **More** menu and click **Repository** in the Tools list.
2. Click the **Download JMX Zip Dump** link.
3. Save the file to a convenient location on your computer.

   The saved .zip file has the name **jmxdump** appended with the current date (in the format YYYY_MM_DD).
4. Extract the file and open the .txt file with your preferred program.

Managing users

The Users tool in the Admin Console enables you to create and manage the Share user accounts.

Searching for and viewing a user account

The User Search feature enables you to locate any Share user and view that user's account information.

1. On the toolbar, expand the **More** menu and click **Users** in the Tools list.

   The **User Search** page appears.

2. In the search box, type the full or partial name of the desired user.

   You must enter a minimum of one (1) character. The search is not case sensitive.
3. Click **Search**.

   In the results table, click the column headings to sort the results as desired.

   In the first column, a green dot indicates the user account is currently enabled; a red dot indicates the account is disabled.
4. Click the name of the desired user to display the related user profile and account details.

The **User Profile** page displays. From here you can edit or delete the user account.

Creating a user account

The Admin Console enables you to easily create users accounts.

1. On the toolbar, expand the **More** menu and click **Users** in the Tools list.

   The **User Search** page appears.
2. Click **New User**.

   The **New User** page appears. Fields marked with an asterisk (*) are required.
3. Complete the required user details.
4. If desired, add the user to existing user groups:
   a. In the search box, type the full or partial name of the desired group.

      You must enter a minimum of one (1) character. The search is not case sensitive.
   b. Click **Search**.
   c. In the list of returned results, click **Add** to the right of each group you want the user to be a part of.

      The groups appear beneath the **Groups** list. Click a group to remove it.
   d. Perform additional searches as necessary to locate and add more groups.
5. In the **Quota** box, specify the maximum space available for this user and select the appropriate unit (GB, MB, or KB).

   This information is not required. When no quota is provided, the user has no space limitations.
6. Click **Create User**.

   If you intend to immediately create another user, click **Create and Create Another**. This creates the user account specified and clears the fields without returning you to the **User Search** page.

Editing a user account

Edit a user account to change a user's personal information, group affiliation, quota, and password.

1. On the toolbar, expand the **More** menu and click **Users** in the Tools list.

   The **User Search** page appears.
2. Search for and select the desired user.
3. On the **User Profile** page, click **Edit User**.

   The **Edit User** page appears.
4. Edit the user's personal details as necessary: **First Name**, **Last Name**, and **Email**.
5. Edit the groups to which this user belongs:

   a. To add a user to a group, use the search field provided to locate the desired group. You must enter a minimum of one (1) character. Click **Add** to the right of each group you want the user to be a part of. The groups the user belongs to display beneath the **Groups** list.
   b. To remove a user from a group, simply click the group you want to remove beneath the **Groups** list.
6. Provide or edit the **Quota**, which indicates the maximum space available for this user. Select the appropriate unit.
7. Change the password, if necessary.
8. Click **Use Default** to reset the user's picture to the default image.
9. Click **Save Changes**.

Deleting a user account

Delete a user account to remove the user from the system.

To retain the user account while denying the user access to the application, consider simply disabling the user account.

1. On the toolbar, expand the **More** menu and click **Users** in the Tools list.

   The **User Search** page appears.
2. Search for and select the desired user.
3. On the **User Profile** page, click **Delete User**.

   A message prompts you to confirm the deletion.
4. Click **Delete**.

Disabling a user account

Disable a user account to prevent a user from having any access to the application. You perform this task as part of editing a user account.

1. On the toolbar, expand the **More** menu and click **Users** in the Tools list.

   The **User Search** page appears.
2. Search for and select the desired user.
3. On the **User Profile** page, click **Edit User**.

   The **Edit User** page appears.
4. Click **Disable Account**.

   A checkmark indicates the account for the current user will be disabled.
5. Click **Save Changes**.

   On the **User Profile** page, the Account Status appears as **Disabled**. On the **User Search** page, the user displays in the search results list with a red dot, indicating the account is disabled.

Changing a user's password

You can change a user’s password as part of editing the user account.

1. On the toolbar, expand the **More** menu and click **Users** in the Tools list.

   The **User Search** page appears.
2. Search for and select the desired user.
3. On the **User Profile** page, click **Edit User**.

The **Edit User** page appears.

4. Enter and confirm the new password for this user in the **New Password** and **Verify Password** boxes.

   The password is case sensitive.
5. Click **Save Changes**.

Managing the user's group membership

Within a user account, you have the opportunity to manage the user’s membership in existing user groups. You can edit a use account at any time to add and remove the user from groups.

1. On the toolbar, expand the **More** menu and click **Users** in the Tools list.

   The **User Search** page appears.
2. Search for and select the desired user.
3. On the **User Profile** page, click **Edit User**.

   The **Edit User** page appears.
4. Edit the groups to which this user belongs:
   a. To add a user to a group, use the search field provided to locate the desired group. You must enter a minimum of one (1) character. Click **Add** to the right of each group you want the user to be a part of. The groups the user belongs to display beneath the **Groups** list.
   b. To remove a user from a group, simply click the group you want to remove beneath the **Groups** list.
5. Click **Save Changes**.

Alfresco Explorer administrative tasks

You perform various administrative functions in the Administration Console located in Alfresco Explorer.

Refer to the Explorer user help for full documentation on these administrative features:

- Managing categories
- Importing the ACP file into a space
- Exporting a space and its contents
- Viewing System Information
- Using the Node Browser

Administering Records Management

The administrator can manage Alfresco Records Management from the Management Console.

Users can only access the Management Console if they are members of the `ALFRESCO_ADMINISTRATORS` group.

Management Console

The Management Console allows you to manage the Records Management site.

You can manage the following Records Management-specific administration tasks:

- Audit
- Custom Metadata

- Define Roles
- Email Mappings
- Events
- List of Values
- Relationships
- User Rights Report

Accessing the Records Management Console

This task assumes that you have access to the Records Management site dashlet and that you are logged in as a user that is a member of the `ALFRESCO_ADMINISTRATORS` group.

In the Records Management dashlet, click **Management Console**

The Management Console displays, with the Audit tool showing, by default.

Records Management Auditing

The function of the Records Management system is to manage and control electronic and physical records according to legislative and regulatory requirements, and it must be capable of demonstrating this compliance.

The Audit tool displays the auditing information collected from the system to show whether business rules are being followed and ensure that unauthorized activity can be identified and traced. The Audit tool is especially important for systems that deal with classified information.

The Audit tool maintains a complete trace of all the actions on every record and it cannot be altered. The information that is captured and stored includes:

- any action on any record, any aggregate, or the File Plan
- user undertaking the action
- date and time of the action

The Audit tool displays by default when you access the Management Console.

Accessing the audit tool

The audit tool displays by default when you access the Management Console.

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, click **Audit**.

   The Audit page displays.
3. Click **Apply**.

The current audit log displays, showing the date timestamp and the list of captured actions of the last 20 entries in the log.

Starting and stopping the audit log

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, select **Audit**.
3. Click **Stop**.

   The auditing tool stops capturing and storing the activity in the Records Management system.
4. Click **Start** to start the audit log again.

Specifying the user

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, select **Audit**.

   The audit log displays the activity for all users.
3. Click **Specify**.
4. Type the full or partial name of the user you want to find.

   You must enter a minimum of three (3) characters. The search is not case sensitive.
5. Click **Add**.

The audit log displays the actions taken by the specified user.

Filing the audit log as a record

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, select **Audit**.

   The audit log displays the activity for all users.
3. Click **File as Record**.

   The Select location of Audit Record window displays.
4. Choose the destination folder for the audit record.
5. Click **OK**.

The audit log appears as an undeclared record in the selected folder in the File Plan.

Exporting the audit log

Export allows you to archive the audit log periodically and enables, for example, external auditors to examine or analyze system activity. When you export the audit log, this does not affect the audit log in the system.

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, select **Audit**.
3. Click **Export**.

   The export log displays relevant node name and link.

Auditing actions

The type of action that is recorded in the audit log includes the following:

- capture of all electronic records: file, declare, undeclared
- re-categorization of an electronic record within the file plan: a move
- any change to any Disposition Schedule (instructions): create, modify, destroy
- any disposition actions carried out by authorized roles: cutoff, retain, transfer, review, close folder, reopen folder
- the placing or removal of a disposal hold (freeze) on an object: freeze, unfreeze
- any change made to any metadata associated with File Plan or electronic records, for example, change to vital record indicator
- amendment and deletion of metadata by a user
- any internal or user event triggered by the system or by the user, for example, SUPERSEDED, GAO Audit, End of Fiscal Year, and so on.
- changes made to the access permissions

- creation, amendment or deletion of a user or group
- changes made to the capabilities (functional access permissions)
- changes made to supplemental markings
- export and import
- deletion / destruction of records
- changes to the auditing levels and settings
- search operations carried out by users
- any access to any record or aggregation should be logged, if the access is for viewing, printing or otherwise presenting it, then the access should be marked as retrieval

Creating custom metadata

The Records Management installation defines a default set of metadata. The metadata is logged against each level in the File Plan and at the record level itself.

Accessing custom metadata

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, click **Custom Metadata**.

   The Custom Metadata page displays.

Creating custom metadata

You can create custom metadata for record series, record categories, record folders, and records.

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, click **Custom Metadata**.

   The Custom Metadata page displays.
3. Select **Record Series**, **Record Category**, **Record Folder**, or **Record** from the left column.
4. Click **New**.

   The New Metadata page displays.
5. Type a name for the metadata in the **Label** field.

   This name is used as the label on the Edit Metadata page.
6. Select the expected data value in the **Type** field.

   The type can be of the following values:

Type	Description
Text	Set the value of this metadata to be a text string. When you select this option, you can set the Use selection list checkbox.
Boolean	Set the value of this metadata to be either True or False.
Date	Set the value of this metadata to be a numeric date sequence.

7. Select the **Use selection list** checkbox to configure this metadata field as a selection menu.
8. Select a list name from the menu.

These list names are configured in the List of Values tool.

9. Select the **Mandatory** checkbox to set this metadata to be a mandatory entry in the Edit Metadata page.
10. Click **Create**.

The new metadata displays in the right column of the Custom Metadata page.

Editing custom metadata

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, click **Custom Metadata**.

   The Custom Metadata page displays.
3. Select **Record Series**, **Record Category**, **Record Folder**, or **Record** from the left column.
4. Click the custom metadata from the right column.
5. Click **Edit**.

   The Edit Metadata page displays.
6. Edit the values in the metadata fields.
7. Click **Save**.

Deleting custom metadata

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, click **Custom Metadata**.

   The Custom Metadata page displays.
3. Select **Record Series**, **Record Category**, **Record Folder**, or **Record** from the left column.
4. Click the custom metadata from the right column.
5. Click **Delete**.

   The system prompts you to confirm whether you want to delete this custom metadata.
6. Click **Delete**.

Defining roles and capabilities

User permissions are set in Records Management using a combination of roles and capabilities.

A role is a named collection of functional user access. A capability refers to the functions that can be assigned to each user.

A role can be assigned to one or more users; however, a user can be assigned one role only at a time.

Roles

The Administrator user has permission to add new roles. The Administrator defines the range of capabilities for each role. Each role can be assigned many capabilities.

Capabilities are not hierarchical, so when the Administrator assigns a capability, it does not grant further capabilities.

Roles for Records Management are:

- Records Management Administrator
- Records Management Power User

- Records Management Records Manager
- Records Management Security Officer
- Records Management User

Capabilities

A capability is an ability that can be granted to a user, which controls the behavior of the system. With respect to the user, this may be to grant a certain operation, or privilege or it may be to alter the behavior of the system for that user.

Capabilities cannot conflict and are not hierarchical. A user can be granted a single capability and that capability will not grant any further capabilities. Any user may have zero or more capabilities within the system. A user that has no capabilities is effectively barred from the records management system.

Viewing the capabilities for a role

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, Click **Define Roles**.

   When you select a role name, the list of capabilities assigned to that role display on the right side.

   The list of available roles displays.
3. Select a role to view.
4. Click **Edit** to view the capabilities of the role.
5. When you have finished viewing the capabilities, click **Cancel**.

Adding new roles

1. In the Records Management dashlet, click **Management Console**.
2. In the Tools list, click **Define Roles**.

   The list of available roles displays.
3. Click **New Role**.
4. Enter a name for the role.
5. Select the capabilities that you wish to apply to the role.
   a. To select individual capabilities, click the check box.
   b. To select a group of capabilities, click **Select All**.

      For example, to select all capabilities for controlling folders, select all the capabilities for the Folder Control section.
6. Click **Create**.

   If **Create** is not active, ensure that you have entered a name for the role in the **Name** field.

The new role displays in the list of available roles.

Mapping emails

The Alfresco Records Management system supports accessing the Alfresco server using IMAP. The protocol allows email applications that support IMAP to connect to and interact with Alfresco repositories directly from the mail application.

The Email mappings tool provides a facility to map the fields of an email header to the properties stored in the repository.

For example, an email `Subject` heading is mapped to the Alfresco property `title`. When you are viewing emails within the Records Management system, the `title` property shows the email's `Subject` heading.

Accessing email mapping

1. In the Records Management dashlet, click **Management Console**.
2. In the tools list, click **Email Mapping**.

   The Email Mappings page displays.

Default email mappings

The Email Mapping page shows a list of the current maps between email headers and Alfresco properties.

For example, the email Subject heading mapping to the property title is shown as: `messageSubject` to `cm:title`

The email header field `messageSubject` is on the left, and is separated by the word "to", which indicates that it is mapped to a property `cm:title`.

The following field mappings are defined:

- private static final String KEY_MESSAGE_FROM = "messageFrom";
- private static final String KEY_MESSAGE_TO = "messageTo";
- private static final String KEY_MESSAGE_CC = "messageCc";
- private static final String KEY_MESSAGE_SUBJECT = "messageSubject";

The following custom mappings are also useful to map:

- `messageCc` to `rma:otherAddress`
- `messageFrom` to `rma:address`
- `Date` to `rma:dateReceived`

Date is case sensitive.

Adding an email map

The pre-defined email mappings cover the most commonly used email headers. You can include additional email header mappings using the Email Mappings tool.

This task assumes that you are in the Email Mappings page of the Records Management Console.

1. Type the email header field in the **Map** box or select an email header from the menu.
2. Select the Alfresco property name from the **to** menu.

   You can select an Alfresco property or a custom property.
3. Click **Add**.

   The new mapping displays in the list of email mappings.
4. Click **Save**.

If you do not wish to save your changes, click **Discard Changes**.

Managing events

In the Records Management system, events can control the life cycle of a record. There are several events that are defined internally to the system.

A system event is generated whenever an action occurs on a record or folder, for example, versioned, cutoff, closed, superseded, and so on. These events can then be used in disposition instructions.

The following events are available in Records Management:

- Event
- Abolished
- All Allowances Granted Are Terminated (DoD 5015.2 event)
- Case Closed (DoD 5015.2 event)
- Case Complete
- No Longer needed
- Obsolete
- Redesignated
- Related Record Transferred
- Separation
- Study Complete
- Superseded
- Training Complete
- WGI action complete

Some events, like Case Closed and Allowances Terminated, are part of the DoD 5015.2 tests, but they are user-defined events, usually defined by the Records Manager.

Accessing events

1. In the Records Management dashlet, click **Management Console**.
2. Click the **Events** tool.

   The Events page displays.

Creating a new event

This task assumes that you are in the Events page of the Records Management Console.

1. Click **New Event**.

   The Create Event page displays.
2. In the **Label** field, enter a name for the event.
3. In the **Type** field, select the type of event from the following:
   - Obsoleted Event
   - Simple Event
   - Superseded Event
4. Click **Save**.

The new event name displays on the Events page.

Editing an event

This task assumes that you are in the Events page of the Records Management Console.

1. Locate the event that you want to edit, and then click **Edit**.

   The Edit Event page displays.

2. Modify the values in the event fields.
3. Click **Save**.

Deleting an event

This task assumes that you are in the Events page of the Records Management Console.

1. Locate the event that you want to delete, and click **Delete**.

   The **Remove event** window displays.
2. Click **Yes**.

   The event is deleted from the Events page.

Creating a list of values

Throughout the Records Management system, there are metadata entry fields. The metadata can be simple text strings, Boolean values, or dates.

Where the value is a text string, you may also enter the value using a list of values menu. For example, on the Edit Metadata page, you enter the value for the Mime type field by selecting a value from the menu.

There are two predefined lists in the Records Management installation that you can modify:

- Supplementary marking list
- Transfer Locations

Initially, these lists are empty. The administrator should populate these lists with appropriate values. You can also add your own lists of values.

Accessing list of values

1. In the Records Management dashlet, click **Management Console**.
2. Click the **List of Values** tool.

   The Lists page displays.

Creating a list of values

This task assumes that you are in the Lists page of the Records Management Console.

1. Click **New List**.

   The Create List window displays.
2. In the **Name** field, enter a name for the list.
3. Click **OK**.

The new list name displays on the Lists page.

Editing a list of values

You can add values to the list and also control the user and group access to the values in this list.

This task assumes that you are in the Lists page of the Records Management Console.

1. Locate the list you want to modify, and then click **Edit**.

   The Edit List page displays, showing the name of the current list.

   For example, if the list name is Priority, the page is called Edit List: Priority.
2. To add values to the list:

   a. In the left column, type your value in the **Value** box.
   b. Click **Add**.

      The value name displays in the list in the left column.
3. To control the user and group access to the individual values in the list:
   a. Click the value you require to set access.

      The value is highlighted in blue to show it is selected.
   b. In the right column, click **Add**.

      The Add Access window displays.
   c. Type a user name or group name to search.

      You must enter at least three characters in your search.
   d. Click **Search**.

      The list of users and groups that match the search characters displays in the window.
   e. Choose a user or group and click **Add**.

      The user or group displays in the right column.
4. When you have finished editing the values and access, click **Done**.

Renaming a list of values

This task assumes that you are in the Lists page of the Records Management Console.

1. Locate the list that you want to rename, and then click **Rename**.

   The Rename List window displays.
2. Enter the list name, and then click **OK**.

The modified name displays in the Lists page.

Deleting a list of values

This task assumes that you are in the Lists page of the Records Management Console.

1. Locate the list that you want to delete, and then click **Delete**.

   The Remove List window displays.
2. Click **OK**.

The list is deleted from the Lists page.

Sizing overview

This section contains practical experience and some basic assumptions about Alfresco sizing. It focuses on Alfresco software only and not on dependencies, such as the database or storage solutions.

Deciding how many servers should be used to run Alfresco is difficult to estimate. Each deployment is different and the ideal configuration can only be based on an understanding of the requirements, use cases, and preferred environment.

The sizing guidelines assume that all servers meet the following hardware configuration:

- Processor: 64-bit Intel Xeon 2.8Ghz or better
- Memory: 8GB RAM
- Disk: 100GB (minimum)

- Operating System: 64-bit Red Hat 5 or later

If the preferred deployment environment is not equivalent to this, care must be taken to adjust the anticipated performance figures to match the actual environment.

Sizing in a production environment

Minimal server configurations are based on whether clustering is required. Clustering is often used to improve performance and to help guarantee high-availability and fault-tolerance. This guide does not cover specific sizing instructions for configuring a high-availability environment.

Non-clustered
In this configuration, there is one server running Alfresco while another runs the database. Alfresco and the database can co-exist on development environments and small deployments.

Clustered
In this configuration, two or more Alfresco servers share a common database and file-system, each on its own dedicated server for a total minimum of four servers, two running Alfresco, one running the database, while the fourth serves as the shared file server.

Sizing methodology

This section describes the basic methodology for sizing.

The most accurate means of estimating size is not concerned with the number of users but rather the overall load on the environment. This methodology focuses on the Transactions Per Second (TPS). Transaction is defined to mean the number of basic repository operations (create, read, update, delete or CRUD) that the server can typically handle under very high load, while still ensuring adequate responsiveness. Calculations are weighted toward Create operations, as those tend to be the most computationally expensive tasks.

Minimally, a single un-optimized server should be able to handle between 3-7 transactions per second during periods of highest usage (usage peaks). Through JVM tuning, and with network and database optimizations, this number can rise to over 15 transactions per second.

Sizing formula

The general goal is to achieve a certain throughput of documents in a certain amount of time during the periods of highest usage, therefore the formula described in this section is a starting point for estimating size.

```
# of Servers = Desired Throughput in TPS (DTW) / Average TPS per Server (ATPS)
An example follows:
Desired Throughput per 5-day Week (DTW):
1,000,000 documents
Desired Throughput in TPS assuming 12 hours of daily operation (DT):
DTW / (5 weekdays * 12 hours * 3600 seconds per hour) = 1,000,000 /
 (5*12*3,600)
Total: 4.6 TPS
Number of Servers assuming 3 TPS per server:
DT / ATPS = 4.6 / 3 = 1.5 Servers round up to 2
```

Formula variations

To map Desired Throughput (DT) to the number of users, the formula in this section estimates the value.

```
DT = (# of Users * Average Transactions per User per Day) / (Average Hours in
 Workday * 3,600 Seconds per Hour)
Example:
```

```
DT = (500 Users * 300 Transactions per Day) / (8 hours * 3,600)
DT = 5.2 TPS
```

Troubleshooting

This section provides help for diagnosing and resolving any Alfresco issues you may encounter.

For additional help, refer to the following:

- Alfresco Support Portal (http://support.alfresco.com)
- **Admin Console** in Alfresco Explorer to view various installation and setup information
- Alfresco Installation forum (http://forums.alfresco.com/)

Debugging an Alfresco installation

When developing add-ins, fixing bugs, or changing Alfresco from the source code, it is helpful to debug an instance of Alfresco running on a standard application server. This section outlines the steps needed to configure Alfresco and Eclipse to provide a real-time view of the server and to troubleshoot issues by stepping through the code line by line.

To debug a running Alfresco server, you must connect to the JVM in which Alfresco is running. The following steps configure the JVM to expose an interface for this connection, and then configure Eclipse to connect to and control that JVM.

Configuring the JVM

This task describes how to configure the JVM to expose an interface for connection to the Alfresco server.

Before you start, you must:

- Have a fully installed, configured, and running instance of Alfresco. These steps assume you are using Tomcat on Windows, but the steps are similar for other application servers on other systems.
- Have an IDE installed. These steps describe how to configure Eclipse, which must be installed first (http://www.eclipse.org/downloads)
- Download and install the Alfresco source code from http://wiki.alfresco.com/wiki/Alfresco_SVN_Development_Environment.
- Ensure the source code is the same version as the installed Alfresco server.

1. Verify the Alfresco server is not running.
2. Edit the JVM options used to start the Alfresco Tomcat instance. If you are using the default `alf_start.bat` to start Alfresco, perform the following:
   a. Edit `alfresco.bat` in a text editor.
   b. Find the line: `set JAVA_OPTS=%JAVA_OPTS% -server –X…`
   c. On the next line, add the following on one line:
      ```
      set JAVA_OPTS=%JAVA_OPTS% -server -Xdebug
      -Xrunjdwp:transport=dt_socket,server=y,suspend=n,
      address=8082
      ```
      where address is a port for your system
3. Save the file and close the editor.

Configuring Eclipse

This task describes how to configure Eclipse to connect to and control the JVM.

1. From the Run menu, choose the **Open Debug** dialog.
2. Right-click **Remote Java Application** and select **New**.
3. In the Name box, type `Debug Local Tomcat Alfresco`.
4. Next to Project, click **Browse**, and select **Web Client**. If this is not available as an option, ensure your source code matches that of your server.
5. In Connection Properties, enter the Port number you added to the `alf_start.bat` file.
6. Check **Allow Termination of remote VM** if you want to be able to stop the Alfresco server from the Eclipse console.
7. Click **Apply** to save the configuration.

You have configured Alfresco and Eclipse. Next, you can start the Alfresco server and start the Debug configuration in Eclipse. Eclipse will connect to the Alfresco JVM. From the Java perspective in Eclipse, you can expand the “core” or “web client” packages, open the class files you are interested in, and set breakpoints for the Alfresco server to stop at. From the Debug perspective, you can then interrogate specific variables from the Alfresco server “live”, and step through the source code line by line.

Debugging an upgrade

The startup log is important to help Alfresco Support diagnose any issues that might arise as a result of the upgrade.

1. Immediately after starting the Alfresco server, make a copy of the `alfresco.log` file.
2. Make a copy of the temporary files that contain the SQL statements executed by the upgrade.

   The locations of the temporary files are written to the `alfresco.log` file.
3. Submit the log file and SQL temporary files to Alfresco Support.

Setting log levels

The `log4j.properties` file lets you configure logging levels to provide debugging information when troubleshooting. To set up logging policies, you must prepend `log4.logger` to the class name you want to log to, and set the logging level. You can set the log level dynamically using the JMX client.

When using log4j, you should:

- Keep local customizations and licenses outside of the web application. For example, in the extension directory:

  ```
  $TOMCAT_HOME/shared/classes/alfresco/extension/...-log4j.properties
  ```
- The Alfresco supplied configuration files should be stored or installed within the web application. For example:

  ```
  WEB-INF/classes/alfresco/extension/...-log4j.properties
  ```

A `dev-log4j.properties` file should never be used in an ongoing during production, nor packaged as a part of any product.

Logging uses Log4J's `HierarchyDynamicMBean`. Note: This is not cluster-aware. If needed, the log level change will need to be applied to each machine. Some consoles (for example, JManage) may provide basic facilities for accessing each machine in an application cluster.

The editable attributes are: dynamic list of loggers with `logLevel` attribute, which can be changed to ERROR, WARN, INFO, DEBUG (editable). The operations with impact are: `addLoggerMBean` - add logger, if it has been loaded.

Testing and debugging links

The `<configRoot>/log4j.properties` file lets you set the level of logging based on the amount of information you need.

- To enable debugging for the background process that continually checks the links in a web project, remove the comment from the following line:

  `#log4j.logger.org.alfresco.linkvalidation.LinkValidationServiceImpl=debug`
- To enable debugging for the action to run when performing a link validation check, add the following line:

  `log4j.logger.org.alfresco.linkvalidation.LinkValidationAction=debug`
- To enable debugging for the link validation report dialog, add the following line:

  `log4j.logger.org.alfresco.web.bean.wcm.LinkValidationDialog=debug`

Error messages

This section lists possible issues you may encounter when installing Alfresco and suggests possible remedies.

ImageMagick

Error message on the console:

```
ERROR [AbstractImageMagickContentTransformer]
JMagickContentTransformer not available:
ERROR [AbstractImageMagickContentTransformer]
ImageMagickContentTransformer not available:
Failed to execute command: imconvert ...
```

These issues will not cause the server to fail. Alfresco is reporting that external document transformation engines are not available for use by the server. You can remove the transformation references if they are not required.

`JAVA_HOME`

Make sure the `JAVA_HOME` variable is set correctly for your Java installation.

FTP Socket

Error message on server startup:

```
ERROR [protocol] FTP Socket error
```

```
java.net.BindException: Address already in use:
JVM_Bind at
```

```
java.net.PlainSocketImpl.socketBind(Native Method)
```

Check to see if you have any services running against port 8080 for the Alfresco server or port 21 for the Alfresco FTP integration.

Troubleshooting an upgrade

This section provides help for diagnosing and resolving any issues that might arise as a result of an upgrade.

1. Open the `alfresco.log` file.
2. Make a copy of the `alfresco.log`.
3. In `alfresco.log`, note the locations of the temporary files containing the SQL statements executed during the upgrade, and make a copy of these temporary files.

4. Submit the log file and temporary files to Alfresco Support.

   By in-place upgrading a copy of the repository, rolling back to the previous version in the event of an upgrade failure is quick and painless. The original installation, configuration, and repository are untouched by this process, so it can simply be restarted. This process also allows for the upgrade to be performed any number of times.

Troubleshooting OpenOffice subsystems

This section provides help for troubleshooting the OpenOffice subsystems.

1. Enable the following log4j properties to debug:

   ```
   log4j.logger.org.alfresco.enterprise.repo.content=DEBUG
   log4j.logger.org.artofsolving.jodconverter=DEBUG
   ```

   The OOoDirect debug entry is: `log4j.logger.org.alfresco.repo.content.transform=DEBUG`.
2. If Tomcat is not shutdown gracefully, the `soffice.bin` process may not be stopped. This can result in errors when starting Tomcat with port 8080 being is use. If this occurs, manually kill the `soffice.bin` process.
3. You may see a failure to connect error message, for example:

   ```
   INFO: ProcessManager implementation is WindowsProcessManager
   org.artofsolving.jodconverter.office.OfficeProcess start
   INFO: starting process with acceptString
    'socket,host=127.0.0.1,port=8101,tcpNoDelay=1'
   and profileDir 'C:\Alfresco\tomcat\temp
   \.jodconverter_socket_host-127.0.0.1_port-8101'
   org.artofsolving.jodconverter.office.OfficeProcess start
   INFO: started process
   ERROR [repo.content.JodConverterSharedInstance] Unable to start
    JodConverter library.
   The following error is shown for informational purposes only.
   org.artofsolving.jodconverter.office.OfficeException: failed to start and
    connect
   ```

   If the OpenOffice process takes more than 30s to fully start up, then Alfresco fails to connect to it. If this occurs, manually kill the `soffice.bin` process before attempting to restart the Jodconverter subsystem.

   The next time that you start OpenOffice, it usually starts fast enough to connect (this is due to operating system caching).
4. If the OpenOffice home location is incorrect, the Jodconverter subsystem will still start, but no OpenOffice process will be running or connected. The error may be reported in the console but not in the `alfresco.log` file.

   The correct value for the `jodconverter.officeHome` property varies with host operating system.

   - For Mac OS X, it should be set to the directory that contains `MacOS/soffice.bin`, which is `/Applications/OpenOffice.org.app/Contents` by default.
   - For other operating systems, it should be set to the directory that contains `program/soffice.bin`. For example, for Debian/Ubuntu, this may be `/usr/lib/openoffice`, for Fedora, `/opt/openoffice.org3`, and for Microsoft Windows, `C:/Alfresco/OpenOffice.org`.
5. When restarting the Jodconverter subsystem using JMX, you need to set the enabled property to true (this will also stop the JOD subsystem if it is running); then use the **start** operation to start the Jodconverter subsystem with the new property settings.

6. The JodConverter can run a pool of multiple reusable instances of the soffice OpenOffice process. To use this capability, set the `jodconverter.portNumbers` property to a comma-separated list of port numbers, all of which must be available for use. For example, `2022, 2023, 2024` for a pool of three `soffice` processes.
7. The JodConverter supports configurable restart behavior for the OpenOffice `soffice` process. To ensure that potential memory leaks within OpenOffice do not accumulate and affect performance, the JodConverter will restart an `soffice` process after a given number of tasks (transformations, metadata extractions) have been performed. The default for `jodConverter.maxTasksPerProcess` is 200.
8. The JodConverter allows long-running or hung tasks to be timed out. The first timeout is controlled by `jodconverter.taskQueueTimeout`, which is 30000 by default (30000 milliseconds = 30 seconds). If a task spends this long in a JodConverter queue awaiting execution, it will be dropped from the queue. The second timeout is controlled by `jodconverter.taskExecutionTimeout`, which is 120000 by default (120000 milliseconds = 2 minutes). If a task has been executing within an `soffice` process for longer than this period, that `soffice` process will be terminated and restarted.
9. Throughput of OOo-related tasks, such as transformations, can be balanced against available hardware resources (memory, CPU) by altering the pool size and the two timeout timers.

Troubleshooting the JMX Dumper

This section provides help for troubleshooting the JMX Dumper.

Invoking the JMX Dumper may result in a stack trace in the log file. When you open `jmx-dumper`, it is trying to find a data source defined in the `web.xml` file. (`<res-ref-name>jdbc/dataSource</res-ref-name>`), but this data source is not declared in the `alfresco.xml` file.

To prevent this logging message for appearing, you can configure the data source in the `$CATALINA_BASE/conf/[enginename]/[hostname]/alfresco.xml` file.

Troubleshooting NFS

This section provides help for diagnosing and resolving any issues that might arise when configuring NFS.

User ID and Group ID

An issue with the NFS server (JLAN-11) transposes the GID and UID of the NFS client user, meaning that Unix accounts that have a user-id that differs from the group-id will not gain authentication. The Alfresco-NFS server will deny them access. The user will only see `ls: /mnt/alfresco: Input/output error`. This issue lasted this long presumably because so many Linux distributions create a new group for each new user, unless told otherwise. Though the bug is declared closed, it has yet to filter down to SVN, and `org.alfresco.filesys.server.auth.AlfrescoRpcAuthenticator.authenticateRpcClient(int, RpcPacket)` still reads the GID before the UID.

NFS server port number is not ephemeral

If the `NFSServerPort` property is not given, it defaults to 2049. This is likely to conflict with a native NFS server, if any. The portmapper daemon, when properly used, removes any dependency upon a well known port number, however neither Alfresco nor any native NFS server seem to use this functionality.

Running native and Alfresco NFS servers on the same host

If you wish to run the native server along side the Alfresco NFS server, you cannot depend upon the portmapper, as there is a 50 percent chance that it will retain the native NFS details. When using `nfs-utils-1.0.10` version on Linux, `mount.nfs` will defer to the portmapper for the port-number, version-number, and protocol of the NFS server in question. Only if all three of these are supplied on the command line will the mount command directly contact the Alfresco NFS server. Failing this, `mount.nfs` will fail as it cannot find the server you have described in the portmapper table. You must therefore configure both `MountServerPort` and `NFSServerPort` to known values above 1024. Afterward the following command line should succeed:

```
mount -oport=yourNfsPort,mountport=yourMountPort,proto=tcp
 yourFfsServerName:/alfresco /mnt/alfresco/
```

The `proto` option may be either `tcp` or `udp`. It is desirable to have functionality to resolve the NFS server required by the volume requested, however, the portmapper only searches for the NFS server on the version and protocol.

Troubleshooting CIFS

This section provides help for diagnosing and resolving any issues that might arise when configuring CIFS.

Password Error

Sometimes, when connecting to an instance of Alfresco Share, the login dialog appears several times until finally taking effect. This problem can be caused by the Share connecting to the Windows file server that is running on native SMB/port 445 rather than trying to connect via NetBIOS.

Native SMB collisions

Native SMB can be disabled by adding the following registry key:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]
 "SMBDeviceEnabled"=dword:00000000
```

Reboot the system after creating this key. Setting the value to one or deleting the registry key will restore native SMB support.

The SMBDeviceEnabled registry key does not seem to be recognized on Vista and Windows 2008. In order to stop native SMB being used when the Alfresco CIFS server is being run under Vista or Windows 2008, the firewall rules can be updated to block inbound connections on port 445.

To set up the Windows firewall on the system running the Alfresco CIFS server:

1. Run the Windows Firewall with Advanced Security application:
   - (Vista) go to **Control Panels > Administrative Tools**
   - (Windows 2008) go to **Start > Administrative Tools**
2. Click on the **Inbound Rules** item in the left hand column.
3. Scroll down to the **File and Printer Sharing** rules and enable the following:
   - File And Printer Sharing (`NB-Datagram-In`), File And Printer Sharing (`NB-Name-In`) and File And Printer Sharing (`NB-Session-In`)
   - The File And Printer Sharing (`SMB-In`) rule should be disabled, this blocks the native SMB/port 445 traffic
   - Other File And Printer Sharing (...) rules are not required and can be left as is

Troubleshooting LDAP duplicate person entries

It is possible that you may find duplicate person entries using LDAP.

Duplicate person entries may occur because:

- A configuration error in the LDAP import: each import creates a new person. The query to find the existing person does not match the person you expect. Therefore, this usually means the `UID` attribute is not correct or consistent over configurations. There is a task to simplify the configuration and make this less likely.
- Before the first LDAP import completes, a person is created automatically as the user logs in. The LDAP import will not see the auto created person - a duplicate will be present after the import completes. One way to avoid this is to disable the auto creation of people.
- There are simultaneous logins for the same person which auto creates the person details

Duplicate person entries can now be handled in a number of ways:

- Find the best match, use it, and then leave all entries as they are
- Find the best match, and then fix the other UIDs to be unique by appending a GUID
- Find the best match and delete all others

The following method describes how to delete duplicates that can no longer be removed using the UI:

1. Create a new Javascript in **Data Dictionary > Javascripts** with the following:
   ```
   people.deletePerson("UserNameToDelete");
   ```
2. Browse to **Company Home > More Actions > View Details**.
3. On the details screen, select **Run Action > Execute Script**, and then select the script that you created.

OpenLDAP tips

This section shows a sample configuration file.

There are a number of things to note:

- The maximum number of results returned has been increased from the default of 500 that even applies to paged results. See the OpenLDAP documentation on limits. If you have more than 500 users or groups this would be an issue.
- Digest authentication has been configured to map from a user ID to the corresponding distinguished name. See the example data.
- Passwords are in clear text (so that any authentication mechanism can be used). It is possible they can be in the correct hashed form for the MD5 digest to work.

```
See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include  /usr/local/etc/openldap/schema/core.schema
include  /usr/local/etc/openldap/schema/cosine.schema
include  /usr/local/etc/openldap/schema/inetorgperson.schema

# Define global ACLs to disable default read access.

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral  ldap://root.openldap.org

pidfile   /usr/local/var/run/slapd.pid
argsfile   /usr/local/var/run/slapd.args
```

```
# Load dynamic backend modules:
# modulepath /usr/local/libexec/openldap
# moduleload back_bdb.la
# moduleload back_ldap.la
# moduleload back_ldbm.la
# moduleload back_passwd.la
# moduleload back_shell.la

# Sample security restrictions
# Require integrity protection (prevent hijacking)
# Require 112-bit (3DES or better) encryption for updates
# Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
# Root DSE: allow anyone to read it
# Subschema (sub)entry DSE: allow anyone to read it
# Other DSEs:
#  Allow self write access
#  Allow authenticated users read access
#  Allow anonymous users to authenticate
# Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
# by self write
# by users read
# by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.  (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!

#######################################################################
# BDB database definitions
#######################################################################

database  bdb
suffix  "dc=company,dc=com"
rootdn  "cn=Manager,dc=company,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# This is secret ....
rootpw          {SSHA}u9AUUYOSVX6idlXcwyYOAG6G84oHFpvG
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory  /usr/local/var/openldap-data
# Indices to maintain
index  objectClass  eq

# Clear text to allow hashing
password-hash  {CLEARTEXT}

# SASL mappings for md5 digest authentication
# Extract the user id and use as the search key

authz-regexp
   uid=([^,]*),cn=digest-md5,cn=auth
   ldap:///dc=company,dc=com??one?(uid=$1)

authz-regexp
   uid=([^,]*),cn=company.com,cn=digest-md5,cn=auth
   ldap:///dc=company,dc=com??one?(uid=$1)
```

```
# Tweaks to increase the result set size and max query time

sizelimit 50000
timelimit 3600
```

The following is a very simple example LDIF file that defines People and Groups Organizational units and some example users and groups.

```
# Initial directory contents
dn: dc=company,dc=com
dc: company
objectClass: top
objectClass: domain

dn: ou=People,dc=company,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Groups,dc=company,dc=com
ou: Groups
objectClass: top
objectClass: organizationalUnit

dn: uid=fullname,ou=People,dc=company,dc=com
objectclass: inetOrgPerson
sn: Name
cn: Full Name
userPassword: inClearText
telephoneNumber: 1234567890
uid: fullname
givenName: Full
mail: full.name@company.com
o: Company Software Inc.

dn: uid=walrus,ou=People,dc=company,dc=com
objectclass: inetOrgPerson
sn: Rus
cn: Wal Rus
userPassword: inClearText
telephoneNumber: 1234567890
uid: walrus
givenName: Wal
mail: wal.rus@company.com
o: Company Software Inc.

dn: cn=Group One,ou=Groups,dc=company,dc=com
objectclass: groupOfNames
cn: Group One
member: uid=fullname,ou=People,dc=company,dc=com

dn: cn=Group Two,ou=Groups,dc=company,dc=com
objectclass: groupOfNames
cn: Group Two
member: cn=Group One,ou=Groups,dc=company,dc=com
member: uid=walrus,ou=People,dc=company,dc=com
```

Active Directory tips

This section describes the tips for using Active Directory with the LDAP synchronization.

- You may need to give special permissions in the Active Directory to the account that you are using to do the LDAP bind (as configured in ldap.synchronization.java.naming.security.principal). To do this, open Active Directory Users and Computers, right click on the domain, and select "Delegate Control..." Click

"Next", then select the user that you are using for the LDAP bind and click "Next". The permission that they will need is on the next screen "Read all inetOrgPerson information."

- The example URL in ldap.authentication.java.naming.provider.url does not use SSL. SSL is recommended for production systems. You'll need to switch the port from 389 (below, non-SSL) to 636 for SSL.
- It is often helpful to screen out non-user accounts and disabled accounts. The default user queries in the ldap-ad subsystem type do this by checking bit fields on the userAccountControl attribute. For example:

```
userAccountControl:1.2.840.113556.1.4.803:=512
```

Troubleshooting SMTP inbound email using StartTLS

For StartTLS support to work for inbound email, you must configure SSL for Java.

To identify whether you are having this problem, enable `DEBUG` logging for the class `org.subethamail` in your `log4j.properties` file.

```
startTLS() failed: no cipher suites in common
```

The following process outlines one methodology for creation of a self-signed certificate. However, this may differ between JVM vendors, so consult your JVM documentation for more information.

1. Create a suitable key and certificate:

```
keytool -genkey -keystore mySrvKeystore -keyalg RSA
```

2. Add the following somewhere in your Tomcat configuration. In RHEL 5, this file would be located at `/etc/tomcat5/tomcat5.conf`. For example:

```
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.keyStore=mySrvKeystore -
Djavax.net.ssl.keyStorePassword=123456"
```

This methodology explains how to create a self-signed certificate only. SSL vendors can provide certificates signed by an authority and may be more suitable for production use.

Handling a higher rate of outbound TCP connections

If you are using the Alfresco Web Services API on a Windows client and frequently see errors such as `java.net.BindException: Address already in use: connect` in the client application, you may need to tune the client operating system parameters so that it can handle a higher rate of outbound TCP connections.

1. Open the Registry.
2. Under the following registry entry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters
```

3. Key in the registry of the Windows client machine.
4. Add the following registry entries:

   TcpTimedWaitDelay
   Add this DWORD with a value of 30.

   MaxUserPort
   Add this DWORD with a value of 32768.

5. Refer to the Windows documentation for further details on these registry entries.

Reference

This section provides additional useful information for Alfresco administrators.

Properties available in a JMX client

This section contains a summary of the properties that can be viewed and changed in a JMX client.

`alfresco.authentication.allowGuestLogin`
Specifies whether to allow guest access to Alfresco.

`alfresco.authentication.authenticateCIFS`
A Boolean that when true enables Alfresco-internal authentication for the CIFS server. When false and no other members of the authentication chain support CIFS authentication, the CIFS server will be disabled.

`ntlm.authentication.mapUnknownUserToGuest`
Specifies whether unknown users are automatically logged on as the Alfresco guest user during Single Sign-On (SSO).

`ntlm.authentication.sso.enabled`
A Boolean that when true enables NTLM based Single Sign On (SSO) functionality in the Web clients. When false and no other members of the authentication chain support SSO, password-based login will be used.

`authentication.chain`
Specifies the authentication chain.

`synchronization.autoCreatePeopleOnLogin`
Specifies whether to create a user with default properties when a user is successfully authenticated, who does not yet exist in Alfresco, and was not returned by a differential sync (if enabled with the property above). The default is true. Setting this to false allows you to restrict Alfresco to a subset of those users who could be authenticated by LDAP; only those created by synchronization are allowed to log in. You can control the set of users in this more restricted set by overriding the user query properties of the LDAP authentication subsystem

`synchronization.import.cron`
Specifies a cron expression defining when the scheduled synchronization job should run, by default at midnight every day.

`synchronization.loggingInterval`
Specifies the number of user or group entries the synchronization subsystem will process before logging progress at INFO level. If you have the following default entry in log4j.properties:

`log4j.logger.org.alfresco.repo.security.sync=info`. The default is 100.

`synchronization.syncOnStartup`
Specifies whether to trigger a differential sync when the subsystem starts up. The default is true. This ensures that when user registries are first configured, the bulk of the synchronization work is done on server startup, rather than on the first login.

`synchronization.syncWhenMissingPeopleLogIn`
Specifies whether to trigger a differential sync when a user is successfully authenticated who does not yet exist in Alfresco. The default is true.

`synchronization.synchronizeChangesOnly`
Specifies if the scheduled synchronization job is run in differential mode. The default is false, which means that the scheduled sync job is run in full mode. Regardless of this setting a differential sync may still be triggered when a user is successfully authenticated who does not yet exist in Alfresco.

`synchronization.workerThreads`
Specifies the number of worker threads. For example, 2.

`cifs.WINS.autoDetectEnabled`
When true causes the cifs.WINS.primary and cifs.WINS.secondary properties to be ignored.

`cifs.WINS.primary`
Specifies a primary WINS server with which to register the server name.

`cifs.WINS.secondary`
Specifies a secondary WINS server with which to register the server name.

`cifs.bindto`
Specifies the network adapter to which to bind. If not specified, the server will bind to all available adapters/addresses.

`cifs.disableNIO`
Disables the new NIO-based CIFS server code and reverts to using the older socket based code.

`cifs.disableNativeCode`
When true, switches off the use of any JNI calls and JNI-based CIFS implementations.

`cifs.domain`
An optional property. When not empty, specifies the domain or workgroup to which the server belongs. This defaults to the domain/workgroup of the server, if not specified.

`cifs.enabled`
Enables or disables the CIFS server.

`cifs.hostannounce`
Enables announcement of the CIFS server to the local domain/workgroup so that it shows up in Network Places/Network Neighborhood.

`cifs.ipv6.enabled`
Enables the use of IP v6 in addition to IP v4 for native SMB. When true, the server will listen for incoming connections on IPv6 and IPv4 sockets.

`cifs.netBIOSSMB.datagramPort`
Controls the NetBIOS datagram port. The default is 138.

`cifs.netBIOSSMB.namePort`
Controls the NetBIOS name server port on which to listen. The default is 137.

`cifs.netBIOSSMB.sessionPort`
Controls the NetBIOS session port on which to listen for incoming session requests. The default is 139.

`cifs.serverName`
Specifies the host name for the Alfresco CIFS server. This can be a maximum of 16 characters and must be unique on the network. The special token {localname} can be used in place of the local server's host name and a unique name can be generated by prepending/appending to it.

`cifs.sessionTimeout`
Specifies the CIFS session timeout value in seconds. The default session timeout is 15 minutes. If no I/O occurs on the session within this time then the session will be closed by the server. Windows clients send keep-alive requests, usually within 15 minutes.

`cifs.tcpipSMB.port`
: Controls the port used to listen for the SMB over TCP/IP protocol (or native SMB), supported by Win2000 and above clients. The default port is 445.

`cifs.urlfile.prefix`
: An absolute URL against which all desktop actions and URL files resolve their folder URL. The special token {localname} can be used in place of the local server's host name.

`filesystem.acl.global.defaultAccessLevel`
: Specifies the default access level. Directly names the access control level (None, Read or Write) that applies to requests that are not in scope of any other access control. Note that it is not valid to use the value None without defining other access controls.

`filesystem.acl.global.domainAccessControls`
: Specifies the set of access controls with domain scope. This is a composite property whose value should be a comma-separated list of domain names. To define the access level for one of the listed domains, use the property filesystem.acl.global.domainAccessControls. value.Domain.accessType.

`filesystem.acl.global.protocolAccessControls`
: Specifies the set of access controls with protocol scope. This is a composite property whose value should be a comma-separated list of access control names.

`filesystem.acl.global.userAccessControls`
: Specifies the set of access controls with user scope. This is a composite property whose value should be a comma-separated list of user names.

`filesystem.domainMappings`
: Specifies the domain mapping rules that are used when the client does not supply its domain in the NTLM request.

`filesystem.name`
: Specifies the name given to the repository file system mount exposed through the CIFS server. For example, Alfresco.

`ftp.enabled`
: Enables or disables the FTP server.

`ftp.ipv6.enabled`
: Enables or disables the IPv6 FTP server.

`ftp.port`
: Specifies the port that the FTP server listens for incoming connections on. Defaults to port 21.

`nfs.enabled`
: Enables or disables the NFS server.

`nfs.user.mappings`
: A composite property that configures the user ID/group ID to the Alfresco user name mappings that are used by the current RPC authentication implementation.

`nfs.user.mappings.default.gid`
: The Group Identifier (GID) for NFS user mappings.

`nfs.user.mappings.default.uid`
: The User Identifier (UID) for NFS user mappings.

`imap.config.home.folderPath`
: Specifies the default locations for the IMAP mount point. For example, `Imap Home`.

`imap.config.home.rootPath`
: Specifies the default location for the IMAP mount point. For example, `/${spaces.company_home.childname}`.

`imap.config.home.store`
: Specifies the default location for the IMAP mount point. For example, `${spaces.store}`.

`imap.config.ignore.extraction`
Defines whether or not attachments are extracted.

`imap.config.server.mountPoints`
Defines whether or not attachments are extracted.

`imap.config.server.mountPoints`
Defines whether or not attachments are extracted.

`imap.config.server.mountPoints`
Defines whether or not attachments are extracted.

`imap.config.server.mountPoints`
Specifies the list of mount points. For example, `AlfrescoIMAP`.

`imap.server.enabled`
Enables or disables the IMAP server. This is set to false, by default.

`imap.server.host`
Specifies the host for the IMAP server.

`imap.server.port`
Specifies the port number for the IMAP server. For example, 143.

`imap.config.server.mountPoints.value.AlfrescoIMAP.modeName`
Specifies the `AlfrescoIMAP` mount point access mode name. For example, `MIXED`.

`imap.config.server.mountPoints.default.rootPath`
Specifies the root path for the mount point.

`imap.config.server.mountPoints.value.AlfrescoIMAP.mountPointName`
Specifies the mount point name.

`imap.config.server.mountPoints.default.store`
Specifies the default store for the mount point.

`server.allowedusers`
A comma-separated list of users who are allowed to log in. Leave empty if all users are allowed to log in.

`server.maxusers`
The maximum number of users who are allowed to log in or -1 if there is no limit.

`server.transaction.allow-writes`
A Boolean property that when true indicates that the repository will allow write operations (provided that the license is valid). When false the repository is in read-only mode.

`img.dyn`
Points to the directory containing the ImageMagick shared library (Unix) or DLL files (Windows). For example, (Windows) `img.dyn=${img.root}`; (Linux) `img.dyn=${img.root}/lib`.

`img.exe`
Points to the ImageMagick executable file name.

`img.root`
Points to the ImageMagick root directory.

`swf.exe`
Points to the SWF Tools executable file name.

`wcm-deployment-receiver.poll.delay`
Specifies how long to wait before polling. For example, 5000.

`wcm-deployment-receiver.rmi.service.port`
Specifies the port number for the RMI service. For example, 44101

JMX bean categories reference

This reference section provides detailed information on the individual bean types exported by Alfresco.

The heading for each bean type provides the JMX object naming scheme, where possible. Each section lists the individual properties for the bean type.

JMX read-only monitoring beans

This section contains the list of read-only monitoring beans.

Alfresco:Name=Authority

Exposes key metrics relating to the authority service:

NumberOfGroups
The number of groups known to the Authority Service.

NumberOfUsers
The number of users known to the Authority Service.

Alfresco:Name=ConnectionPool

Allows monitoring of the Apache Commons DBCP database connection pool and its configuration. It exposes the following properties:

DefaultTransactionIsolation
The JDBC code number for the transaction isolation level, corresponding to those in the `java.sql.Connection` class. The special value of -1 indicates that the database's default transaction isolation level is in use and this is the most common setting. For the Microsoft SQL Server JDBC driver, the special value of 4096 indicates snapshot isolation.

DriverClassName
The fully-qualified name of the JDBC driver class.

InitialSize
The number of connections opened when the pool is initialized.

MaxActive
The maximum number of connections in the pool.

MaxIdle
The maximum number of connections that are not in use kept open.

MaxWait
The maximum number of milliseconds to wait for a connection to be returned before throwing an exception (when connections are unavailable) or -1 to wait indefinitely.

MinEvictableIdleTimeMillis
The minimum number of milliseconds that a connection may sit idle before it is eligible for eviction.

MinIdle
The minimum number of connections in the pool.

NumActive
The number connections in use; a useful monitoring metric.

NumIdle
The number of connections that are not in use; another useful monitoring metric.

Url
The JDBC URL to the database connection.

Username
The name used to authenticate with the database.

RemoveAbandoned
A Boolean that when true indicates that a connection is considered abandoned and eligible for removal if it has been idle longer than the `RemoveAbandonedTimeout`.

RemoveAbandonedTimeout
The time in seconds before an abandoned connection can be removed.

TestOnBorrow
A boolean that when true indicates that connections will be validated before being borrowed from the pool.

TestOnReturn
A boolean that when true indicates that connections will be validated before being returned to the pool.

TestWhileIdle
A boolean that when true indicates that connections will be validated whilst they are idle.

TimeBetweenEvictionRunsMillis
The number of milliseconds to sleep between eviction runs, when greater than zero.

ValidationQuery
The SQL query that will be used to validate connections before returning them.

Alfresco:Name=ContentStore,Type=*,Root=*

Allows monitoring of each of Alfresco content stores. When `Type=FileContentStore`, the Root attribute of the name holds the file system path to the store. The following properties are exposed:

TotalSize
The total size in bytes.

WriteSupported
Stated whether the store currently allow write operations.

Alfresco:Name=ContentTransformer,Type=*

Exposes key information about the transformation utilities relied upon by Alfresco. Currently, there are two instances:

- `Alfresco:Name=ContentTransformer,Type=ImageMagick`
- `Alfresco:Name=ContentTransformer,Type=pdf2swf`

The following properties are exposed:

Available
A boolean that when true indicates that the utility is actually installed correctly and was found when the Alfresco server started up.

VersionString
The version information returned by the utility, if it was found to be available.

Alfresco:Name=DatabaseInformation

Exposes metadata about the database itself.

DatabaseMajorVersion
The database version number.

DatabaseMinorVersion
The database version number.

DatabaseProductName
The database product name.

DatabaseProductVersion
The database product version.

DriverMajorVersion
The driver major version number.

DriverMinorVersion
The driver minor version number.

DriverName
Product name of the JDBC driver.

DriverVersion
The driver version number.

JDBCMajorVersion
The major version number of the JDBC specification supported by the driver.

JDBCMinorVersion
The minor version number of the JDBC specification supported by the driver.

StoresLowerCaseIdentifiers

StoresLowerCaseQuotedIdentifiers

StoresMixedCaseIdentifiers

StoresMixedCaseQuotedIdentifiers

StoresUpperCaseIdentifiers

StoresUpperCaseQuotedIdentifiers

URL
The JDBC URL of the database connection.

UserName
The name used to authenticate with the database.

Alfresco:Name=Hibernate

An instance of the `StatisticsService` class provided by Hibernate, allowing access to an extensive set of Hibernate-related metrics.

Alfresco:Name=LicenseDescriptor

Exposes the parameters of the Alfresco Enterprise license.

Days
The number of days of usage that the license allows from its issue date, if the license is time limited.

HeartBeatDisabled
A boolean that when true indicates that the license permits the usage of the Alfresco server with its heartbeat functionality disabled (involving the automatic submission of basic repository statistics to Alfresco).

Holder
The person or entity to which the license was issued.

Issued
The date and time on which the license was issued.

Issuer
Who issued the license (always Alfresco).

RemainingDays
The number of days of usage that the license allows from today, if the license is time limited.

Subject
The product edition to which the license applies.

ValidUntil
The date on which the license will expire, if the license is time limited.

Alfresco:Name=LuceneIndexes,Index=*

Allows monitoring of each searchable index. The Index attribute of the name holds the relative path to the index under `alf_data/lucene-indexes` and the following properties are exposed:

ActualSize
The size of the index in bytes.

EntryStatus
A composite table containing the current status of each entry in the index (double-click the value in JConsole to expand it and view its rows). Each row in the table has a key of the format `<ENTRY TYPE>-<ENTRY STATE>`, for example, `DELTA-COMMITTED` and a value containing the number of entries with that type and state.

EventCounts
A composite table containing the names and counts of significant events that have occurred on the index since the server was started (double-click the value in JConsole to expand it and view its rows). Examples of event names are `CommittedTransactions`, `MergedDeletions` and `MergedIndexes`.

NumberOfDocuments
The number of documents in the index.

NumberOfFields
The number of fields known to the index.

NumberOfIndexedFields
The number of these fields that are indexed.

UsedSize
The size of the index directory in bytes. A large discrepancy from the value of `ActualSize` may indicate that there are unused data files.

Alfresco:Name=ModuleService

Allows monitoring of installed modules.

AllModules
A composite table containing the details of all modules currently installed. Double-click the value in JConsole to expand it and use the **Composite Navigation** arrows to navigate through each module.

Alfresco:Name=OpenOffice

Exposes information about the OpenOffice server used for document conversions. In addition to the property below, this bean has a property corresponding to each registry key in the `org.openoffice.Setup` sub-tree of the OpenOffice configuration registry, providing useful metadata about the particular flavor of OpenOffice that is installed. For example, `ooName` provides the product name, for example, `"OpenOffice.org"` and `ooSetupVersionAboutBox` provides its version, for example, "3.0.0".

available
A Boolean that when true indicates that a connection was successfully established to the OpenOffice server.

Alfresco:Name=PatchService

Allows monitoring of installed patches.

AppliedPatches
A composite table containing the details of all patches currently installed. Double-click the value in JConsole to expand it and use the "Composite Navigation" arrows to navigate through each patch.

Alfresco:Name=RepositoryDescriptor,Type=*

Exposes metadata about the Alfresco repository. Currently, there are two instances of this bean:

Alfresco:Name=RepositoryDescriptor,Type=Installed
Exposes information about the initial repository installation, before any patches or upgrades were installed. Of most relevance to patch and upgrade scenarios.

Alfresco:Name=RepositoryDescriptor,Type=Server
Exposes information about the current server version, as contained in the Alfresco war file. This instance should be used to determine the current properties of the server.

Both expose the following properties:

Edition
The Alfresco edition, for example, "Enterprise".

Id
The repository unique ID. This property is only available from the Installed descriptor.

Name
The repository name.

Schema
The schema version number.

Version
The full version string, including build number, for example, "3.1.0 (stable r1234)".

VersionBuild
The build number.

VersionLabel
An optional label given to the build, such as "dev" or "stable".

VersionMajor
The first component of the version number.

VersionMinor
The second component of the version number.

VersionNumber
The full version number, composed from major, minor and revision numbers.

VersionRevision
The third component of the version number.

Alfresco:Name=Runtime

Exposes basic properties about the memory available to the JVM. Note that a Sun JVM exposes much more detailed information through its platform MX Beans.

FreeMemory
The amount of free memory in bytes.

MaxMemory
The maximum amount of memory that the JVM will attempt to use in bytes.

TotalMemory
The total amount of memory in use in bytes.

Alfresco:Name=Schedule,Group=*,Type=*,Trigger=*

Allows monitoring of the individual triggers, i.e. scheduled jobs, running in the Quartz scheduler. The attributes of the object name have the following meaning:

Group
The name of the schedule group that owns the trigger. Typically DEFAULT.

Type
The type of trigger, typically MonitoredCronTrigger or MonitoredSimpleTrigger. Triggers of different types have different properties, as you will see below.

Trigger
The name of the trigger itself. Must be unique within the group.

All instances have the following properties:

CalendarName
The name of the scheduling Calendar associated with the trigger, or null if there is not one.

Description
An optional textual description of the trigger.

EndTime
The time after which the trigger will stop repeating, if set.

FinalFireTime
The time at which the last execution of the trigger is scheduled, if applicable.

Group
The name of the schedule group that owns the trigger.

JobGroup
The name of the schedule group that owns the job executed by the trigger.

JobName
The name of the job executed by the trigger.

MayFireAgain
A Boolean that when true indicates that it is possible for the trigger to fire again.

Name
The name of the trigger.

NextFireTime
The next time at which the trigger will fire.

PreviousFireTime
The previous time at which the trigger fired.

Priority
A numeric priority that decides which trigger is executed before another in the event of a 'tie' in their scheduled times.

StartTime
The time at which the trigger should start.

State
The current state of the trigger.

Volatile
A Boolean that when true indicates that the trigger will not be remembered when the JVM is restarted.

When Type=MonitoredCronTrigger, the following additional properties are available:

CronExpression
A unix-like expression, using the same syntax as the cron command, that expresses when the job should be scheduled.

TimeZone
The name of the time zone to be used to interpret times.

When Type=MonitoredSimpleTrigger the following additional properties are available:

RepeatCount
The number of times the job should repeat, after which it will be removed from the schedule. A value of -1 means repeat indefinitely.

RepeatInterval
The time interval in milliseconds between job executions.

TimesTriggered
The number of times the job has been run.

Alfresco:Name=SystemProperties

A dynamic MBean exposing all the system properties of the JVM. The set of standard system properties is documented on the Apache website.

JMX configuration beans

This section contains the list of configuration beans. Alfresco introduces an innovative way to manage the configuration of the individual Spring beans that compose the server. This feature is available for security and authentication configuration, which can be particularly complex to manage given the possibility of multiple-chained authentication services and authentication components, each with their own DAOs and other supporting services.

To help with the management of such configuration, the key properties of key authentication bean classes are annotated with a special `@Managed` annotation, that causes them to be exposed automatically through dynamic MBeans under the `Alfresco:Type=Configuration` naming tree. This means that the key beans that make up your authentication chain will become visible to a JMX client, no matter how they are named and wired together.

The current set of authentication classes that have this facility include:

- Authentication Components, including chained, JAAS, LDAP and NTLM components
- Authentication Services, including chained and unchained
- Authentication DAOs
- `LDAPInitialDirContextFactories`, encapsulating the parameters of the LDAP server
- `LDAPPersonExportSource`, controlling the synchronization of person information with an LDAP server

In JConsole, the view of a server with a particularly complex authentication configuration that shows all the authentication classes are visible under the Alfresco`:Type=Configuration` naming tree and navigable with JConsole. These beans provide a read-only view of the configuration.

JMX editable management beans

This section contains the list of editable management beans.

Alfresco:Name=FileServerConfig

Allows management and monitoring of the various file servers.

Read-only properties:

CIFSServerAddress
Not implemented.

CIFSServerName
The CIFS server name, if available.

Editable Properties:

These are not cluster-aware. If more than one file server is running (for example, load-balanced FTP) then changes will need to be applied to each machine. Some consoles (for example, JManage) may provide basic facilities for accessing each machine in an application cluster.

CIFSServerEnabled
A Boolean that when true indicates that the CIFS server is enabled and functioning.

FTPServerEnabled
A Boolean that when true indicates that the FTP server is enabled and functioning.

NFSServerEnabled
A Boolean that when true indicates that the NFS server is enabled and functioning.

Alfresco:Name=Log4jHierarchy

An instance of the HierarchyDynamicMBean class provided with log4j that allows adjustments to be made to the level of detail included in the Alfresco server's logs. Note that it is possible to run Alfresco using JDK logging instead of log4j, in which case this bean will not be available.

Read-only properties:

The bean has a property for each logger known to log4j, whose name is the logger name, usually corresponding to a Java class or package name, and whose value is the object name of another MBean that allows management of that logger (see `#log4j:logger=*`). Despite how it might seem, these properties are read-only and editing them has no effect.

Editable properties:

There is one special editable property and note again that it is not cluster aware.

threshold
Controls the server-wide logging threshold. Its value must be the name of one of the log4j logging levels. Any messages logged with a priority lower than this threshold will be filtered from the logs. The default value is ALL, which means no messages are filtered, and the highest level of filtering is OFF which turns off logging altogether (not recommended).

Operations with Impact:

addLoggerMBean
This adds an additional logger to the hierarchy, meaning that the bean will be given an additional read-only property for that logger and a new MBean will be registered in the `#log4j:logger=*` tree, allowing management of that logger. Is is not normally necessary to use this operation, because the Alfresco server pre-registers all loggers initialized during startup. However, there may be a chance that the logger you are interested in was not initialized at this point, in which case you will have to use this operation. The operation requires the fully qualified name of the logger as an argument and if successful returns the object name of the newly registered MBean for managing that logger.

For example, if in Java class `org.alfresco.repo.admin.patch.PatchExecuter` the logger is initialized as follows:

```
private static Log logger = LogFactory.getLog(PatchExecuter.class);
```

Then the logger name would be `org.alfresco.repo.admin.patch.PatchExecuter`.

log4j:logger=*

An instance of the LoggerDynamicMBean class provided with log4j that allows adjustments to be made to the level of detail included in the logs from an individual logger. Note that it is possible to run Alfresco using JDK logging instead of log4j, in which case this bean will not be available.

Read-only properties:

name
The logger name

Editable properties:

There is one special editable property and note again that it is not cluster aware.

priority
The name of the minimum log4j logging level of messages from this logger to include in the logs. For example, a value of ERROR would mean that messages logged at lower levels such as WARN and INFO would not be included.

Alfresco:Name=VirtServerRegistry,Type=VirtServerRegistry

This is used directly by the Alfresco Virtualization Server.

Search syntax

The following sections describe the Alfresco search syntax.

Search for a single term

Single terms are tokenized before the search according to the appropriate data dictionary definition(s).

If you do not specify a field, it will search in the content and properties. This is a shortcut for searching all properties of type content.

```
banana
TEXT:banana
```

Both of these queries will find any nodes with the word "banana" in any property of type `d:content`.

If the appropriate data dictionary definition(s) for the field supports both FTS and untokenized search, then FTS search will be used. FTS will include synonyms if the analyzer generates them. Terms cannot contain whitespace.

Search for a phrase

Phrases are enclosed in double quotes. Any embedded quotes may be escaped using `"\"`. If no field is specified then the default TEXT field will be used, as with searches for a single term.

The whole phrase will be tokenized before the search according to the appropriate data dictionary definition(s).

```
"big yellow banana"
```

Search for an exact term

To search for an exact term, prefix the term with "=". This ensures that the term will not be tokenized, therefore you can search for stop words.

If both FTS and ID base search are supported for a specified or implied property, then exact matching will be used where possible.

```
=running
```

Will match "running" but will not be tokenized. If you are using stemming it may not match anything.

For the `cm:name` filed, which is in the index as both tokenized and untokized, it will use the untokenized field. For example, `=part` will only match the exact term "part". If you use `=part*` it will match additional terms, like "partners". If there is no untokenized field in the index, it will fall back to use the tokenized field, and then, with stemming/plurals, it would match.

Search for term expansion

To force tokenization and term expansion, prefix the term with "~".

For a property with both ID and FTS indexes, where the ID index is the default, force the use of the FTS index.

```
~running
```

Search for conjunctions

Single terms, phrases, and so on can be combined using "AND" in upper, lower, or mixed case.

```
big AND yellow AND banana
TEXT:big and TEXT:yellow and TEXT:banana
```

These queries search for nodes that contain the terms "big", "yellow", and "banana" in any content.

Search for disjunctions

Single terms, phrases, and so on can be combined using "OR" in upper, lower, or mixed case.

If not otherwise specified, by default search fragments will be ORed together.

```
big yellow banana
big OR yellow OR banana
TEXT:big TEXT:yellow TEXT:banana
TEXT:big OR TEXT:yellow OR TEXT:banana
```

These queries search for nodes that contain the terms "big", "yellow", or "banana" in any content.

Search for negation

Single terms, phrases, and so on can be combined using "NOT" in upper, lower, or mixed case, or prefixed with "!" or "-".

```
yellow NOT banana
yellow !banana
yellow -banana
NOT yellow banana
-yellow banana
!yellow banana
```

Search for optional, mandatory, and excluded elements of a query

Sometimes AND and OR are not enough. If you want to find documents that must contain the term "car", score those with the term "red" higher, but do not match those just containing "red".

Operator	Description
"|"	The field, phrase, group is optional; a match increases the score.
"+"	The field, phrase, group is mandatory (Note: this differs from Google - see "=")
"-", "!"	The field, phrase, group must not match.

The following example finds documents that contain the term "car", score those with the term "red" higher, but does not match those just containing "red":

```
+car |red
```

At least one element of a query must match (or not match) for there to be any results.

All AND and OR constructs can be expressed with these operators.

Search for fields

Search specific fields rather than the default. Terms, phrases, etc. can all be preceded by a field. If not the default field TEXT is used.

```
field:term
field:"phrase"
=field:exact
~field:expand
```

Fields fall into three types: property fields, special fields, and fields for data types.

Property fields evaluate the search term against a particular property, special fields are described in the following table, and data type fields evaluate the search term against all properties of the given type.

Description	Type	Example
Fully qualified property	Property	{http://www.alfresco.org/model/content/1.0}name:apple
Fully qualified property	Property	@{http://www.alfresco.org/model/content/1.0}name:apple
CMIS style property	Property	cm_name:apple
Prefix style property	Property	cm:name:apple
Prefix style property	Property	@cm:name:apple
TEXT	Special	TEXT:apple
ID	Special	ID:"NodeRef"
ISROOT	Special	ISROOT:T
TX	Special	TX:"TX"
PARENT	Special	PARENT:"NodeRef"
PRIMARYPARENT	Special	PRIMARYPARENT:"NodeRef"
QNAME	Special	QNAME:"app:company_home"
CLASS	Special	CLASS:"qname"
EXACTCLASS	Special	EXACTCLASS:"qname"
TYPE	Special	TYPE:"qname"
EXACTTYPE	Special	EXACTTYPE:"qname"
ASPECT	Special	ASPECT:"qname"
EXACTASPECT	Special	EXACTASPECT:"qname"
ALL	Special	ALL:"text"
ISUNSET	Special	ISUNSET:"property-qname"
ISNULL	Special	ISNULL:"property-qname"

Description	Type	Example
ISNOTNULL	Special	ISNOTNULL:"property-qname"
Fully qualified data type	Data Type	{http://www.alfresco.org/model/dictionary/1.0}content:apple
prefixed data type	Data Type	d:content:apple

Search for wildcards

Wildcards are supported in terms, phrases, and exact phrases using "*" to match zero, one, or more characters and "?" to match a single character. The "*" wildcard character may appear on its own and implies Google-style. The "anywhere after" wildcard pattern can be combined with the "=" prefix for identifier based pattern matching.

The following will all find the term apple.

```
TEXT:app?e
TEXT:app*
TEXT:*pple
appl?
*ple
=*ple
"ap*le"
"***le"
"?????"
```

Search for ranges

Inclusive ranges can be specified in Google-style. There is an extended syntax for more complex ranges. Unbounded ranges can be defined using MIN and MAX for numeric and date types and "\u0000" and "\FFFF" for text (anything that is invalid).

Lucene	Google	Description	Example

`[#1 TO #2]`	`#1..#2`	The range #1 to #2 inclusive
		`#1 <= x <= #2`
			`0..5`
			`[0 TO 5]`

`<#1 TO #2]`		The range #1 to #2 including #2 but not #1. `#1 < x <= #2`	`<0 TO 5]`
`[#1 TO #2>`		The range #1 to #2 including #1 but not #2. `#1 <= x < #2`	`[0 TO 5>`
`<#1 TO #2>`		The range #1 to #2 exclusive. `#1 < x < #2`	`<0 TO 5>`

```
TEXT:apple..banana
my:int:[0 TO 10]
my:float:2.5..3.5
my:float:0..MAX
mt:text:[l TO "\uFFFF"]
```

Search for fuzzy matching

Fuzzy matching is not currently implemented. The default Lucene implementation is Levenshtein Distance, which is expensive to evaluate.

Postfix terms with "~float"

```
apple~0.8
```

Search for proximity

Google-style proximity is supported.

To specify proximity for fields, use grouping.

```
big * apple
TEXT:(big * apple)
big *(3) apple
TEXT:(big *(3) apple)
```

Search for boosts

Query time boosts allow matches on certain parts of the query to influence the score more than others.

All query elements can be boosted: terms, phrases, exact terms, expanded terms, proximity (only in filed groups), ranges, and groups.

```
term^2.4
"phrase"^3
term~0.8^4
=term^3
~term^4
cm:name:(big * yellow)^4
1..2^2
[1 TO 2]^2
yellow AND (car OR bus)^3
```

Search for grouping

Groupings of terms are made using "(" and ")". Groupings of all query elements are supported in general. Groupings are also supported after a field - field group.

The query elements in field groups all apply to the same field and cannot include a field.

```
(big OR large) AND banana
title:((big OR large) AND banana)
```

Search for spans and positions

Spans and positions are not currently implemented. Positions will depend on tokenization.

Anything more detailed than one *(2) two are arbitrarily dependent on the tokenization. An identifier and pattern matching, or dual FTS and ID tokenization, may well be the answer in these cases.

```
term[^] - start
term[$] - end
term[position]
```

These are of possible use but excluded for now. Lucene surround extensions:

```
and(terms etc)
99w(terms etc)
97n(terms etc)
```

Escaping characters

Any character may be escaped using the backslash "\" in terms, IDs (field identifiers), and phrases. Java unicode escape sequences are supported. Whitespace can be escaped in terms and IDs.

For example:

```
cm:my\ content:my\ name
```

Mixed FTS ID behavior

This relates to the priority defined on properties in the data dictionary, which can be both tokenized or untokenized.

Explicit priority is set by prefixing the query with "=" for identifier pattern matches.

The tilde "~" can be used to force tokenization.

Search for order precedence

Operator precedence is SQL-like (not Java-like). When there is more than one logical operator in a statement, and they are not explicitly grouped using parentheses, `NOT` is evaluated first, then `AND`, and finally `OR`.

The following shows the operator precedence from highest to lowest:

```
"
[, ], <, >
()
~ (prefix and postfix), =
^
+, |, -
NOT,
AND
OR
```

`AND` and `OR` can be combined with `+`, `|`, `-` with the following meanings:

AND (no prefix is the same as +)	**Explanation**
`big AND dog`	big and dog must occur
`+big AND +dog`	big and dog must occur
`big AND +dog`	big and dog must occur
`+big AND dog`	big and dog must occur
`big AND |dog`	big must occur and dog should occur
`|big AND dog`	big should occur and dog must occur
`|big AND |dog`	both big and dog should occur, and at least one must match
`big AND -dog`	big must occur and dog must not occur
`-big AND dog`	big must not occur and dog must occur
`-big AND -dog`	both big and dog must not occur
`|big AND -dog`	big should occur and dog must not occur

OR (no prefix is the same as +)	**Explanation**
`dog OR wolf`	dog and wolf should occur, and at least one must match
`+dog OR +wolf`	dog and wolf should occur, and at least one must match
`dog OR +wolf`	dog and wolf should occur, and at least one must match
`+dog OR wolf`	dog and wolf should occur, and at least one must match

OR (no prefix is the same as +)	Explanation
`dog OR |wolf`	dog and wolf should occur, and at least one must match
`|dog OR wolf`	dog and wolf should occur, and at least one must match
`|dog OR |wolf`	dog and wolf should occur, and at least one must match
`dog OR -wolf`	dog should occur and wolf should not occur, one of the clauses must be valid for any result
`-dog OR wolf`	dog should not occur and wolf should occur, one of the clauses must be valid for any result
`-dog OR -wolf`	dog and wolf should not occur, one of the clauses must be valid for any result

Forms reference

This reference contains detailed information for forms controls and the configuration syntax.

Form controls

Controls are represented by a Freemarker template snippet, and each field has a control and an optional set of parameters.

The following controls are available.

association.ftl

The `association` control is used to allow objects in the repository to be picked and ultimately associated with the node being edited. The control uses the JavaScript `Alfresco.ObjectPicker` component to allow the user to browse the repository and pick objects.
The following parameters are available:

- `compactMode`: Determines whether the picker will be shown in compact mode
- `showTargetLink`: Determines whether a link to the document details page will be rendered to content items

category.ftl

The `category` control is used to allow the user to select categories for the node being edited. The control uses the JavaScript `Alfresco.ObjectPicker` component to allow the user to browse the category hierarchy.
The following parameters are available:

- `compactMode`: Determines whether the picker will be shown in compact mode

checkbox.ftl

The `checkbox` control renders a standard HTML check box control.
The following parameters are available:

- `styleClass`: Allows a custom CSS class to be applied to the check box

date.ftl

The `date` control renders a date field allowing free form entry of dates, as well as a calendar widget allowing dates to be selected visually. If appropriate a time field is also rendered.
The following parameters are available:

- `showTime`: Determines whether the time entry field should be displayed

encoding.ftl

The `encoding` control renders a selectable list of encodings.
The following parameters are available:

- `property`: The name of a content property to retrieve the current encoding from; if omitted the `field.value` value is used
- `styleClass`: Allows a custom CSS class to be applied to the select list

invisible.ftl

The `invisible` control renders nothing at all; it can be used when a form definition needs to be requested and returned but not displayed. This control has no parameters.

mimetype.ftl

The `mimetype` control renders a selectable list of mime types.
The following parameters are available:

- `property`: The name of a content property to retrieve the current mime type from, if omitted the field.value value is used
- `styleClass`: Allows a custom CSS class to be applied to the select list

period.ftl

The `period` control renders a selectable list of periods and an expression entry field.
The following parameters are available:

- `dataTypeParameters`: A JSON object representing the period definitions to show in the list

selectone.ftl

The `selectone` control renders a standard HTML select list.
The following parameters are available:

- `options`: A comma separated list of options to display, for example `"First,Second,Third"`. If a value for an option also needs to be specified, use the `"First|1,Second|2,Third|3"` format.
- `size`: The size of the list, that is, how many options are always visible
- `styleClass`: Allows a custom CSS class to be applied to the select list

size.ftl

The `size` control renders a read only human readable representation of the content size.
The following parameters are available:

- `property`: The name of a content property to retrieve the current content size from; if omitted the `field.value` value is used

textarea.ftl

The `textarea` control renders a standard HTML text area field.
The following parameters are available:

- `rows`: The number of rows the text area will have
- `columns`: The number of columns the text area will have
- `styleClass`: Allows a custom CSS class to be applied to the text area

textfield.ftl

The `textfield` control renders a standard HTML text field.
The following parameters are available:

- `styleClass`: Allows a custom CSS class to be applied to the text field
- `maxLength`: Defines the maximum number of characters the user can enter
- `size`: Defines the size of of the text field

Forms configuration syntax

The `share-config-custom.xml` file uses an XML configuration syntax.

The XML syntax is described as follows:

default-controls
The type element defines what control to use, by default, for each type defined in the Alfresco content model. The name attribute contains the prefix form of the data type, for example `d:text`. The template attribute specifies the path to the template snippet to use to represent the field. If the path value should be a relative path, it is relative from the `alfresco` package. If the path value is absolute, it is looked up relative to the `alfresco/web-extension/site-webscripts` package, normally found in the application server shared classes location. The `control-param` element provides a mechanism to pass parameters to control templates, meaning that control templates can be re-used.

constraint-handlers
The constraint element defines what JavaScript function to use to check that fields with constraints are valid before being submitted. The `id` attribute is the unique identifier given to the model constraint in the Alfresco content model, for example `LIST`. The `validation-handler` attribute represents the name of a JavaScript function that gets called when the field value needs to be validated. The `event` attribute defines what event will cause the validation handler to get called. This will be a standard DOM event, that is, `keyup`, `blur`, and so on. The validation handler called usually has a default message to display when validation fails, the `message` and `message-id` attributes provide a way to override this message. However, the validation messages are not shown (the **Submit** button is enabled/disabled).

dependencies
The `dependencies` element defines the list of JavaScript and CSS files required by any custom controls being used in the application. In order for valid XHTML code to be generated, the dependencies need to be known ahead of time so the relevant links can be generated in the HTML head section. The `src` attribute of both the JavaScript and CSS elements contains the path to the resource, the path should be an absolute path from the root of the web application (but not including the web application context).

form
The `form` element represents a form to display. If the form element exists within a config element that provides an evaluator and condition, the form will only be found if the item being requested matches the condition. If the form element exists within a config element without an evaluator and condition, the form is always found. The optional `id` attribute allows an identifier to be associated with the form, thus allowing multiple forms to be defined for the same item. The `submission-url` allows the action attribute of the generated form to be overridden so that the contents of the form can be submitted to any arbitrary URL.

view-form
The `view-form` element allows the default template that auto generates the form UI to be overridden. The `template` attribute specifies the path to the template to be used when the form is in view mode. The value is usually an absolute path, which is relative to the `alfresco/web-extension/site-webscripts` package, normally found in the application server shared classes location. If this element is present, the `field-visibility` element is effectively ignored and therefore does not have to be present.

edit-form
The `edit-form` element allows the default template that auto generates the form UI to be overridden. The `template` attribute specifies the path to the template to be used when the form is in edit mode. The value is usually an absolute path, which is relative to the `alfresco/web-extension/site-webscripts` package, normally found in the application server shared classes location. If this element is present, the `field-visibility` element is effectively ignored and therefore does not have to be present.

create-form

The `create-form` element allows the default template that auto generates the form UI to be overridden. The `template` attribute specifies the path to the template to be used when the form is in create mode. The value is usually an absolute path, which is relative to the `alfresco/web-extension/site-webscripts` package, normally found in the application server shared classes location. If this element is present, the `field-visibility` element is effectively ignored and therefore does not have to be present.

field-visibility

The `field-visibility` element defines which fields are going to appear on the form, unless a custom template is used.

show

The `show` element specifies a field that should appear on the form. The `id` attribute represents the unique identifier for a field, for example, `cm:name`. The optional `for-mode` attribute indicates when the field should appear. Valid values for the attribute are `view`, `edit`, and `create`. If the attribute is not specified, the field will appear in all modes. If present, the field will only appear for the modes listed. For example, to only show a field in view and edit modes, the `for-mode` attribute would contain `view,edit`.
There are fields that may be optional for an item, and by default they may not be returned by the server. The `force` attribute can be used to indicate to the form service that it should do everything it can to find and return a definition for the field. An example might be a property defined on an aspect, if the aspect is not applied to the node, a field definition for the property will not be returned If force is `true`, it would indicate that server needs to try and find the property on an aspect in the content model.

hide

The `hide` element normally comes into play when multiple configuration files are combined as it can be used to hide fields previously configured to be shown. The `id` attribute represents the unique identifier for a field, for example `cm:name` that should not be displayed. The optional `for-mode` attribute indicates in which modes the field should not appear. Valid values for the attribute are view, edit, and `create`. If the attribute is not specified, the field will never appear. If present, the field will be hidden for the modes listed. For example, to hide a field in view and edit modes, the `for-mode` attribute would contain `view,edit`.
The algorithm for determining whether a particular field will be shown or hidden works, as follows:

1. If there is no `field-visibility` configuration (show or hide tags) then all fields are visible in all modes.
2. If there are one or more hide tags then the specified field(s) will be hidden in the specified modes. All other fields remain visible as before.
3. As soon as a single `show` tag appears in the configuration XML, this is taken as a signal that all field visibility is to be manually configured. At that point, all fields default to hidden and only those explicitly configured to be shown (with a `show` tag) will be shown.
4. Show and hide rules will be applied in sequence, with later rules potentially invalidating previous rules.
5. Show or hide rules, which only apply for specified modes, have an implicit element. For example, `<show id="name" for-mode="view"/>` would show the name field in view mode and by implication, hide it in other modes.

appearance

The optional `appearance` element controls the look and feel of the controls that make up the form. Unlike the `field-visibility` element, this element will be processed and the information available to custom templates defined with the `view-form`, `edit-form` and `create-form` elements, it is up to those templates whether they use the available data. The configuration of what fields are present and how they appear has been separated to provide the maximum flexibility, and although it maybe slightly more verbose, the separation allows the appearance to be defined for fields that are not explicitly mentioned within the `field-visibility` element.

set

The optional `set` element provides the basis of creating groups of fields. The `id` attribute gives the set a unique identifier that other set definitions and fields can refer to. The `parent` attribute allows sets to be nested, and the value should reference a valid set definition, previously defined. The `appearance` attribute specifies how the set will be rendered. Currently, the only supported and allowed values are `fieldset` and `panel`. If an `appearance` attribute is not supplied, the set will not be rendered. The `label` and `label-id` attributes provide the title for the set when it is rendered. If neither are supplied, the set identifier is used. A default set with an identidier of `""` (empty string) is always present, and any fields without an explicit set membership automatically belong to the default set. The default set will be displayed with a label of `Default`.

field

The `field` element allows most aspects of a field's appearance to be controlled from the label to the control that should be used. The only mandatory attribute is `id`, which specifies the field to be customized. However, the field identifier does not have to be present within the `field-visibility` element. The `label` and `label-id` attributes define the label to be used for the form. If neither attribute is present, the field label returned from the Form Service is used. The `description` and `description-id` attributes are used to display a tool tip for the field. If neither is present, the description returned from the Form Service is used (this could also be empty). The `read-only` attribute indicates to the form UI generation template that the field should never be shown in an editable form. Finally, the optional `set` attribute contains the identifier of a previously defined set. If the attribute is omitted, the field belongs to the default set.

control

The `control` element allows the control being used for the field to be configured or customized. If present, the `template` attribute specifies the path to the template snippet to use to represent the field overriding the `default-control` template. If the path value is relative, it is relative from the `alfresco` package. If the path value is absolute, it is looked up relative to the `<web-extension>/site-webscripts` package, normally found in the application server shared classes location. The `control-param` sub-elements provide a mechanism to pass parameters to control templates. This template could either be the one defined locally or the template defined in the `default-control` element for the data type of the field.

constraint-handlers

The `constraint` sub-elements define the JavaScript function to use for checking that fields with constraints are valid before being submitted. The main purpose of this element is to allow aspects of the constraint to be overridden for a particular field. Each attribute effectively overrides the equivalent attribute.

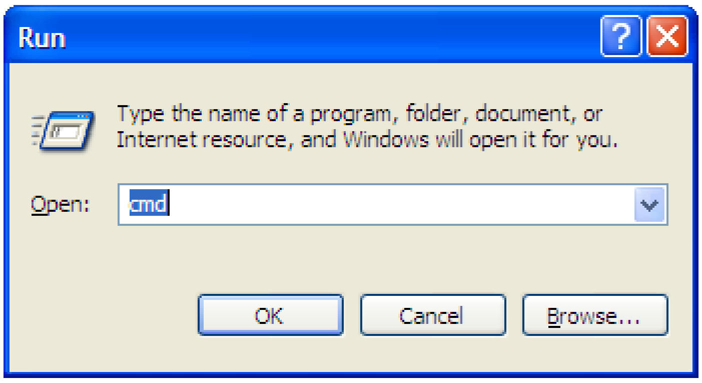
Frequently occurring tasks

This section describes tasks that are frequently used or referred to in this guide.

Opening a Windows command prompt

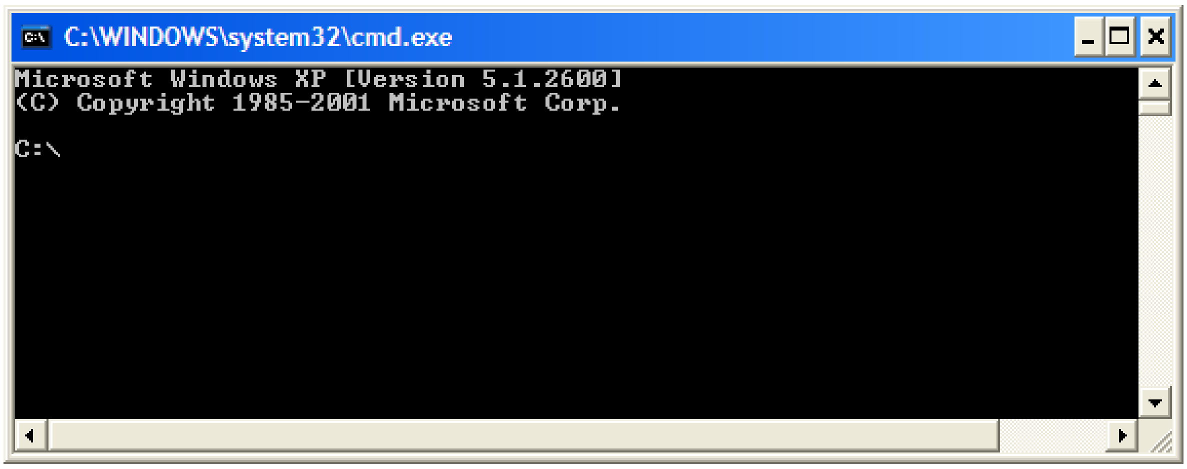
You may need to run and edit scripts in a command prompt when installing on a Windows-based system.

1. On the Windows task bar, click **Start > Run**.
2. In the **Run** dialog box, type `cmd`.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
cmd
OK
Cancel
Browse...

3. Click **OK**.

   The **Run** dialog box closes and a command prompt opens.



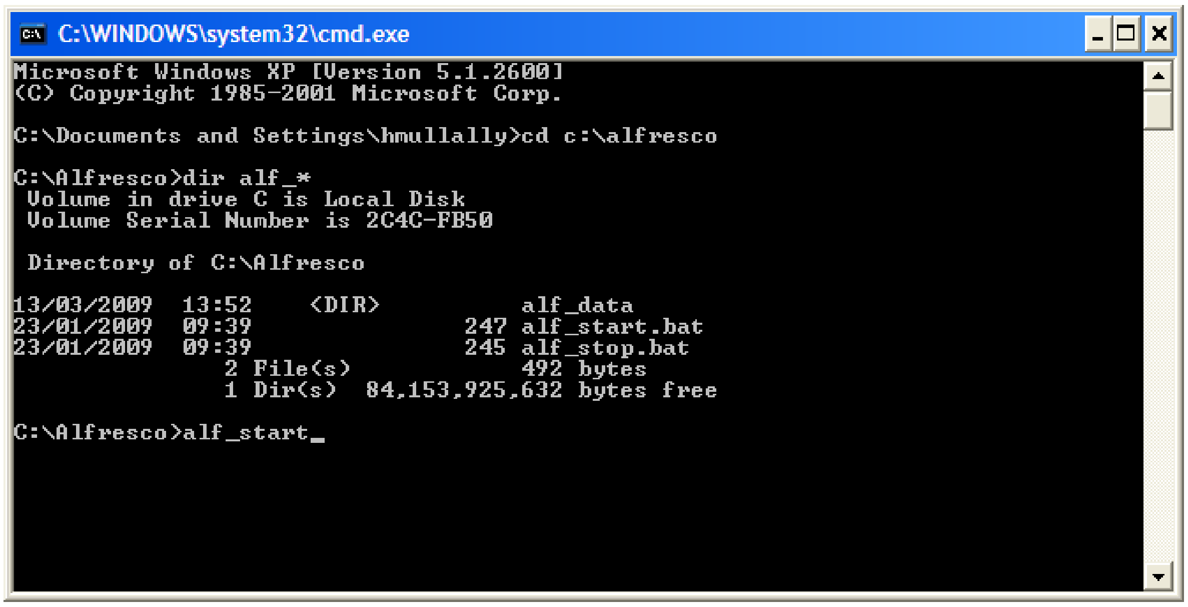
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\
```

Running Windows batch files

When you have installed Alfresco on a Windows-based system, you may prefer to run Alfresco from a batch file. A batch file is a Windows file with a `.bat` extension.

1. In Windows Explorer, browse to `C:\Alfresco`.
2. Double-click a file name with a `.bat` extension.

   For example, to start Alfresco, double-click the file name `alf_start.bat`.
3. Alternatively, in a command prompt, type `cd c:\alfresco`, and press ENTER.
4. To check that you are in the correct directory, type `dir alf_*`, and look for `alf_start.bat`.
5. Type `alf_start`.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\hmullally>cd c:\alfresco

C:\Alfresco>dir alf_*
 Volume in drive C is Local Disk
 Volume Serial Number is 2C4C-FB50

 Directory of C:\Alfresco

13/03/2009  13:52    <DIR>          alf_data
23/01/2009  09:39               247 alf_start.bat
23/01/2009  09:39               245 alf_stop.bat
               2 File(s)            492 bytes
               1 Dir(s)  84,153,925,632 bytes free

C:\Alfresco>alf_start_
```

The command prompt is closed on normal completion, or if the program is terminated by a command error. If the command prompt closes before you have time to see the error that caused the program to terminate, you can run the batch program by opening a command prompt yourself.

Adding folder paths to the Windows path variable

You may need to add folder paths to the Windows `path` variable when installing on a Windows-based system.

1. On the Windows desktop, right-click **My Computer**.
2. In the pop-up menu, click **Properties**.
3. In the **System Properties** window, click the **Advanced** tab, and then click **Environment Variables**.
4. In the **System Variables** window, highlight **Path**, and click **Edit**.
5. In the **Edit System Variables** window, insert the cursor at the end of the **Variable** value field.
6. If the last character is not a semi-colon (;), add one.
7. After the final semi-colon, type the full path to the file you want to find.

   For example: `path C:\jdk`
8. Click **OK** in each open window.

   The new path will be used the next time a command prompt is opened, or a service is started.

Changing the default shell (Unix/Linux/Solaris) for shell scripts

When you run Alfresco on the Unix, Linux, or Solaris operating systems, the default shell is `sh`. You can edit the `alfresco.sh` file to change to your preferred shell.

1. Open the `alfresco.sh` file.

   These steps also apply to any shell script, for example: `apply_amps.sh` or `deploy_start.sh`.
2. Edit the shell command to specify your preferred shell.

For example, change the `#!/bin/sh` line to `#!/bin/bash`.

3. Save the `alfresco.sh` file.

Setting file limits for Linux

When running Alfresco on Red Hat Linux, if you encounter a "Too many open files" error message, you must increase the file limits setting.

These steps assumes that Alfresco is running as the root `alfresco` user.

1. Edit the following file:

   `/etc/security/limits.conf`
2. Add the following settings:

   ```
   alfresco soft nofile 4096
   alfresco hard nofile 65536
   ```

   This sets the normal number of file handles available to the `alfresco` user to be 4096. This is known as the soft limit.
3. As the `alfresco` user, set a system-level setting for Linux, up to the hard limit, using the following command:

   `ulimit -n 8192`

Administrator best practices

This section provides best practice guidelines for Alfresco administrators.

Tips for getting the most out of Alfresco

This section lists the recommended tips for improving your experience of Alfresco.

1. Allow sufficient time to plan your project and identify the most optimal path for you.
2. Benchmark the system you want to use to ensure you can tune it for best performance and high availability before you go live.
3. Ensure customizations occur using the `<extensions>` and `<web-extensions>` directories, and/or `AMP` files to help smooth upgrade and debugging processes.
4. Discover more about FreeMarker templates. You can create custom views for your spaces, and email templates to fit your organization, among other things.
5. Discover more about web scripts. This requires some, but not extensive, technical knowledge, and is very powerful.
6. Use a space template to create reusable components and enable business processes.
7. Leverage the CIFS interface to easily integrate with existing applications using drag and drop.
8. For Microsoft shops, Microsoft Office integration makes adoption of Alfresco seamless.
9. Email integration provides simple and safe way to store emails inside the Alfresco repository.
10. Coordinate with Alfresco on short-term consulting. This allows you and/or your System Integrator to work with Alfresco on architecture and planning.
11. Take advantage of the support for multiple security protocols, which makes it suitable for large enterprises.
12. Use the Alfresco Support Portal, a member-only (Enterprise subscription) benefit that provides a customer portal, downloads, further documentation, and a Knowledge Base.

13. Take advantage of Alfresco training. Get the knowledge and information you need to make your implementation successful.

Common mistakes made by Alfresco administrators

This section lists the most common mistakes to avoid when administering an Alfresco environment.

1. Not copying the Enterprise license. Administrators often forget to do this before the trial period expires, resulting in a system that goes into read-only mode.
2. Not keeping extended configurations and customizations separate in the shared directory. Do not put them in the configuration root. If you do, you will lose them during upgrades.
3. Not ensuring that the database driver is copied to the application server `lib` directory when installing.
4. Not testing the backup strategy.
5. Making changes to the system without testing them thoroughly on a test and pre-production machine first.
6. Failing to set the `dir.root` property to an absolute path location.
7. Not fully shutting down a running instance of Alfresco, so the next time you try and start it, Alfresco says: `Address already in use: JVM_Bind:8080` (especially on Linux).

Eight shortcuts every Alfresco administrator should know

This section lists the recommended shortcuts within Alfresco.

1. Make sure you use a transactional database.
2. Keep your Lucene indexes on your fastest local disk.
3. Version only what and when you need to.
4. If you find yourself constantly creating the same space hierarchy as well as rules and aspects to them, consider creating a Space template instead.
5. Refer to Customizing Alfresco ExplorerThere are several different ways that you can customize the Explorer configuration items. The Explorer configuration file is called `web-client-config-custom.xml`. and Customizing Alfresco Share for some easy customizations.
6. Increase the database connection pool size for large numbers of concurrent users or sessions.
7. Use the System Information to view system properties, such as schema and server versions.
8. Use the Node Browser (searchable by node reference, xpath, or lucene) to view all properties, parent and child nodes, aspects applied, permissions, and associations.

Glossary

ACP
ACP (Alfresco Content Package) files hold exported information produced when using the Export feature.

alf_data
Directory containing binary content and Lucene indexes.

alfresco-global.properties
The `alfresco-global.properties` file contains the customizations for extending Alfresco. The standard global properties file that is supplied with the installers contains settings for the location of the content and index data, the database connection properties, the location of third-party software, and database driver and Hibernate properties.

Alfresco WAR
The Alfresco Web application Archive (WAR) file is for deployment in existing application servers.

AMP
AMP (Alfresco Module Package) is a collection of code, XML, images, CSS, that collectively extend the functionality or data provided by the standard Alfresco repository. An AMP file can contain as little as a set of custom templates or a new category. It can contain a custom model and associated user interface customizations. It could contain a complete new set of functionality, for example records management.

AVM
Alfresco Advanced Versioning Manager (AVM) is an advanced store implementation designed to support the version control requirements of large websites and web applications.

breadcrumb
A navigation link that allows you to jump to any part of the breadcrumb path.

<classpathRoot>
The <classpathRoot> is the directory whose contents are automatically added to the start of your application server's classpath. The location of this directory varies depending on your application server.

<configRoot>
The `<configRoot>` directory is where the default configuration files are stored. Where possible, you should not edit these files but you can edit the overrides in the `<extension>` directory. For example, for Tomcat, `<configRoot>` is: `<TOMCAT_HOME>/webapps/alfresco/WEB-INF/`

<configRootShare>
The `<configRootShare>` directory is where the default configuration files for Share are stored. Where possible, you should not edit these files but you can edit the Share override files in the `<web-extension>` directory. For example, for Tomcat, `<configRootShare>` is `<TOMCAT_HOME>/webapps/share/WEB-INF`

CIFS
Microsoft Common Internet File System (CIFS) is a network file system for sharing files across the Internet.

content
Files or documents made of two main elements: the content itself and information about the content (metadata). For example, documents, video, audio, images, XML, and HTML.

dashboard
The Alfresco dashboard is an interactive user interface that presents and organizes information to the user.

dashlet
A dashlet is an application that appears in the Alfresco dashboard that presents information to the user. Users can organize dashlets into different layouts and set keyboard short cuts for each dashlet.

dir.root
The `dir.root` property is specified in the `alfresco-global.properties` file. It points to the directory `alf_data`, which contains the content and the Lucene indexes.

dir.indexes
This folder contains all Lucene indexes and deltas against those indexes.

Enterprise Content Management (ECM)
Enterprise Content Management (ECM) is a set of technologies used to capture, store, preserve and deliver content and documents and content related to organizational processes. ECM tools and strategies allow the management of an organization's unstructured information, wherever that information exists.

Quoted from: http://en.wikipedia.org/wiki/Enterprise_content_management

Enterprise Edition
The Enterprise Edition is production-ready open source. It is the stress-tested, certified build that is supported by Alfresco Software. It is recommended for corporations, governments, and other organizations looking for a production-ready open source ECM solution, with the primary benefit of being a stable, reliable, certified, supported application with warranty and indemnity, with the support of Alfresco and its certified partners.

<extension>
The `<extension>` directory is where you store files that extend and override the Alfresco default files. When Alfresco is installed, there are sample files in this directory. Many of these files have a `.sample` suffix, which must be removed to activate the file.

For example: for Tomcat, `<extension>` is:`<TOMCAT_HOME>/shared/classes/alfresco/extension/`

Hibernate
Hibernate is an object-relational mapping (ORM) library for the Java language, providing a framework for mapping an object-oriented domain model to a traditional relational database. Hibernate solves Object-Relational impedance mismatch problems by replacing direct persistence-related database accesses with high-level object handling functions.

ImageMagick
ImageMagick is a software suite to create, edit, and compose bitmap images. It can read, convert and write images in a large variety of formats. Images can be cropped, colors can be changed, various effects can be applied, images can be rotated and combined, and text, lines, polygons, ellipses and Bézier curves can be added to images and stretched and rotated.

Quoted from: http://www.imagemagick.org/script/index.php

Java Content Repository (JCR) API
Java Content Repository API is a standard Java API (as defined by JSR-170) for accessing content repositories. Alfresco provides support for JCR level 1 and level 2 giving standardized read and write access.

Java Management Extension (JMX) interface
The JMX interface allows you to access Alfresco through a standard console that supports JMX remoting (JSR-160). Example consoles include, JConsole, MC4J, and JManage.

JVM
Java Virtual Machine

Lucene
Apache Lucene is a high-performance, full-featured text search engine library written entirely in Java. It is a technology suitable for nearly any application that requires full-text search, especially cross-platform.

Quoted from: http://lucene.apache.org/java/docs/index.html

repository
The repository is the combination of the content, the indexes, and the database.

sandbox
An environment for testing, experimenting, or using as a working area. In WCM, a sandbox is an area where users can make changes to web content. In the sandbox, a user can add, edit, and delete both folders and files.

site
A site is a collaborative area for a unit of work or a project.

Spring
Spring is an open-source application framework for Java/JEE. The Alfresco repository uses the Spring Framework as the core foundation of its architecture.

store
A store is a logical partition within the repository, grouped for a particular automated use. Each store contains a hierarchy of nodes with one root node. Two main stores in Alfresco are the Document Management (DM) and the Advanced Versioning Manager (AVM) stores. AVM stores are used for Web Content Management. Each store is identified by a content store reference. This reference consists of a store protocol (such as archive or workspace) and a store id (such as SpaceStore or User).

WAR
The Alfresco Web application ARchive (WAR) file is for deployment in existing application servers.

Web Content Management (WCM)
Web Content Management is an Alfresco product for the rapid deployment of web content, allowing users to create, develop, and maintain content for websites.

WebDAV
Web-based Distributed Authoring and Versioning. A protocol that allows users to edit and manage files on remote web servers.

<web-extension>
The `<web-extension>` directory is where you store files that extend and override the Alfresco default files for Alfresco Share. When Alfresco is installed, there are sample files in this directory. Many of the files have a `.sample` suffix, which must be removed to activate the file.

For example: for Tomcat, `<web-extension>` is:`<TOMCAT_HOME>/shared/classes/alfresco/web-extension/`

workflow
A workflow is a work procedure and workflow steps that represent the activities users must follow in order to achieve the desired outcome. Alfresco provides two different types of workflow: simple and advanced. Simple workflow defines content rules for a space. Advanced workflow provides two out-of-the-box workflows (Review and Approve; Adhoc Task).