AltimateSystems

Your Document Solutions Partner

OpenEDMS Administrator Guide

Version 3.0

Developed by Altimate Systems Inc.

Printed in Toronto, CANADA

Disclaimer

Table of Contents

Table of Figures

1. OPENEDMS SERVER ENVIRONMENT

Database Servers:

- MS SQL Server 2000
- Microsoft SQL Server 2000 Desktop Engine (MSDE 2000)

SMTP Server:

- Required for email forwarding and workflow notification.

Servlet Engine:

- The **OpenEDMS** Document and Workflow Management System implements J2EE Servlet technology. It can be deployed in any servlet engine that supports servlet 1.3 specification.

Sun Java Development Kit:

- Version 1.3 or higher.

A valid OpenEDMS License Key:

- Visit http://www.altimate.ca/contact.html to find a local sales office; requests can be sent by email to info@altimate.ca

Optional Components:

- A valid X509 server certificate for SSL protocol support
- FTP server for directory and batch transfers
- Web server

1.1 STARTING THE OPENEDMS SERVER

If the Tomcat servlet engine was installed with the **OpenEDMS** server, the installation program will have created a corresponding menu item on the Start menu: under **Programs**, select **Altimate OpenEDMS** and click **Start Tomcat**.

If **OpenEDMS** was installed with an alternative servlet engine, it can be started once the current servlet engine has been reset.

To verify **OpenEDMS** server installation, start the web browser client by selecting the **OpenEDMS** menu item from the **Altimate OpenEDMS** program folder, or visit http://localhost:8080/edms to connect directly to the **OpenEDMS** server.

1.2 SYSTEM SECURITY FRAMEWORK

The robust **OpenEDMS** security framework guards against infiltration and protects documents and data from unauthorized exposure. There are three levels of security within the security framework:

- *Transport Layer Security* covers data encryption and the Secure Socket Layer (SSL) protocol for transporting data
- *Server Level Security* addresses firewalls, filtering routers, operating systems, and data integrity
- *Host Level Security* deals with system transmissions and administration

1.2.1 TRANSPORT LAYER SECURITY

Transport Layer Security consists of several components which function together to uphold the confidentiality of information transferred over the Internet. Secure Socket Layer (SSL) is an open security protocol that allows users to establish a secure channel for communicating with the **OpenEDMS** server through any SSL-compliant, 128-bit encrypted browser (such as Netscape Navigator 7.0 or Microsoft Internet Explorer 6.0).

SSL employs highly effective, universally accepted cryptographic techniques to ensure that the information passed between browser and server is authentic, that it cannot be deciphered by a third party, and that it has not been altered or compromised en route. SSL also utilizes a digitally signed certificate, which confirms that the user is communicating with the **OpenEDMS** server and not with a third party attempting to intercept the transmission.

An SSL-enabled browser session will display a lock icon  in the lower right-hand corner of the browser window. Once a secure connection has been established between the browser and the server, the user must provide a registered user ID and valid password before he/she can access **OpenEDMS**. This information is encrypted and stored by the server while a request to log on to the system is processed.

To further ensure the security of user IDs and passwords, all **OpenEDMS** sessions automatically time-out after a fixed period of time has elapsed (dependent on server settings). The **OpenEDMS** Directory Monitor or web browser interface may be used to encrypt highly sensitive documents with an individuated public key stored in the server repository. In order to encrypt a file, a user must have read-permission and be able to retrieve a valid certificate; a user can also use his or her own certificate to encrypt the file for personal use.

1.2.2 SERVER LEVEL SECURITY

All transactions sent to **OpenEDMS** must first pass through a filtering router, which automatically directs the request to the appropriate server after ensuring the method of access is a secure browser. The routers verify the source and destination of each network packet and determine which packets are allowed through the filter. The filtering routers also work to prohibit all other types of Internet access, blocking all non-secure activity, and defending against unauthorized server access.

OpenEDMS uses *Password Based Encryption* (PBE) to encrypt all files stored on the server. The system administrator defines the encryption password in the OpenEDMS System Configuration module. Authorized users can then use this password to encrypt folder and files imported in the repository. OpenEDMS automatically decrypts files for authorized users who have at minimum *Read-level access* to OpenEDMS. You can create encrypted folders, sub-folders, or files. All sub-folders and files created in an encrypted folder are by default encrypted.

1.2.3 HOST LEVEL SECURITY

Once authenticated, a user may process authorized transactions using host data. Communication time-outs ensure that the request must be received, processed, and executed within a fixed time frame; any outside attempt to delay, disrupt, or alter the process will be unsuccessful. Further password encryption techniques are implemented at the host level: user passwords are withheld even from the system administrator.

In addition, **OpenEDMS** exhaustively records and stores all user registrations, log-in/log-out activity, file access, and file operations in the form of system audit reports. These inclusive log files provide a chronological history of system resource usage and comprehensive audit trails of all domain activity.

System audit reports contain such information as the user ID and IP address of the individual responsible for each system action, as well as the name of the file or folder, the nature of the operation, the date, and the time of the action. This allows system and domain administrators to trace every action or operation to its exact origin, ensuring strict compliance with internal and/or external regulatory standards.

2. SYSTEM ADMINISTRATION

This guide is intended for those users designated by their organizations as the **system administrator** for OpenEDMS. In this guide you will learn how to:

- Log in and modify passwords
- Use the OpenEDMS administrative tools
- Set-up file identification
- Configure and use WebDAV with OpenEDMS

2.1 LOGGING IN & MODIFYING PASSWORD SETTINGS

The default system administrator login ID and password are as follows:
User Name: **system**
Password: **openedms**

Note: *all passwords are case-sensitive.*

It is recommended that you change the default password after logging in: click on the displayed user name at the bottom of the active window (e.g. System Admin @ OpenEDMS) to access the administrator profile where you can create a new password.

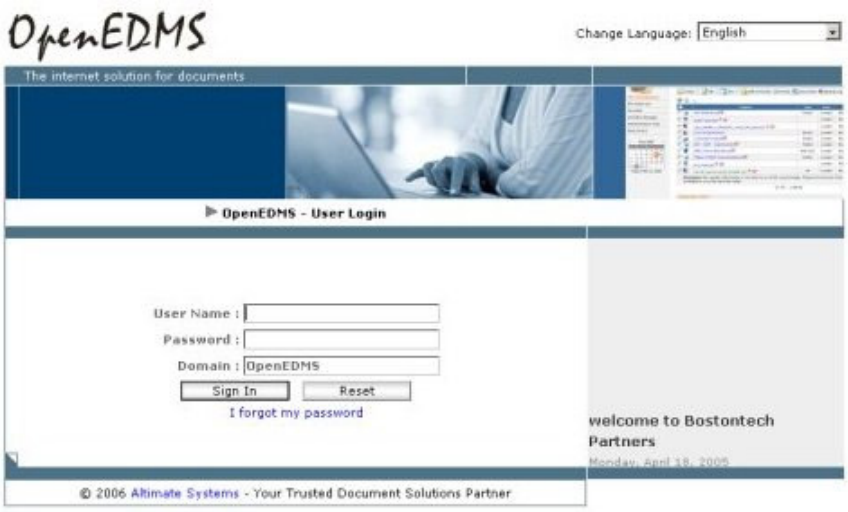

Figure 1: OpenEDMS Login Screen

To select a preferred language, other than the system default (English), click on the **Change Language** drop-down list.

When logging in, you must specify a domain from the **Domain** drop-down list (a newly installed system will only display a single domain). Once logged in, the system administrator can create and configure any number of additional domains, as required by your implementation plan. You can also designate a default domain for the system. For more information refer to the Domain Management section of this guide.

The **File Browser** is displayed by default when you log in to OpenEDMS. In the **System Configuration** component of the **Administrative tools**, you can click on **Default Panel Configuration** to change the panel that is displayed when users log in to OpenEDMS.

3. ADMINISTRATIVE TOOLS

When you first log in to **OpenEDMS**, the **File Management** > **File Browser** dialog is displayed. To access the administrative tools, click on **Administrative Tools** in the left side panel.

Figure 2: OpenEDMS File Browser

The **Administrative Tools** dialog is displayed.

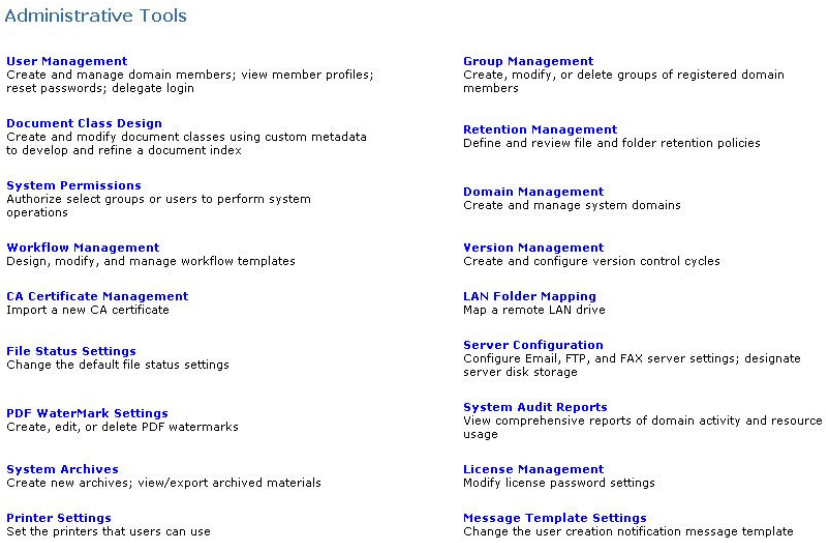

Figure 3: OpenEDMS Administrative Tools

All of the administrative tools are accessible to you directly from within the web browser.

Note: once you have created users in the system, they too will have access to some of the administrative tools if you have identified them as *Admin* users; all other users are restricted from accessing these tools.

3.1 USER MANAGEMENT

When **OpenEDMS** is first installed, it is initially accessible only by a single user: the **System Administrator**. Once logged in, you can create new domain members by selecting **User Management** from the **Administrative Tools**.

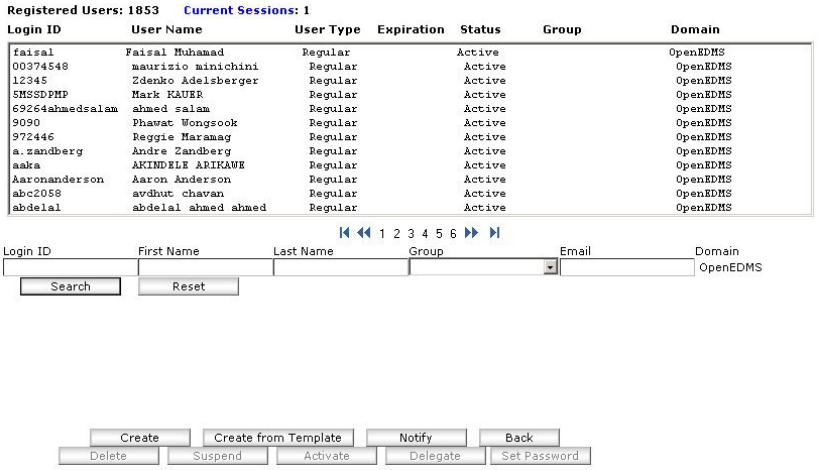

Figure 4: User Management

OpenEDMS supports three categories of user:

1. System administrator
2. Domain administrator
3. Regular user

The System administrator has full control of and access to **OpenEDMS**. Domain administrators have full access to, but limited control of **OpenEDMS**. Regular users are able to log in to **OpenEDMS** but have no other access other than that provided by the domain administrator through ACL permissions. The domain administrator can assign a limited set of admin functions to regular users on an as needed basis. For example, a regular user can be designated to act as the *user group manager*.

From the **User Management** dialog, you can create, suspend, delete, or delegate domain members and modify the password settings of existing members.

Note: users can modify their own passwords by clicking on their login name at the bottom centre of the OpenEDMS window (for example, System Admin @ OpenEDMS).

You can also view detailed member profile information by selecting a registered user ID and clicking **View Profile** (double-clicking on the user ID will also bring up the corresponding user profile).

In order to facilitate domain management and configuration, you can *designate* other registered members as domain administrators by selecting a registered user ID and clicking **Delegate**. Domain administrators have access to nearly the entire range of administrative tools within their assigned domains (excepted are: CA Certificate Management; Domain Management; System Configuration; and License Management).

To designate a domain administrator, double-click on the user ID to access his or her profile and click **Set as Admin** (administrative privileges can subsequently be revoked by clicking **Unset as Admin**).

Additionally, groups or individual users can be appointed as administrators of particular folders. All individuals assigned admin-level folder access can control the folder's security settings by assigning or revoking user permissions. To establish a group or user as a folder administrator, select the **Admin** option from the **Access Control** dialog.

At the top of the User Management window are two information items:

1. **Registered Users**: identifies the total number of users registered in the system.
2. **Concurrent Sessions**: identifies the total number of users currently logged into the system. This number cannot exceed the number of concurrent user licenses you have purchased.

To create a new user:

1. Click **Create** on the **User Management** window. The **Create New User** dialog is displayed.

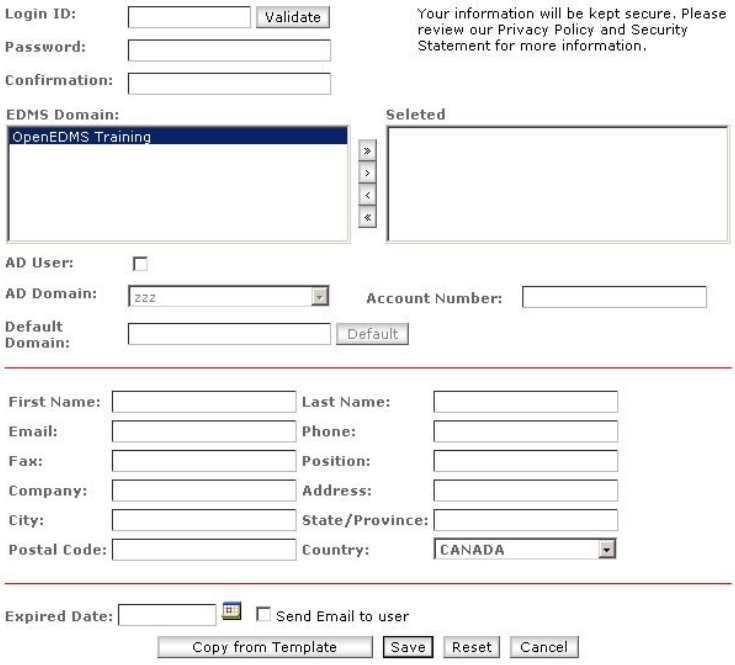

Figure 5: Create New User Profile

2. Enter the login ID. If you are using Active Directory to authenticate user IDs, click the **Validate button** to authenticate the login ID in the Active Directory.
3. Enter the login password. Re-enter the password to confirm.
4. Select the **OpenEDMS Domain(s)** to which the user will have access.
5. Indicate whether or not the user is an Active Directory (**AD**) user.
6. If the user is an **AD** user, select the **AD Domain** in which the user is registered.
7. If you are giving customers limited access to OpenEDMS, you can optionally enter an **Account Number** for them.

8. Identify the **OpenEDMS Default Domain** for the user. The domain you specify here is the domain to which the user will by default log into. If a user has permission to access multiple domains, they can select a different domain from the drop down list when they log in or whenever they are in **OpenEDMS**.
1. Enter the user's **First Name**.
2. Enter the user's **Last Name**.
9. Enter the user's **Email** Address.
10. Enter the user's **Phone** number.
11. Enter the user's **Fax** number
12. Enter the user's job **Position**.
13. Enter the name of the user's **Company**.
14. Enter the **Address** of the company.
15. Enter the **City** in which your company is located.
16. Enter the **State** in which your company is located.
17. Enter the **Postal Code**.
18. Select the **Country** in which the company is located from the dropdown list.
19. Enter the date on which the user login ID and password will expire, if applicable. For example, you can allow a user temporary access to an **OpenEDMS** domain so that they can perform some specific task, when the task is completed in the given timeframe, OpenEDMS can automatically lift access permissions.
20. Check the **Send email to user** to send an email to the user informing them that they are now registered in **OpenEDMS** and what their login ID and password are.
21. Click **Save** to create the new user profile. Click **Reset** to delete all field entries. Click **Back** to return to the **User Management** window. Click **Cancel** to return to the **User Management** window without creating the new user profile.

To change user profile information:

1. Click on the **username@domain name** (for example, *Jill@Demo*) at the bottom of the OpenEDMS window. The **User Profile** dialog is displayed.

   Note: regular users cannot change some of the information in this dialog; only a system or domain administrator can change them.

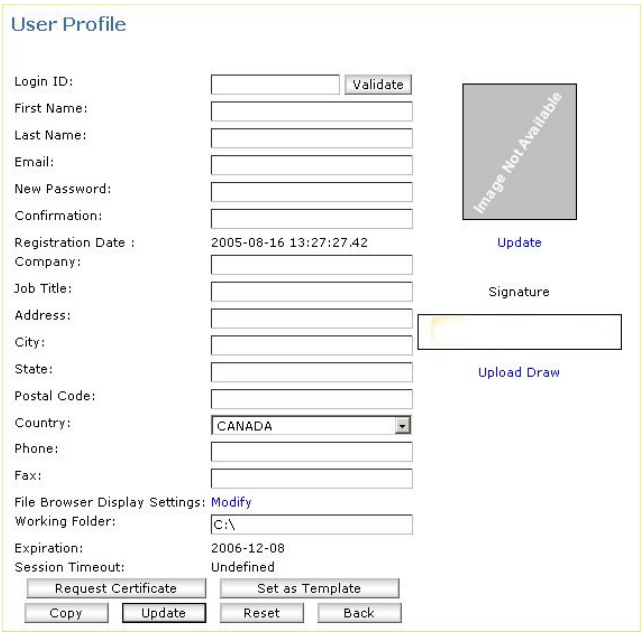

Figure 6: Change User Profile

2. Enter your login ID. If you are using Active Directory to authenticate user IDs, click the **Validate button** to authenticate your login ID in the Active Directory.
3. Enter your **First Name**.
4. Enter your **Last Name**.
5. Enter your **Email** Address.
6. Enter your new **Password**. Enter it again to Confirm.
7. The **Registration Date** identifies the date you were first registered in OpenEDMS. You cannot change this date.
8. Enter the name of your **Company**.
9. Enter your **Job Title**.
10. Enter the **Address** of your company.
11. Enter the **City** in which your company is located.
12. Enter the **State** in which your company is located.
13. Enter the **Postal Code**.
14. Select the **Country** in which your company is located from the dropdown list.
15. Enter the **Phone** number of your company.
16. Enter your company's **Fax** number.
17. Click **Modify** to change your default file browser settings.
18. Enter your **Default-Working Folder**. Whenever you download documents to your local machine they will be downloaded to your working folder.
19. **Expiration** identifies the date your login ID and password expire. You cannot change this date.

20. The **Session Timeout** value identifies the length of time, in minutes, in which the session will timeout. You cannot change this value.
21. Click **Update** to save any changes you made. Click **Back** to return to the window from which you accessed the **View User Profiles** dialog.
22. Click **Request Certificate** to open the CA Certificate dialog in which you can request a CA Certificate for yourself. You only need to do this once. If you attempt to do it a second time, you will receive a message informing you that you already have a valid certificate. You can use the CA Certificate to digitally sign documents in OpenEDMS as part of workflow task processing.
23. Click **Set As Template** to use this user profile as a template from which to create additional user IDs. Whenever you create a user profile from a template, this generic user profile will serve as the template.
24. Click **Copy** to copy your user profile information into a **Create New User Profile** window. This action does not use your user profile as a template.
25. Click **Update** below the photo to add/change the photo that is displayed in OpenEDMS.
26. Click **Upload Draw** to add/change the signature that will be used when you *sign* documents in OpenEDMS.

*Note: only admin users can access the **Set as Template** or **Copy** buttons.*

3.2 GROUP MANAGEMENT

You can create groups comprised of any number of registered domain members assembled under a common name, for example the *project review group*. Whenever a group is selected as the target of any action or operation, all group members will be affected uniformly.

Administrators can add any number of new members to an existing group and individual users can be added to any number of existing groups.

The system automatically creates an **All Users** group for each new domain; all users registered in the domain – as well as all new users subsequently created – are automatically included.

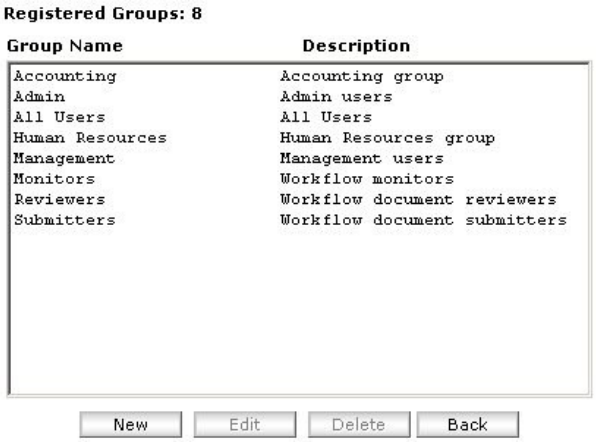

Figure 7: User Group Management

To create a new user group:

1. Click **New** on the **Group Management** window. The **Create New Group** dialog is displayed.

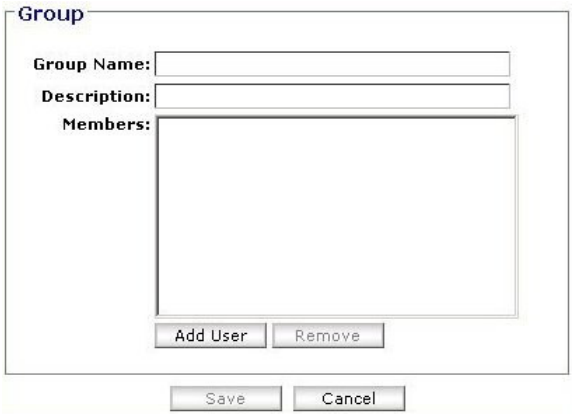

Figure 8: Create New User Group

2. Enter the **Group Name**.
3. Enter a **Description** of the group.
4. Identify the **Members** of the group. Click the **Add User** button to open the **Person Search** dialog in which you can select the members of the group. When you have selected all of the members, click **Close** to return to the **Create New Group** dialog.
5. If you need to remove an individual from the group, select the member from the list and click remove.
6. Click **Save** to create the new group or **Cancel** to return to the **Group Management** window without creating the new group.

To edit an existing group:

1. Select the group and click **Edit**. The **Edit Group** dialog is displayed.
2. Make the necessary changes and click **Save** to save the changes or **Cancel** to return to the **Group Management** window without saving the changes.

To delete an existing group:

3. Select the group and click **Delete**. The selected group is removed from the list of available groups.

3.3 DOCUMENT CLASS DESIGN & METADATA MANAGEMENT

System and domain administrators can develop a domain-based document index comprised of any number of user-defined document classes, each distinguished by an associated series of custom **metadata** attributes.

Existing document classes can be assigned to particular folders so as to define and delimit their intended content: only the folder's assigned document class(es) will be available for use when new files are uploaded to the directory, ensuring that only certain types of documents can be created in certain folders.

A default document class can also be selected so that any file uploaded to the directory will automatically assume the metadata property fields of the selected class.

Document classes allow you to sort/group documents based on similar characteristics. Document classes, in addition, control the folders in which documents can be stored, the retention policy of the document, and access permissions based on the folder in which the document can be stored.

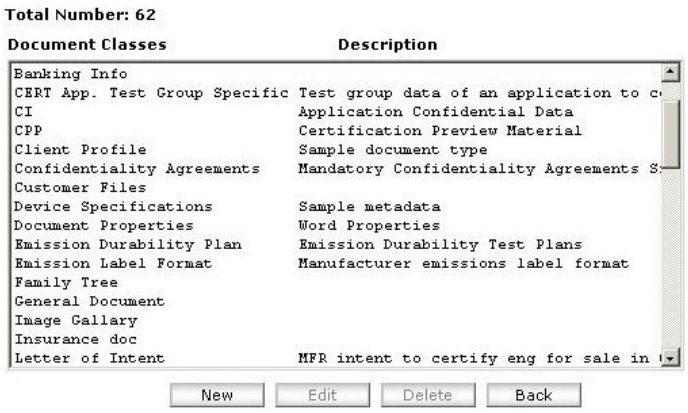

Figure 9: Document Class/Metadata Management

To create a new document class:

1. Click **New** on the **Document Class Management** dialog. The **New Document Class** dialog displays.

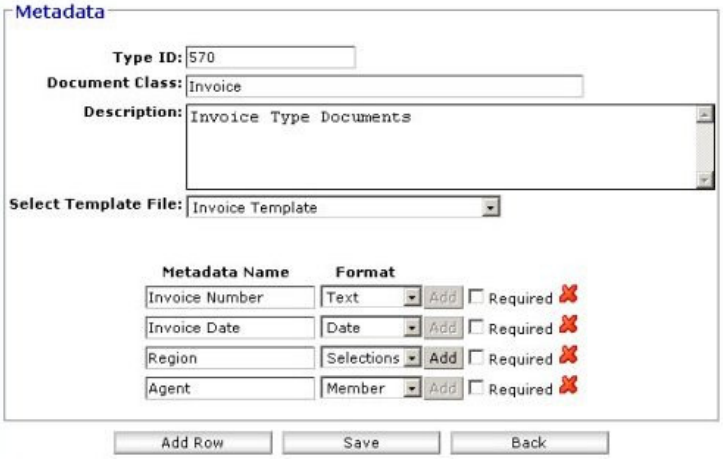

Figure 10: Create New Document Class/Metadata

2. Enter the name of the document class in the **Document Class** field.
3. Enter a brief **Description** of the document class.
4. Define metadata elements for the document class by entering a **Metadata Name**, choosing the **Format** of the metadata, and indicating if the metadata element is **Required** entry. If you select **Required**, users will be prompted to enter a value in this field whenever they assign the document class to a document.

   Metadata are an essential component of document management: they not only provide a stable framework for a document index, but ensure that unstructured content can be streamlined and systematized according to any number of user-defined criteria.

Metadata can be used to classify and distinguish documents on the basis of their business function while serving as useful properties for precision searches: if a particular document class is selected when conducting an **advanced search**, any document belonging to the selected class can be searched by any of that class's assigned metadata property fields.

Metadata attributes can be any one of the following data types:

- Text: free text strings can be used to describe metadata fields, such as title, subject, name, etc.
- Date: the field value must be a valid calendar date.
- Number: the field value must be a digital number.
- Member: the field value must be a registered domain member.
- Selections: the field value must be from the list of customized selections.

*Note: if you choose **Selections** as the **Format Type** an additional button is displayed, **Add**. Click **Add** to display a dialog in which you can enter the values to be included in a drop down list for the metadata element.*

5. To define additional metadata elements, click **Add Row**.
6. To delete a metadata element, click the **Delete Row** icon .
7. Click **Save** to save the new document class or **Back** to return to the **Document Class Management** window without creating the new document class.

To edit a document class:

1. Select a document class from the list and click **Edit**. The **Edit Document Class** dialog is displayed.
2. Make the necessary changes and click **Save** to save changes to the document class or **Back** to exit without saving the changes.

To delete a document class:

1. Select the document class from the list and click **Delete**.

3.4 RETENTION POLICY MANAGEMENT

Retention policies define the length of time that documents stored in a specific folder or belonging to a certain class will be retained in the system before they can be moved to the archive or purged from the system. The **OpenEDMS Retention Management** function enables authorized users to define delete, archive, and review policies for folders and documents based on time and document classifications. The system will notify the specified notification list (user and/or groups) by the given notification protocol (email or instant message). To manage retention policies, select **Retention Policy Management** on the **Administrative Tools** panel. The **Retention Policy Management** dialog is displayed.

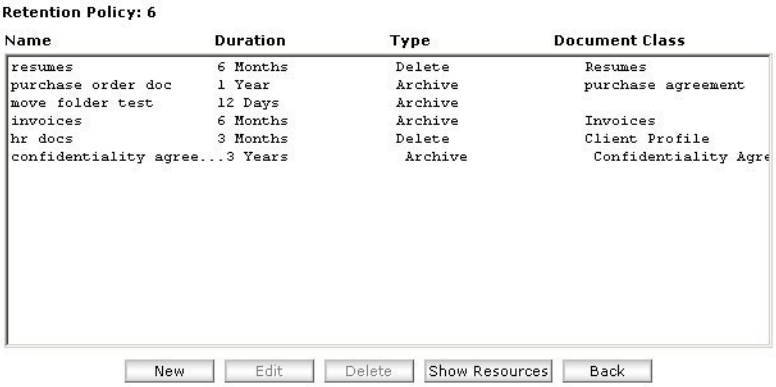

Figure 11: Retention Policy Management

To create a new retention policy:

1. Click **New** on the **Retention Policy Management** dialog. The **Retention Policy** dialog is displayed.

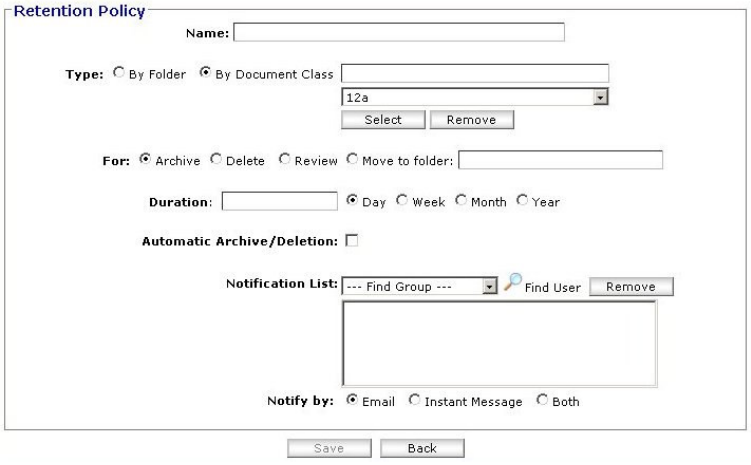

Figure 12: Create New Retention Policy

2. Enter a **Name** for the new retention policy.
3. In the **Type** field, identify whether the retention policy you are creating applies to **Folder(s)** or to a specific **Document Class**. If you select **Folder**, you can apply the retention policy to any folder in the OpenEDMS repository. If you select **Document Class**, the retention policy will apply to all folders / files with the specified document class.

   If you select **Document Class**, select a document class from the dropdown list and click **Select** to define the document class for the retention policy. Click **Remove** to remove the selected document class and choose a new one from the drop down. Once you have chosen a new document class, click **Select**.
4. Select the **Disposal Method** for resources with this retention policy: *Archive*, *Delete*, *Review*, or *Move to Folder*. If you select **Archive**, resources with this retention policy will be moved to the archive when the retention policy expires. If you select **Delete** resources with this retention policy will be deleted when the policy expires. If you select **Review** a message will be sent to the groups/users identified in the **Notification List**, that the retention policy has expired and that they must review the resources to determine their disposition. If you select **Move to**

Folder, resources with this retention policy will be moved to the folder you identify here when the policy expires. Resources are moved at the time specified by the value identified in the System Timer field.

5. Identify the **Duration** of the retention policy in **days**, **weeks**, **months**, or **years**.
6. Identify whether you want **OpenEDMS** is to **automatically** execute the retention policy's disposal method (archive or delete) upon its expiration. If you do not check this box, **OpenEDMS** will notify the individual(s) identified in the **Notification List** below, that the retention policy is about to expire and that he / she / they must archive or delete the resources involved.
7. In the **Notification List**, select a user group, groups, or individual user(s) to whom notification is to be sent when the retention policy is about to expire.
8. Select the method by which those in the **Notification List** are to be notified: *Email*, *Instant Message*, or *Both*.
9. Click **Save** to save the retention policy or click **Back** to return to the **Retention Policy Management** window without saving any changes.

To edit an existing retention policy:

1. Select a retention policy from the list of retention policies and click **Edit**. The **Edit Retention Policy** dialog is displayed.
2. Make the necessary changes and click **Save** to save changes to the retention policy or click **Back** to return to the **Retention Policy Management** dialog without saving any of the changes.

To delete a retention policy:

1. Select a retention policy from the list of retention policies and click **Delete**. The selected retention policy is deleted from the list.

To view resources assigned a selected retention policy:

1. Select a retention policy from the list of retention policies and click **View Resources**. The **Retention Policy Resources** dialog is displayed.

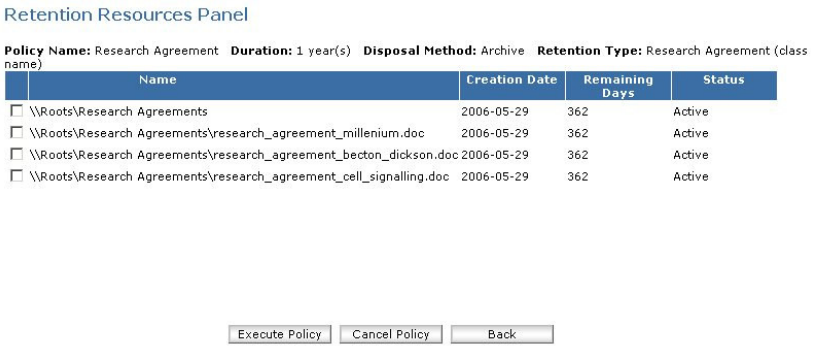

Figure 13: View Retention Policy Resources

This dialog displays status information relating to each of the resources having that retention policy. The information displayed includes:

- **Name** of the resource
- **Creation Date** of the resource

- **Remaining Days** until execution of the retention policy's disposal method
- Current **Status** of the resource.

2. Select a resource from the list and click **Execute Policy** to execute the disposal method of the policy.
3. Select a resource from the list and click **Cancel Policy** to cancel the policy for the resource.
4. Click **Back** to return to the **Retention Policy Management** dialog without making any changes.

3.5 SYSTEM PERMISSIONS

When you first access **OpenEDMS**, only the **System Administrator** has any access to the features and functions in the system. The **System Administrator** can create users in the **User Management** module and assign them permission to access system related functions in the **System Permissions** module. Users only have access to the system permissions assigned to them. Authorized administrators can edit assigned permissions when necessary.

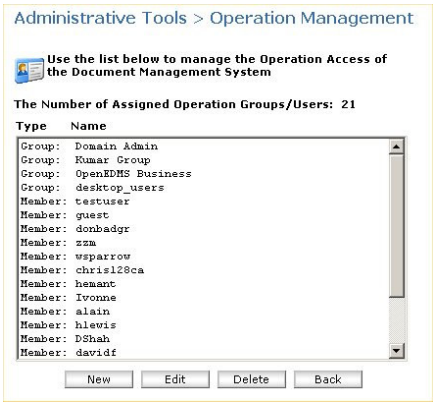

Figure 14: System Permission Management

In order to prevent unauthorized system activity, the range of actions and operations available to general end-users is, by default, strictly limited.

System and domain administrators can assign domain members access permissions on a folder-by-folder basis, but it is also possible for administrators to enable greater end-user autonomy by delegating select groups or users authority to perform any of the following system operations:

- Archive Manager: to consign selected repository resources to the system archives.
- CA Certificate Management: to create, manage, or import CA certificates.
- Create File Templates: to create new template documents or to establish existing documents as template types.
- Delegate Users: to login as another domain member.
- Domain Management: to create, enable, or disable system domains.
- LAN Folder Mapping: to enable remote access to the contents of one or more folders stored on a connected LAN drive.
- Fax Files: to forward repository documents to an external fax machine.
- Group Management: to create groups of registered users, change group names, add or delete group members, or delete groups.
- License Management: to modify license password settings.

- Message Management: to create and publish internal and external messages on the **News Board**.
- Metadata Management: to design new document classes using custom metadata attributes.
- OpenEDMS Desktop Login: to use the **OpenEDMS Desktop** application to upload directories and batch files to the server. Refer to the **OpenEDMS Desktop Guide** for more information.
- Operation Management: to perform any of the system operations enumerated here.
- Retention Policy Management: to define new document or folder lifecycles.
- Send to All: to forward documents to the **All Users** group.
- System Configuration: to configure email, fax, and ftp servers, local disk drive settings, and browser time out values.
- System Report Management: to view audit reports of domain activity and resource usage.
- System Theme Management: to change system display settings (colour scheme, logos, etc.)
- User Management: to create new users, suspend or delete existing users, and to reset user passwords.
- Version Management: to create and configure version cycles for phase-based document development.
- Workflow Management: to create, modify, activate, or suspend workflow process plans.

To assign new system permissions to a user group/user:

1. Click **New** on the **System Permissions Management** dialog. The **Add Operation** dialog is displayed.

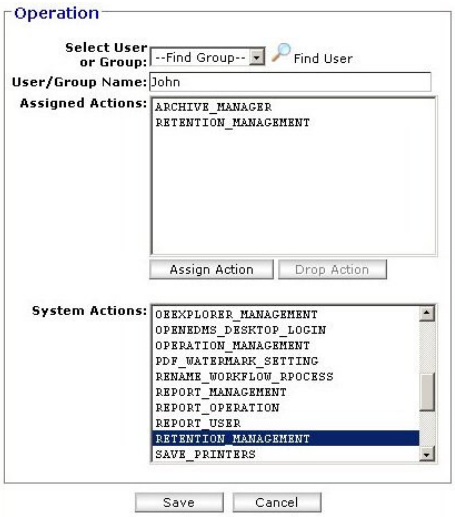

Figure 15: Assign System Permissions

2. Select a group from the **Group** dropdown list or click **Find User** to open the **Person Search** dialog in which you can select the user(s) for whom system permissions are to be defined.
3. In the **Assigned Actions** scroll list select the systems actions for which permission is to be granted and click **Assign Action**.

4. To remove Assigned Actions from the user group/user(s), select the actions from the **Assigned Actions** scroll list and click **Drop Action**.
5. Click **Save** to save the new systems action permissions or **Back** to return to the **System Permissions Management** dialog without saving the changes.

To edit system permissions for a user group/user:

1. Select the user group and/or user from the list and click **Edit**. In this dialog you can **Assign Actions** to the selected group/user or **Drop Actions**.

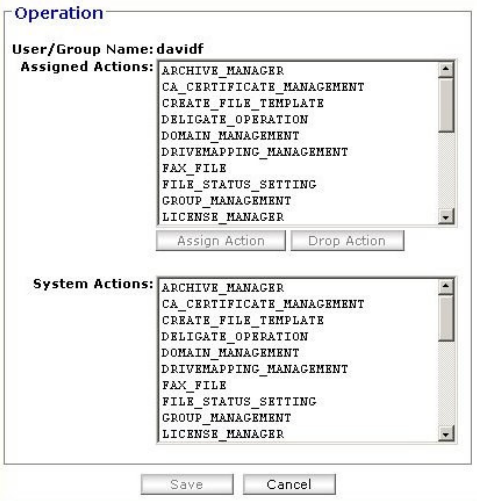

Figure 16: Edit System Permissions

To delete system permissions from a user group/user:

1. Select the user group and/or user from the list and click **Delete**. The specified user group/user is removed from the system permissions list and no longer has any access to system related actions in OpenEDMS.

3.6 DOMAIN MANAGEMENT

Domains are top-level structural units intended to organize groups of related users and relevant documents according to their job or business functions.

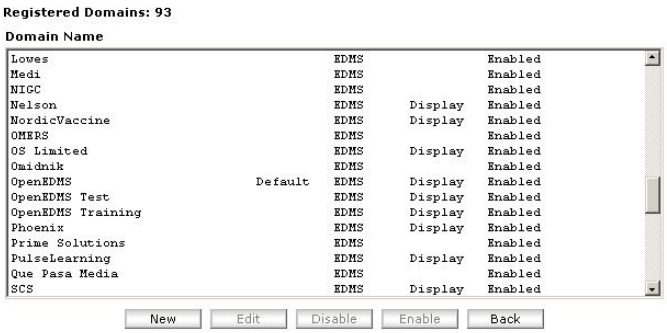

Figure 17: Domain Management

To ensure privacy of information, user IDs and passwords are valid only for those domain(s) in which they are registered: users can only login to their assigned domain(s) and all documents are domain-specific, stored, and manipulated independently of other domains. The same user can be registered in multiple domains under the same login ID.

To create a new domain:

1. Click **New** on the **Domain Management** window. The **Domain** dialog displays in which you can define the new domain.

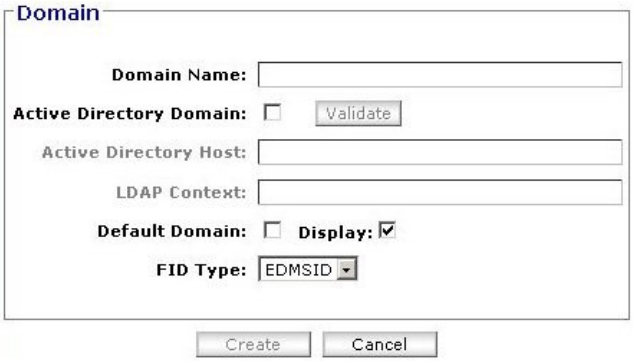

Figure 18: Create New Domain

2. Enter a **Domain Name** for the new domain.
3. Indicate if the new domain is to be integrated with your **Active Directory Domain**. If you check this box, and click **Validate**, all registered users of the new domain will be authenticated against your *Active Directory*.
4. If you are creating a domain that is to be integrated with an **Active Directory** domain, enter the **Active Directory Host** server location.
5. If you are creating a domain that is to be integrated with an **Active Directory** domain, enter the **LDAP Context** string containing server binding information.
6. Indicate if the new domain is to be the **Default Domain** for **OpenEDMS**. If you indicate that the new domain is to be the default, it will be displayed whenever users login to **OpenEDMS**.
7. By default, the new domain is **Display**ed. If you are setting up a multi-domain environment, deselecting this checkbox will hide the domain from the list of accessible domains.
8. In the **FID Type** dropdown select the file ID type to be used to automatically generate ID numbers for your imported resources.

Once enabled, newly created domains will appear listed in the domain drop-down list on the login screen.

3.7 WORKFLOW MANAGEMENT

Please consult the companion **OpenEDMS Desktop Guide** for detailed information on creating, refining, and managing document workflow templates.

3.8 VERSION MANAGEMENT

Administrators and authorized users can create customized version cycles to facilitate stage-based document development and revision.

Version cycles can be assigned to designated project folders so that all folder content will automatically be subject to the selected version cycle settings.

To create a new version cycle:

1. Click on **New** to display the new version cycle dialog.

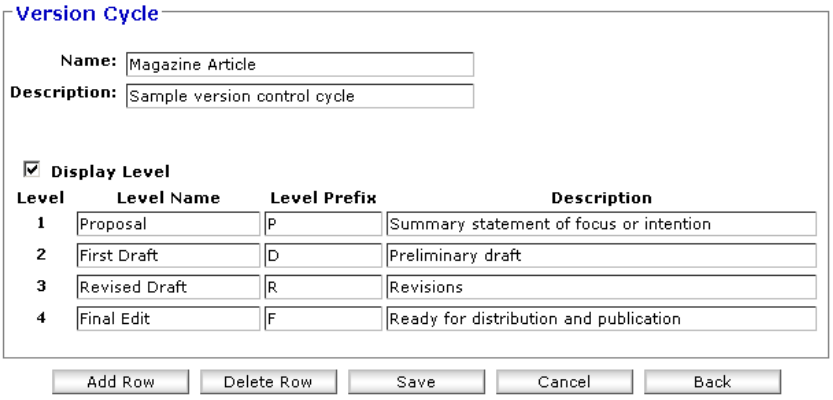

Figure 19: Create New Version Cycle

2. Enter a **Name** for the new version cycle.
3. Enter a brief **Description** of the new version cycle.
4. Enter the **Level Name**, **Level Prefix**, and **Description** for each level of the version cycle.
5. Click **Add Row** to add additional levels to the version cycle.
6. Click **Delete Row** to delete a level.
7. Click **Save** to save the new version cycle and return to the **Version Cycle Management** window.
8. Click **Back** to return to the **Version Cycle Management** window without saving changes to the version cycle.

If the above *Magazine Article* version control cycle were applied to a repository folder, each new file uploaded to that directory path would automatically inherit *P1.0* (Proposal – level 1.0) as its base version number. In the event of subsequent changes, the version number would ascend as follows: *P1.0 – P1.1 – P1.2 – P1.3 …*

As soon as the file passes through the *Proposal* (P) phase and reaches the *First Draft* (D) phase, the version **level** can be promoted so as to reflect the stage and status of the document under development (i.e. *P1.3 – D1.0*).

Version cycles can also be applied to workflow templates so as to automate version promotion. For detailed information, please consult the companion **OpenEDMS Workflow Guide.**

To edit a version cycle:

1. Select a version cycle and click **Edit** to display the version cycle dialog in which you can make the necessary changes.
2. Click **Save** to save changes to the version cycle.

To delete a version cycle:

1. Select a version cycle and click **Delete** to remove the version cycle. Deleted version cycles will no longer be available for assignment to folders/files.

To suspend a version cycle:

1. Select a version cycle and click **Suspend** to suspend the version cycle. Suspended version cycle cannot be assigned to folders/files.

To define a default version cycle:

1. Select a version cycle and click **Set as Default** to set the selected version cycle as the default for all documents imported into OpenEDMS.
2. Click **Clear Default** to clear the default version cycle. You can then select a different version cycle as the default.

3.9 CA CERTIFICATE MANAGEMENT

A valid Certificate Authority (CA) certificate is required for PKI-based document encryption and digital signatures. You can either import a commercial server certificate (e.g. Entrust, VeriSign, etc.), or use the system certificate management tool to create self-signed server certificates.

Figure 20: CA Certificate Management

To create a new certificate:

1. Click **Create New Certificate** on the **CA Certificate Management** window to display the **Create New Certificate** dialog.

Figure 21: Create New CA Certificate

2. Enter the **Certificate Authority (CA)** name. This is a mandatory entry field.
3. Enter the **CA email** address
4. Enter the **Name** of your company. This is a mandatory entry field.

5. Enter the **Company Address**. This is a mandatory entry field.
6. Select the **Country** from the dropdown list. This is the country in which your company is located.
7. Enter the **Certificate Alias**. This is a mandatory entry field.
8. Enter the **Key Password**. This is a mandatory entry field.
9. Re-enter the **Key Password to Confirm**. This is a mandatory entry field.
10. Check **Certificate Password is the same as the Key Password** if the passwords are the same.
11. Enter the **Certificate Password**.
12. Click **Create** to create the new certificate or **Back** to return to the **CA Certificate Management** window without creating the new certificate.

To import a certificate:

1. Click **Import Certificate** on the **CA Certificate Management** window to display the **Import New Certificate** dialog.

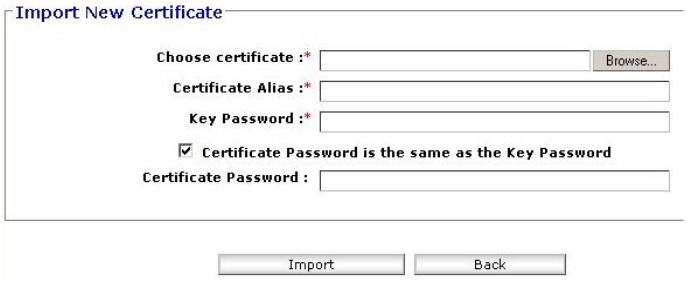

Figure 22: Import New CA Certificate

2. Enter the name of the **Certificate** (directory path) or click **Browse** to open browser in which you can select the certificate to import.
3. Enter the **Certificate Alias**. This is a mandatory entry field.
4. Enter the **Key Password** for the certificate. This is a mandatory entry field.
5. Check **Certificate Password is the same as the Key Password** if the passwords are the same.
6. Enter the **Certificate Password**.
7. Click **Import** to import the new certificate or **Back** to return to the **CA Certificate Management** window without importing the new certificate.

3.10 LAN FOLDER MAPPING

You can use **LAN Folder Mapping** to allow remote access to a target folder stored on any connected **LAN** drive in the OpenEDMS server environment. With the **LAN** folder mapping utility, system administrators can make the content of a remote folder available to authorized users directly from within the repository without having to import it.

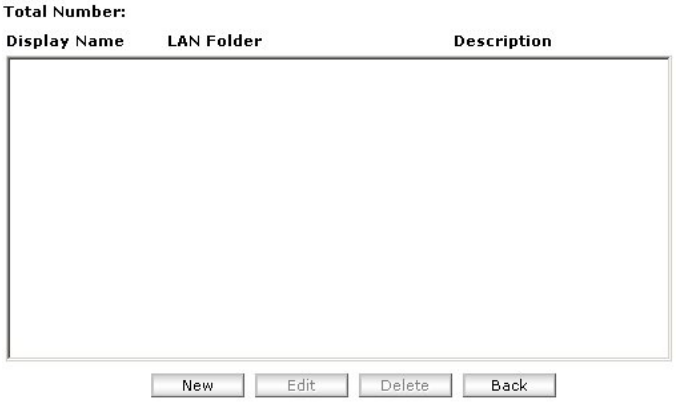

Figure 23: LAN Folder Mapping Management

To map a new LAN folder:

1. Click **New** on the **LAN Folder Mapping Management** window to display the **LAN Folder Mapping** dialog.

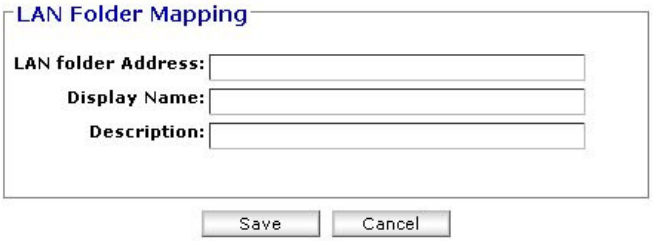

Figure 24: LAN Folder Mapping

2. Enter the **LAN Folder Address**.
3. Enter the **Display Name** of the LAN folder.
4. Enter a **Description** of the LAN folder.
5. Click **Save** to save the new LAN folder mapping or click **Cancel** to return to the **LAN Folder Mapping Management** window without creating the new LAN folder mapping.

To edit LAN folder mapping:

1. Select a LAN folder mapping from the list and click **Edit** to display the **LAN Folder Mapping** dialog in which you can make the necessary changes.

To delete LAN folder mapping:

2. Select a LAN folder mapping from the list and click **Delete** to remove the selected LAN folder mapping from the list.

Note: the mapped LAN folder will be available over the Internet as a public URL, folders that contain sensitive documents or confidential information should not be mapped.

3.11 FILE STATUS SETTINGS

You can use the **File Settings Status** tool to define the various status levels that users can apply to documents as they move through a workflow process. The statuses you define here are available to authorized users in the **Workflow Manager**. For detailed information on using file status settings, refer to the companion **OpenEDMS Workflow Guide**.

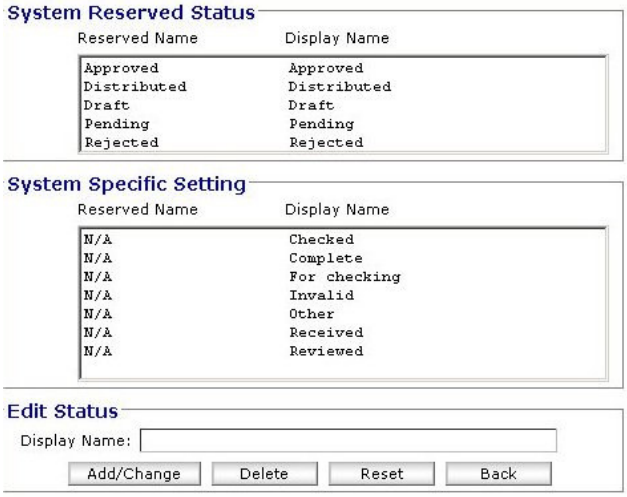

Figure 25: File Status Settings

To add a file status setting:

1. Enter a file status in the **Display Name** field and click **Add**/**Change**. Prior to clicking **Add**/**Change**, you can click **Reset** to delete what you have entered in the **Display Name** field.
2. Click **Back** to return to the **Administrative Tools** panel.

To change a file status setting:

1. Select a file status, enter a new **Display Name**, and click **Add**/**Change**. Prior to clicking **Add**/**Change**, you can click **Reset** to delete what you have entered in the **Display Name** field.
2. Click **Back** to return to the **Administrative Tools** panel.

To delete a file status setting:

1. Select a file status and click **Delete**.
2. Click **Back** to return to the **Administrative Tools** panel.

3.12 SYSTEM CONFIGURATION

You can use the Server Configuration tool to:

- Configure the outbound Email server
- Configure the FTP server
- Configure the FAX service
- Configure Disk Drives
- Configure the Default Panel Configuration
- Set the default Browser Time Out Value
- Set the Encryption password

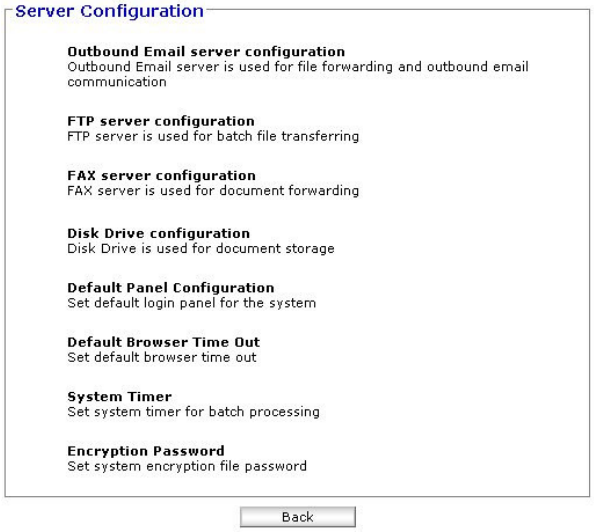

Figure 26: Server Configuration Management

3.12.1 CONFIGURE THE OUTBOUND EMAIL SERVER

To define the outbound email server, click **Outbound Email Server Configuration**. The outbound Email server is used to deliver workflow notification as well as to forward documents to registered members or external parties.

Figure 27: Outbound Email Server Configuration

To configure the outbound email server:

1. Enter the **Outbound Email Server (SMTP)** address.
2. Enter the **Reply-to Email Account**.

3. Enter an **Email Forward Subject**.
4. From the dropdown list select the **Multi Part Email** type: *text* or *html*.
5. Enter the **Email Forward URL**.
6. Enter the **Email Footer Message**.
7. Indicate whether or not authentication is required.
8. If you indicated that authentication is required, enter the outbound email server **Authentication User Name**.
9. If you indicated that authentication is required, enter the outbound email server **Authentication Password**.
10. Click **Save** to save the outbound email configuration or back to exit without saving.

3.12.2 CONFIGURE THE FTP SERVER

To define the FTP server, click **FTP Server Configuration**. The FTP server can be used to transfer batch files from the **OpenEDMS Desktop** utility to the **OpenEDMS** server.

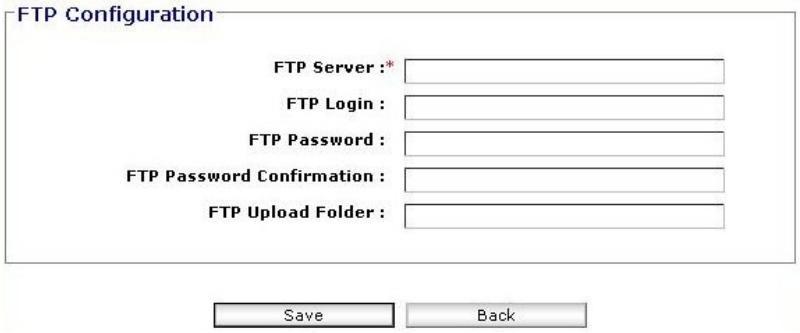

Figure 28: FTP Server Configuration

To configure the FTP server:

1. Enter the **FTP Server** address.
2. Enter the **FTP Login** ID.
3. Enter the **FTP Password**. Re-enter the password to confirm.
4. Identify the **FTP Upload Folder**.
5. Click **Save** to save the FTP configuration or **Back** to exit without saving.

3.12.3 CONFIGURE THE FAX SERVICE

To define the Fax service, click **FAX Server Configuration**. The Fax service is used to fax documents from the **OpenEDMS** repository. The fax modem must be installed on the OpenEDMS server.

Figure 29: Fax Service Configuration

To configure the fax server:

1. Identify the type of **FAX Allow Files**, for example, PDF, TXT, or DOC.
2. In Bytes, identify the **Maximum FAX File Size**.
3. From the dropdown select the **FAX Default Mode**.
4. Identify the **FAX Port** used by the fax modem service.
5. Identify the **FAX Timeout** value of the fax modem service.
6. Identify the **FAX Send Area Code** of the fax modem service.
7. Identify the **FAX International Code** of the fax modem service.
8. If you are using the EFAX service, identify the **EFAX Email Account**.
9. Click **Save** to save the FAX configuration or **Back** to exit without saving.

3.12.4 CONFIGURE DISK DRIVES

To configure your disk drives, click **Disk Drive Configuration**. Disk Drive Configuration allows administrators to designate the primary and secondary disk drives where documents will be stored in the **OpenEDMS** server environment.

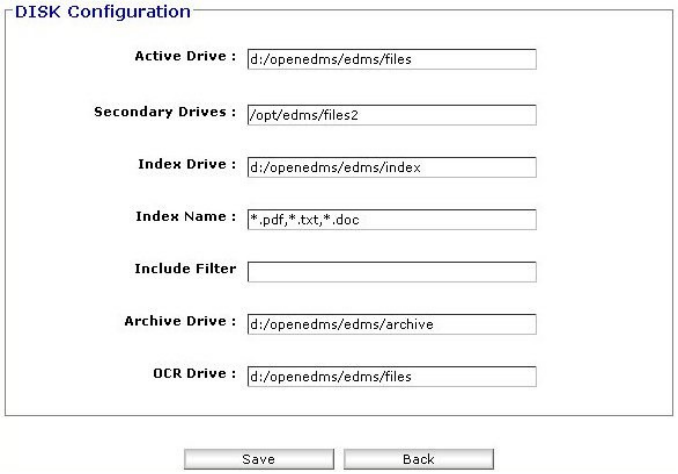

Figure 30: Disk Drive Configuration

To configure the disk drives:

1. Enter the address of the **Active Drive**; this is the primary location where files will be stored on the server.
2. Enter the address of the **Secondary Drive**; this is the secondary location where files will be stored on the server.
3. Identify the address of the **Index Drive**; this is the location where file indices will be stored on the server.
4. Enter the **Index Name**.
5. Enter the **Include Filter** name, for example, **.pdf*, **.txt*, or **. doc*.
6. Enter the **Archive Drive** address; this is the location where archived files will be stored on the server.
7. Enter the **OCR Drive** address; this is the location where the OCR engine is installed on the server.
8. Click **Save** to save the disk drive configuration or **Back** to exit without saving.

3.12.5 CONFIGURE THE DEFAULT PANEL CONFIGURATION

To define the default panel configuration, click **Default Panel Configuration**. You can identify the panel that will display immediately after users log in to **OpenEDMS**.

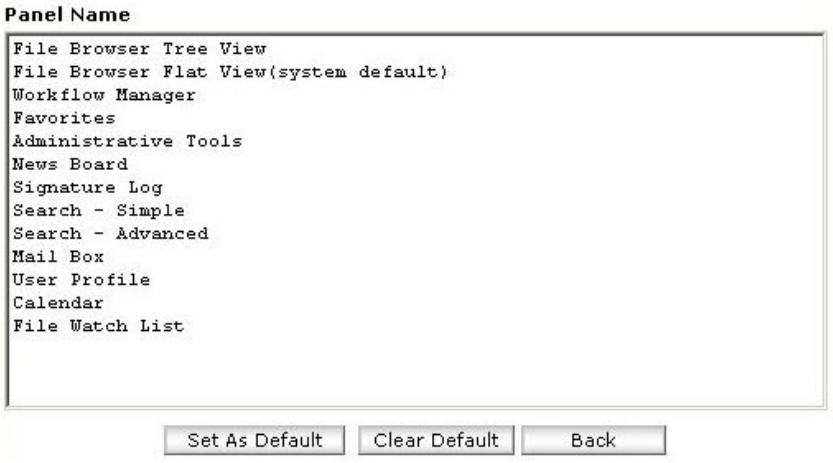

Figure 31: Default Panel Configuration

To configure the default panel:

1. Select a panel from the list and click **Set as Default**.
2. Click **Clear Default** to remove the default panel.
3. Click **Back** to exit without changing the default panel configuration.

3.12.6 SET THE DEFAULT BROWSER TIME OUT VALUE

To define the default browser timeout value, click **Default Browser Time Out**. When the active browser session times out, a session warning displays informing users that the session will expire in *x* seconds. Users have the option of letting the session expire, of logging out, or of keeping the session alive.

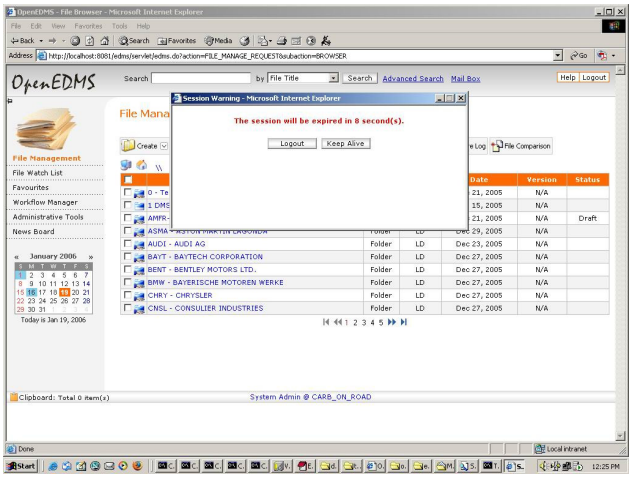

Figure 32: Browser Time Out Warning Message

To set the session time out value:

1. Enter a value in minutes.
2. Click **Save** to update the session time out value or **Back** to exit this dialog without saving changes.

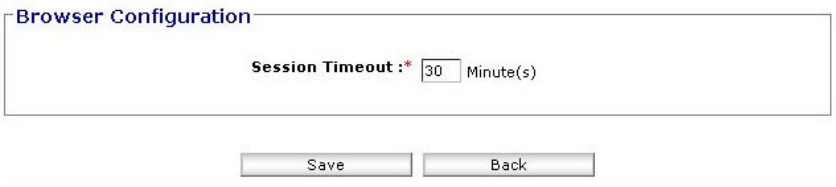

Figure 33: Browser Time Out Configuration

3.12.7 SET THE SYSTEM TIMER

The system timer allows you to set the time of day at which batch processing of OCR scans, workflow notifications, retention policy expiration notifications, retention policy folder moves, etc. will be executed.

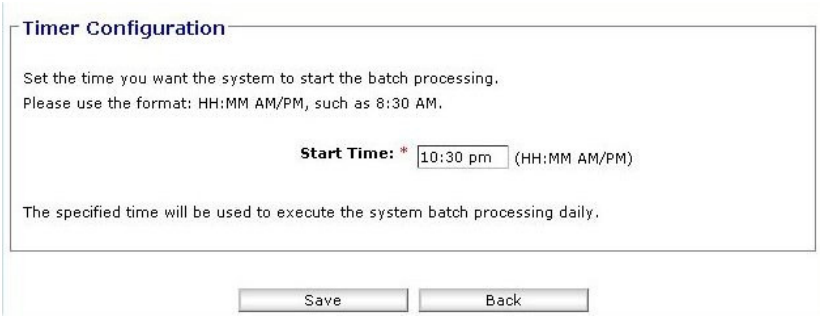

Figure 34: System Timer Configuration

To set the system timer:

1. Enter the time (**HH:MM AM**/**PM**) at which you want to daily execute all batch processing.
2. Click **Save** to update the system timer value or click **Back** to exit this dialog without saving the changes.

3.12.8 DEFINE ENCRYPTION PASSWORD

OpenEDMS uses **P**assword **B**ased **E**ncryption (PBE) to encrypt folders and files in the **OpenEDMS** repository. OpenEDMS will use the password you enter here to automatically encrypt and decrypt folders and files for authorized users. Authorized users do not need to enter the password to view encrypted files; they only need have the required access permissions.

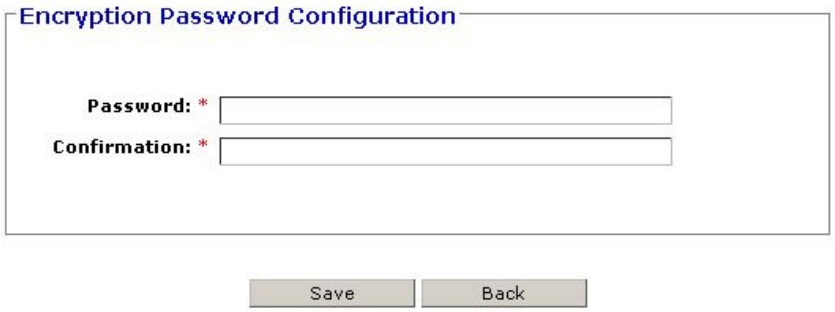

Figure 35: Encryption Password

To define the encryption password:

1. Enter the **password**. The password can be of any length and combination of alphanumeric characters.
2. Enter the password again to **confirm**.
3. Click **Save** to save the encryption password and return to the Server Configuration window. Click **Back** to exit without saving the encryption password.

3.13 PDF WATERMARK SETTINGS

You can create, edit, and delete PDF watermark images. These watermarks can be added to pdf documents distributed when a workflow process is completed.

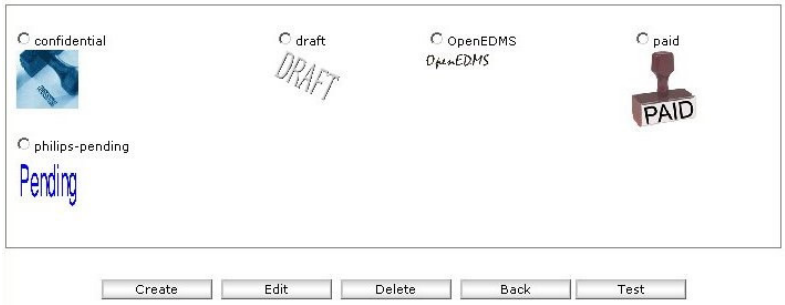

Figure 36: Watermark Management

To create a new PDF watermark:

1. Click **Create**. The **Watermark Image** dialog is displayed.

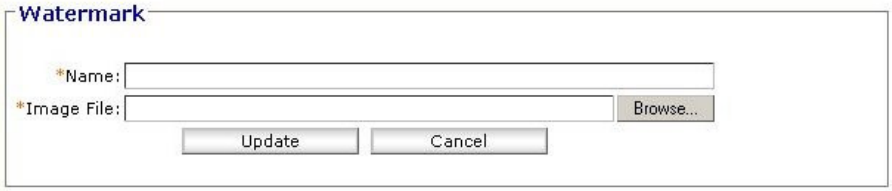

Figure 37: Create Watermark Image

2. Enter a **Name** for the new PDF watermark.
3. Enter the **Image File** you want to use or click **Browser** to select an image file.
4. Click **Update** to add the image to the list of available PDF watermarks or click **Cancel** to return to the **PDF Watermark Settings** dialog.

To edit a PDF watermark:

1. Select a PDF watermark and click **Edit**. The **Edit Watermark Image** dialog is displayed.
2. Make the necessary changes.
3. Click **Update** to save changes to the PDF watermark or click **Cancel** to exit the Edit Watermark Image dialog without saving any changes.

To delete a PDF watermark:

4. Select a PDF watermark and click **Delete**. The selected PDF watermark is removed from the list.

To test a PDF watermark:

5. Select a PDF watermark and click **Test**. A sample pdf document is displayed showing the PDF watermark. This sample is how documents will appear when they are distributed from a completed workflow process.

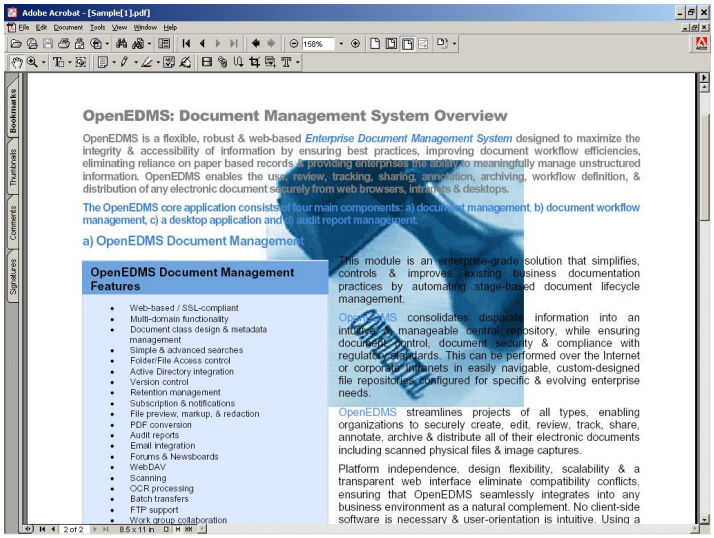

Figure 38: Sample PDF Watermark

3.14 SYSTEM AUDIT REPORTS

At any time, system administrators can review comprehensive system audit reports containing precise and detailed information about all domain activity and resource usage.

Additionally, it is possible to view all activity within a fixed time frame by specifying an exact or approximate date range.

In this way, every event or operation can be traced to its exact origin so as to ensure end-user accountability and strict compliance with internal or external regulatory standards.

For detailed information on OpenEDMS system audit reports, refer to the companion **OpenEDMS Reports Guide**.

3.15 ARCHIVE MANAGEMENT

Rather than delete repository resources that have ceased, for the current time, to serve an active purpose, you can consign selected resources to the system archives where you can subsequently retrieve them, if needed. Archiving resources enables you to remove outdated or inactive resources from the repository without the risk of irretrievably losing them. Archives can also be used as backups to your document repository.

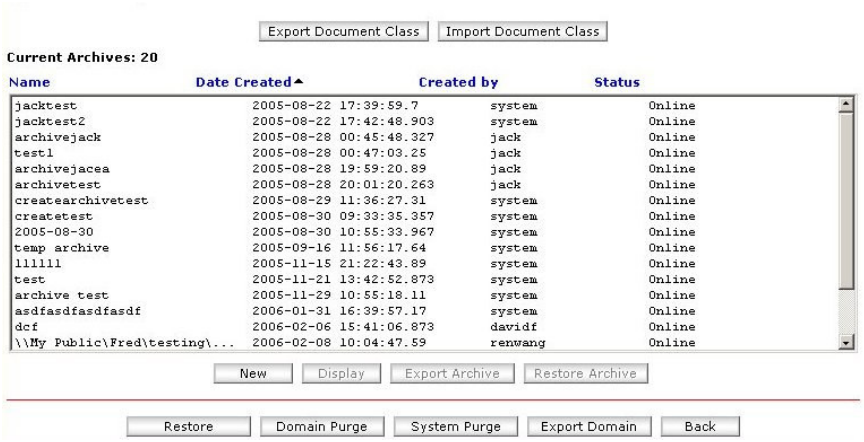

Figure 39: Archive Management

To create a new archive:

1. Click **Create** on the **Archive Management** window. **The Create New Archive** dialog is displayed.

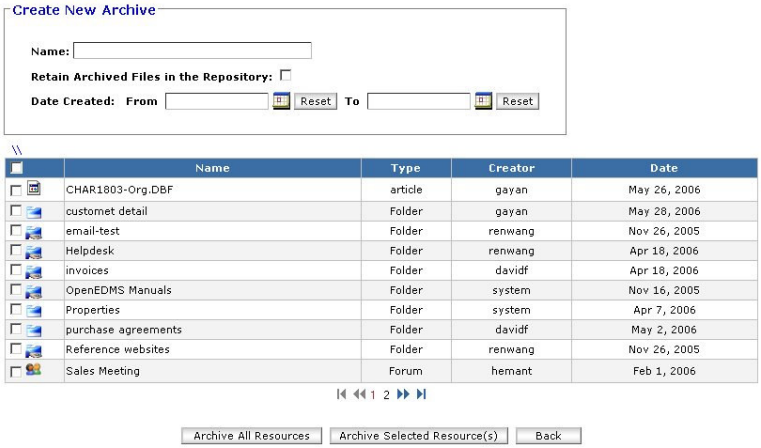

Figure 40: Create New Archive

2. Enter a **Name** for the new archive.
3. Select whether or not to **Retain Archived Files in the Repository**. If you check this box, a copy of the selected resources will be stored in the archive; the originals will remain in the document repository. The resources will continue to be displayed in the **File Browser**.
4. Enter the **Date Created** range for the archive.

5. In the displayed File Browser, select the resources to be archived and click **Archive Selected Resource(s)** to archive only the selected resources.
6. Click **Archive All Resources** to archive all resources currently stored in the repository. This allows you to create a back up of your domains for use in disaster recovery procedures.
7. Click **Back** to return to the **Archive Management** window.

To display the contents of an archive:

1. Select the archive to be viewed and click **Display**. The **Archive Information** dialog is displayed.

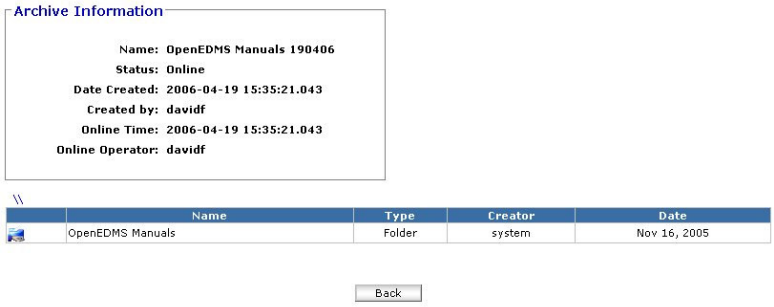

Figure 41: Displaying the Contents of an Archive

2. You can navigate the archive information in the same way as you navigate the **File Browser**.
3. Click **Back** to return to the **Archive Management** window.

To export an archive:

1. Select the archive to be exported and click **Export Archive**. When you click **Export Archive** a message is displayed informing you that the selected archive has been saved to the server.

   ***Note**: the System Administrator defines the default archive storage location on the server in the Disk Drive Configuration function of the Server Configuration module.*

To restore an archive:

1. Select the archive to be restored and click **Restore Archive**. The selected archived resources will be copied to the repository in the specified location.

To export a document class:

1. Click **Export Document Class** on the **Archive Management** window. A text file containing the document class listing is emailed to you. Click **Back** to return to the **Archive Management** window.

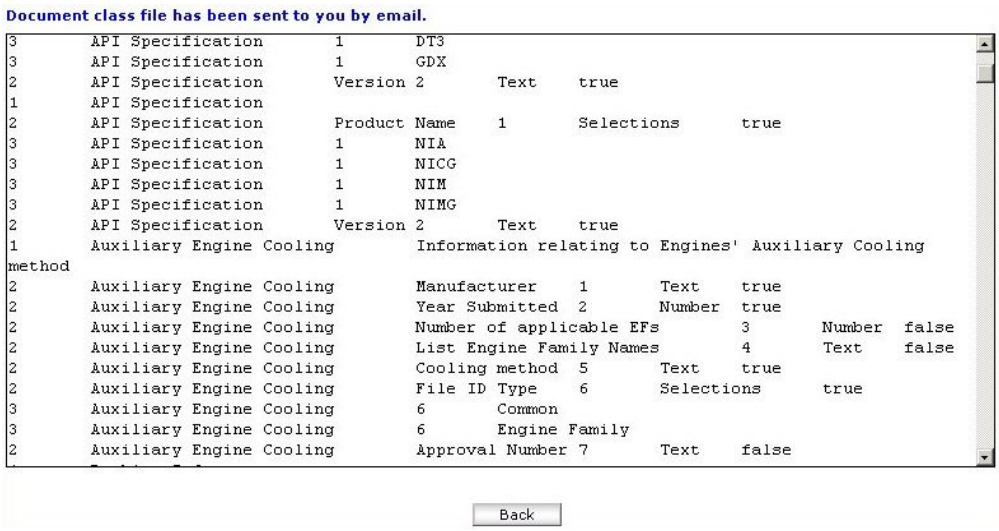

Figure 42: Export Document Class

To import a document class:

1. Click **Import Document Class** on the **Archive Management** window. The **Select Document Class** dialog is displayed.

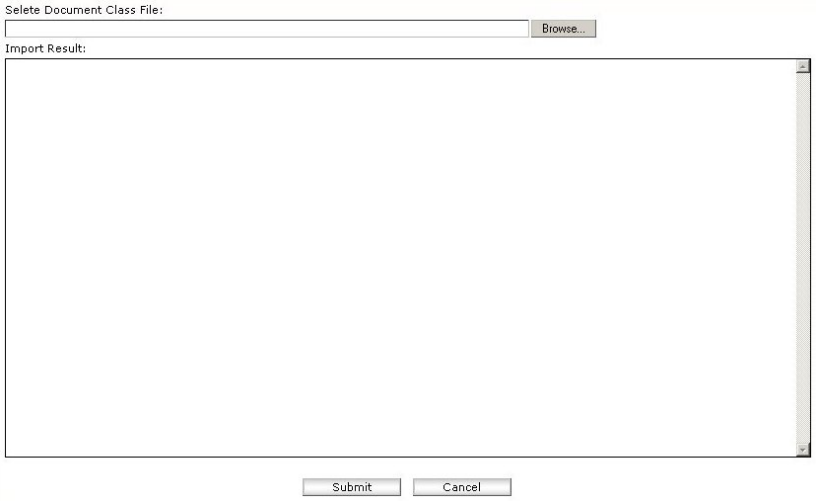

Figure 43: Import Document Class

2. Click **Browse** to select the document class file to import.
3. Click **Submit** to initiate the import of the selected document class file(s).
4. The **Import Result** field lists the document class file(s) that were imported to the Document Class Management module.
5. Click **Cancel** to return to the **Archive Management** window.

3.16 LICENSE MANAGEMENT

A valid license key password is required to activate the **OpenEDMS** server. In the **License Management** module you can enter the **OpenEDMS** license. Click **License Management** on the **Administrative Panel** to display the **Activate License** dialog.

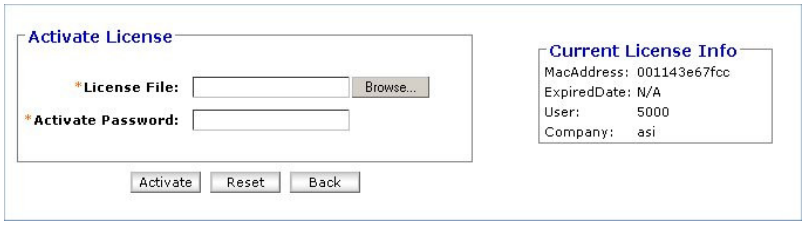

Figure 44: License Management

To activate the OpenEDMS server:

1. Enter the **License File**. Click **Browse** to locate the License File on your server. The install package includes an temporary evaluation license file “asiedms.lic”. You can find the file in the [openedms_install_directory]\edms\template folder. The temporary evaluation license files is valid for three (3) months, for ten (10) concurrent users.
2. Enter the **Activate Password**.
3. Click **OK** to enter/change the license password, **Reset** to empty the fields so you can re-enter the password, or **Back** to return to the **Administrative Panel** without changing the license password.

In the **Current License Info** panel, you will find current information regarding your OpenEDMS license.

- **MAC Address**: This field identifies your server’s MAC address. The license key is only valid for this MAC address.
- **Expire Date**: This field identifies the date on which the license will expire. This applies only to the temporary evaluation license.
- **Concurrent Users**: This field identifies the number of concurrent users supported by your license.
- **Company**: This field identifies your company.

3.18 MESSAGE TEMPLATE SETTINGS

In **Message Template Settings** you can define the default message sent to all users who register in **OpenEDMS**. You can define a plain text message or add html code to the message to define a specific look and feel, particular to your organization.

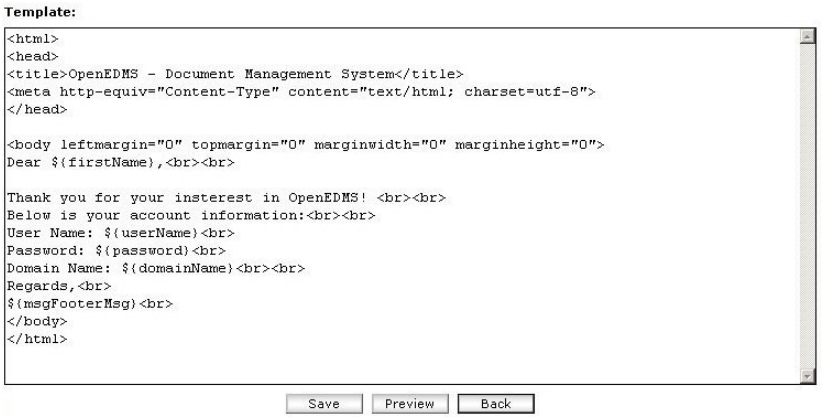

Figure 45: Message Template Settings

To create a message template:

1. Enter and format the message text.
2. Click **Preview** to see how the message will appear to recipients.
3. Click **Save** to save the message and return to the **Administrative Tools** panel.
4. Click **Back** to return to the **Administrative Tools** panel without saving any changes to the message template.

3.19 PRINTER SETTINGS

Printer Settings identify the system printers, which authorized users can use to print documents. The printer is attached to a server and allows server-side printing.

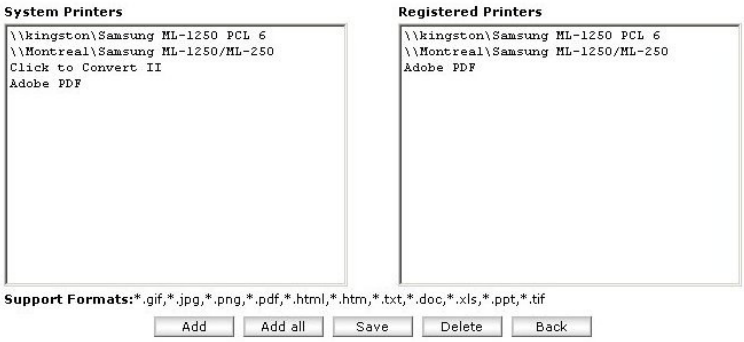

Figure 46: Printer Settings

1. **System Printers** lists all of the printers attached to the server.
2. Click **Add** to add a system printer to the list of **Registered Printers** that authorized users can print from.
3. Click **Add All** to add all identified system printers to the list of **Registered Printers**.
4. Select a printer in the list of registered printers and click **Delete** to remove that printer from the list of **Registered Printers**.

5. Click **Save** to save changes to the **System Printers Settings** dialog.
6. Click **Back** to return to the **Administrative Tools** panel without saving and changes to the **System Printer Settings**.

3.20 NEWS BOARD MANAGEMENT

OpenEDMS supports a news board in which users of **OpenEDMS** can create and publish news items that can be published internally within **OpenEDMS** or externally on the **OpenEDMS** website login screen.

To access News Board Management:

1. Click on **News Board Management** in the right side panel. The **News Board Management** dialog is displayed.

Figure 47: News Board Management dialog

In the **News Board Management** module, regular users can create news items and view all internal and external news.

***Note**: Regular users of **OpenEDMS** can only create news articles, they cannot publish it to the system. Admin users can create and publish news.*

To create news:

1. Click **Create News**. The **Create News** dialog is displayed.

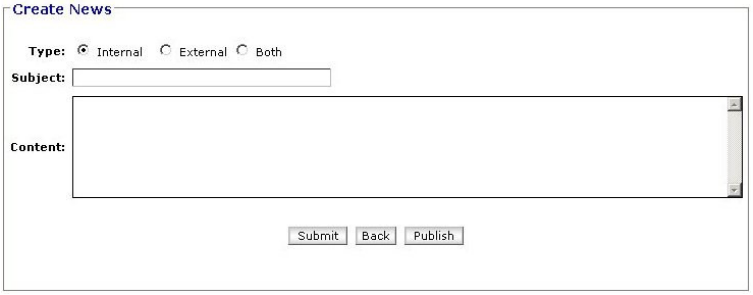

Figure 48: Create News dialog

2. Select the **Type** of news item you are creating: *Internal*, *External*, or *Both*. **Internal** news (i.e. private) can only be seen by those logged in to OpenEDMS. **External** news (i.e. public) can be viewed by anyone who visits the website, regardless of whether or not they are a registered user. **Both**, publishes the news internally and externally.
3. Enter the **Subject** of the news item.
4. Enter the **Content** of the news item.
5. If you are a regular user of **OpenEDMS**, click **Submit** to submit the news article to review by the system or domain administrator. Click **Back** to return to the

News Board Management dialog without submitting the news item to review. If you are an admin user, click **Publish** to publish the news.

***Note**: Submitted news must be reviewed and published by an admin user.*

To view news:

1. Click **View News**. The **View News** dialog is displayed. In this dialog you can search for news based type, status, and date range. Admin users can also update/modify news and publish it.

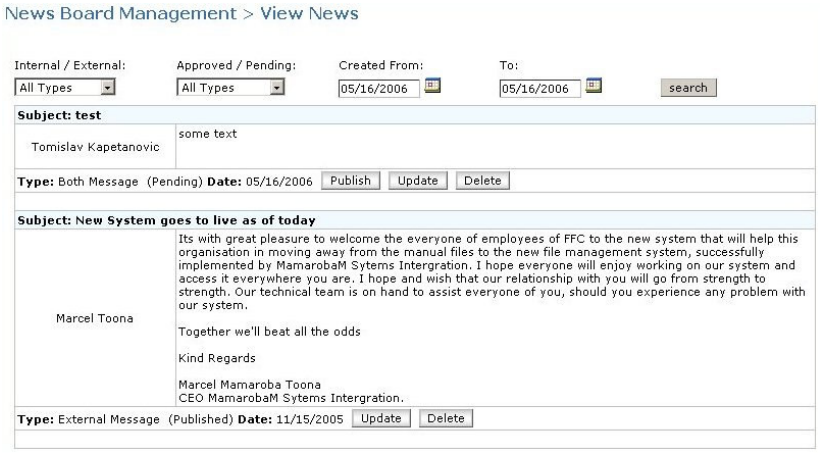

Figure 49: View News dialog

To publish news:

1. In the **View News** dialog, click the **Publish** button corresponding to the news item you wish to publish. The news item is immediately published (internally, externally, or both; depending on the specified **Type**).

To update news:

1. In the **View News** dialog, click the **Update** button corresponding to the news item you wish to update/modify. The **Update News** dialog is displayed.

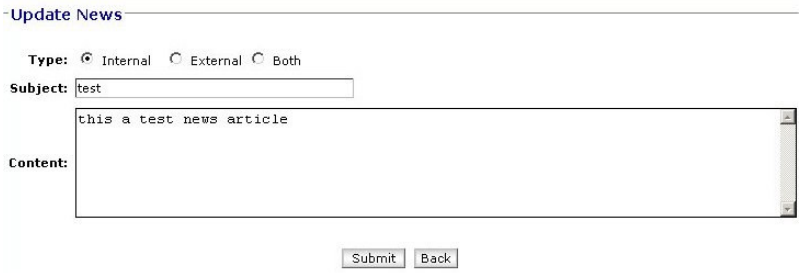

Figure 50: Update News dialog

2. Select the **Type** of news item you are creating: *Internal*, *External*, or *Both*. **Internal** news (i.e. private) can only be seen by those logged in to OpenEDMS. **External** news (i.e. public) can be viewed by anyone who visits the website, regardless of whether or not they are a registered user. **Both**, publishes the news internally and externally.
3. Enter the **Subject** of the news item.
4. Enter the **Content** of the news item.
5. Click **Submit** to submit the news item for review, or click **Back** to return to the **View News** dialog without saving any changes to the news item.

***Note**: If you click **Submit**, you then have to publish the news item from the **View News** dialog.*

To delete news:

1. Click the **Delete** button corresponding to the news item you wish to delete. The news item is automatically deleted from the system. The **View News** dialog refreshes automatically.

To search news:

You can search for news items based on news item type (internal, external, or both), status (pending or published), and date range.

1. Enter your search criteria and click **Search**. News items corresponding to your search criteria are displayed in the **View News** window.

4. SYSTEM BACKUP AND RECOVERY

4.1 DATABASE BACKUP

OpenEDMS uses the *MS SQL Server Backup Agent* to perform the database backup. In the EDMS server, the *MS SQL Server Backup Agent* can be configured to automatically start the database backup process every day at a specific time, such as 1:00 AM. The backup information will be saved into the target backup file, for example, d:\openedms\database-backups\database.db file, which contains daily incremental database information.

The tape backup process should save the d:\openedms\database-backups\database.db daily and put it onto a permanent media weekly for system recovery.

4.2 NATIVE FILE BACKUP

In the OpenEDMS Server environment, all of the native files (including all the versions) are saved in the system active and secondary drives. These folders should be stored on the tape daily and put onto permanent media weekly for recovery purposes.

4.3 OPENEDMS APPLICATION BACKUP

The OpenEDMS system was installed in the EDMS server. The system binary files are stored in the application server “webapps” folder. All its subfolders and files should be backed up monthly to permanent media for recovery.

The system configuration file **oe.cfg** and system html template files from the template folder and subfolders should be saved to a backup media. Since these files are static, they only need to be saved once.

4.4 SYSTEM RECOVERY PROCESS

Altimate Systems can provide assistance to conduct OpenEDMS System recovery provided all the backup files (Database backup, Native File backup, and application backup) are available.

Client system administrators may also perform the backup process by:

a. Recovering the database to MS SQL Server using the database backup file.
b. Recovering the native files to the EDMS Server by copying the native file backup to the target file folder
c. Recovering the OpenEDMS Application server to the application server by copying the *edms* folder (including its subfolders and files) to the webapps directory.
d. Copying the EDMS template files to the target template folder.
e. Copying the EDMS configuration files to the tomcat installation folder.

5. FILE IDENTIFICATION

Every resource contained in the repository can optionally be tagged with a system-generated, timestamp-based identification number assigned as a metadata property.

It is also possible for clients to implement their own File ID system by modifying the **OpenEDMS** configuration file (oe.cfg) using a Java File ID API.

For example, a File ID with a new class called BarCodeID could be added to **OpenEDMS** by modifying the oe.cfg file as follows:

FileIDMode=BARCODE
BARCODE=com.myco.BarCodeFid

The File ID class name *BARCODE* would then appear listed as an available option whenever File ID is selected as a metadata attribute of a new document class.

6. WEBDAV CONFIGURATION

WebDAV, or **Web**-based **D**istributed **A**uthoring and **V**ersioning, is a set of extensions to HTTP protocol which allow users to collaboratively edit and manage files stored on remote web servers in a familiar Windows environment.

To enable WebDAV access to a remote **OpenEDMS** server from Microsoft Windows®, open **My Network Places** and select **Add a network place.**

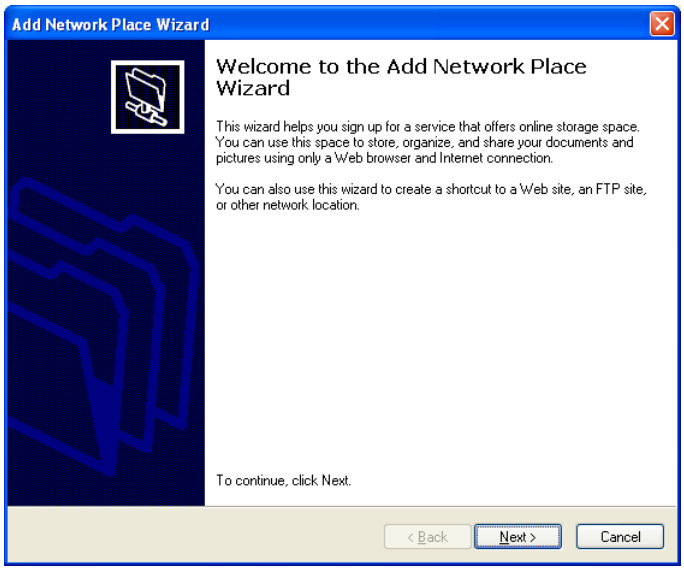

Figure 51: Add Network Place Wizard

When prompted to select a service provider by the **Add Network Place Wizard**, click **Choose another location** and enter a valid WebDAV URL followed by an active domain name (e.g. *http://www.openedms.com:80/edms/webdav/Demo*).

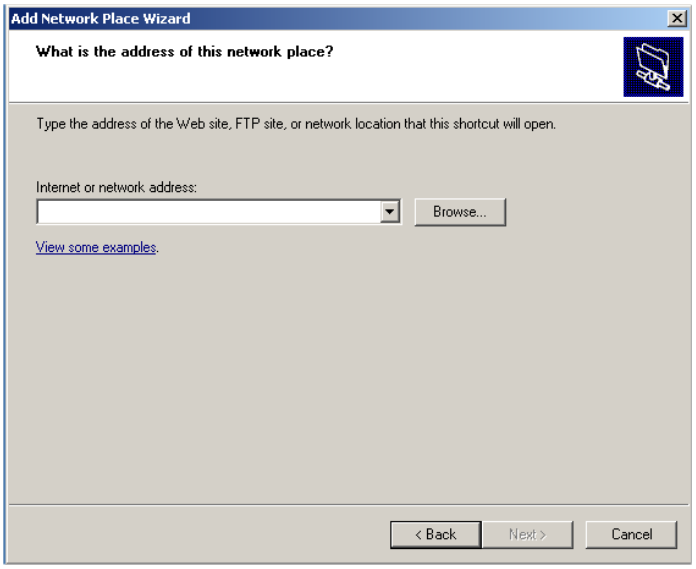

Figure 52: Define Network Location

Enter a valid user ID and password (each of which must be registered in the target domain) before specifying a name for the shortcut to the domain.

Once the WebDAV client has been properly configured, registered users can login to **OpenEDMS** and directly access domain content from a familiar Windows environment.

The remote **OpenEDMS** server will be treated as a local network drive, which can be opened at any time from **My Network Places** on the Windows desktop. For more information on using OpenEDMS WebDAV, please refer to the companion **OpenEDMS User Guide**.

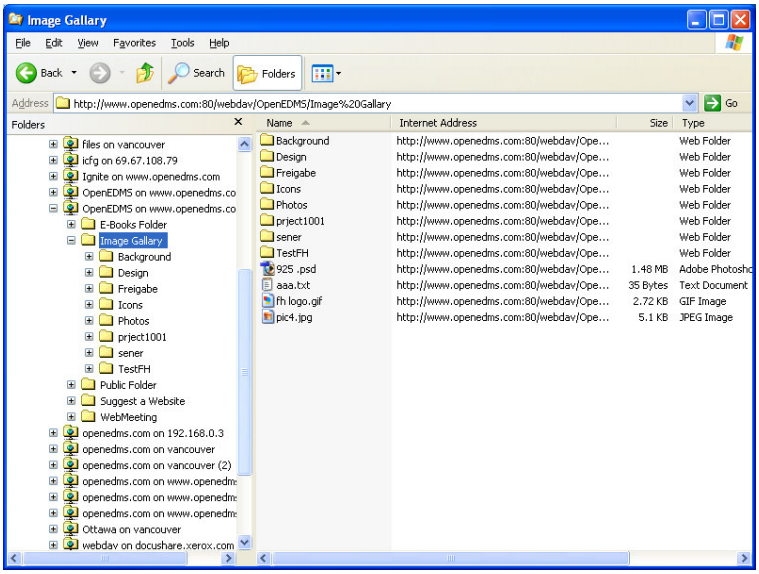

Figure 53: OpenEDMS via WebDAV

7. APPENDIX A. RELATED DOCUMENTS

- **OpenEDMS User Guide**
- **OpenEDMS Installation Guide**
- **OpenEDMS Desktop Guide**
- **OpenEDMS Report Guide**

8. **INDEX**