Security: User Feature Rights

Laserfiche Implementation

Company: **Cybercrime Investigation and Coordinating Center (CICC)**

Project Name: **LASERFICHE ENTERPRISE CONTENT MANAGEMENT SYSTEM**

	1	2	3	4	5	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
Migrate Documents															
Delete															
Properties															
Process															
Move Object															
Edit text															
Export															
Print															
Search															
Import															
Scan															

User Name	Group
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	

Metasystems Development Inc.		**Cybercrime Investigation and Coordinating Center**	
Name:	Earl Abada Signature over Printed Name	Name:	 Signature over Printed Name
Title:	Manager	Title:	
Date:		Date:	

Security: User Access Rights

Laserfiche Implementation

Company: **Cybercrime Investigation and Coordinating Center (CICC)**

Project Name: **LASERFICHE ENTERPRISE CONTENT MANAGEMENT SYSTEM**

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
Create Folders															
Create Documents															
Write Metadata															
Access Control															
See Through Redaction															
Annotate															
See Annotation															
Create Shortcuts															
Rename															
Delete Shortcuts															
Delete															
Append Data															
Write															
Read															
Browse															

User Name	Group	Folder / Document
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

Metasystems Development Inc.

Name: Earl Abada
Signature over Printed Name

Title: Manager

Date:

Cybercrime Investigation and Coordinating Center

Name:
Signature over Printed Name

Title:

Date:

Security: Privileges

Laserfiche Implementation

Company: **Cybercrime Investigation and Coordinating Center (CICC)**

Project Name: **LASERFICHE ENTERPRISE CONTENT MANAGEMENT SYSTEM**

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
Manage Connections															
Manage Entry Access															
Manage Metadata															
Manage Volumes															
Manage Trustees															

User Name	Group
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	

Metasystems Development Inc.

Name: Earl Abada
Signature over Printed Name

Title: Manager

Date:

Cybercrime Investigation and Coordinating Center

Name:
Signature over Printed Name

Title:

Date:

Security Definition

Laserfiche’s security system provides access controls to documents and folders. It has two fundamental purposes:

- To prevent unauthorized access to confidential information
- To safeguard data against loss and corruption due to improper operation of the system.

Users and Groups

The Laserfiche Server maintains its own set of accounts, which are separate from operating system accounts. Each Laserfiche account in a repository must be assigned a unique name.
One set of accounts that a Laserfiche Server maintains consists of groups. A group is a named set of users. Groups can be used to model roles in an organization. This can reduce the burden on the Laserfiche security administrator, as access controls can be applied to sets of users that correspond to job functions in an organization rather than explicitly assigning access rights to individual user accounts.
The other set of accounts that a Laserfiche Server maintains consists of users. A person can use a Laserfiche user account to access a Laserfiche repository. A user account enables the user to authenticate to the repository and, with the appropriate rights, allows access to documents and folders stored in the repository. The groups to which a user belongs affects that user's privileges and feature rights. A user can log on with a user account, but not with a group account.

An ***administrator*** is any user that has been granted the ability to perform operations beyond the normal operations of working with documents and folders in a Laserfiche repository. Administrators are usually those tasked with maintenance duties.

There are several types of rights in the Laserfiche security system: feature rights, access rights and privileges.

Feature Rights

Feature rights allow a user to perform specific actions, such as scanning and printing. The right to perform these specific features applies across the entire repository. For example, if the user does not have the feature right that allows printing, then the user cannot print any documents in the repository. Assigning a feature right to a user does not mean that the user will be able to perform the desired action on all documents and folders. The user must still have the appropriate entry access rights on the document or folder.
The following is a list of available feature rights.

- **Scan:** Grants the ability to scan into a new or existing document.
- **Import:** Grants the ability to import files into the repository.
- **Search:** Grants the ability to perform any type of search.
- **Print:** Grants the ability to print information from the repository.
- **Export:** Grants the ability to export images, text, briefcases, folder list contents, listings of search results, and electronic files.
- **Edit Text:** Grants the ability to modify the text associated with a document.
- **Move Object:** Grants the ability to move documents, electronic documents, and folders to a different folder. It also grants the ability to move pages from one document to another document.
- **Process:** Grants the ability to OCR image pages, index documents, retrieve text from an electronic file, or process electronic documents using Laserfiche Snapshot. This feature right does not affect whether you can print an electronic file using Laserfiche Snapshot.
- **Properties:** Grants the ability to view property information.
- **Delete:** Grants the ability to delete documents and folders.
- **Migrate Documents:** Grants the ability to migrate documents from one volume to another.

Access Rights

Access rights checking is the primary mode of access control. Each operation on a document or folder has a set of required entry access rights. If the user attempting the action does not have the necessary rights, the user is denied the operation.
Note: The privilege security mechanism can bypass certain aspects of access rights checking. Privileges control access to system functions, whereas entry access rights control access to documents and folders.
The following is a list of entry access rights:

- **Browse:** Grants the ability to see the existence of a document or folder when browsing through folders. This right has no bearing on the following functionality: whether a document or folder appears as a search result, whether a document's content can be seen, or whether a folder can be opened.

Important: The Browse right is not sufficient to view the contents of a folder. The Read entry access right on the parent folder is also required. If a user has been granted Browse entry access right, but not the Read right on the parent folder, then the folder will appear empty when it is opened by that user.

- **Read:** Grants the ability to open a folder, open a document, view field values, search for a document, view all metadata, and view all properties. Note that to view the images, text, and/or electronic file associated with a document requires the Read volume access right and that to view field values requires the Read field access rights.
- **Write:** Grants the ability to modify the contents of a document. This includes generating or replacing text via OCR. This right allows the user to add pages, move pages, remove pages, rotate images, and move documents and folders to other folders. This right implicitly grants the following entry access rights: Read, Append Data, Annotate, See Annotations, and See Through Redactions.
- **Append Data:** Grants the ability to add pages to the end of a document. If a document does not have preexisting text, then this right grants the ability to generate the text of a document via OCR. This right implicitly grants the Read entry access right. This right does not allow a user to append text to the end of preexisting text. This right does not allow a user to add any type of annotation.
- **Delete:** Grants the ability to delete a document or folder. When deleting a folder, the user must also have the necessary rights to delete all entries that reside in the folder. This right does not allow a user to delete pages or text from a document.
- **Delete Shortcut:** Grants the ability to delete shortcuts to an entry.
- **Rename:** Grants the ability to rename an entry.
- **Create Shortcut:** Grants the ability to create a shortcut to an entry.
- **See Annotations:** Grants the ability to see all annotations (sticky notes, stamps, highlights, and redactions). However, this right doesn't grant the ability to see through redactions. This right implicitly grants a user the Read entry access right.
- **Annotate:** Grants the ability to add, modify, or remove annotations to a document. However, adding, modifying, or removing redactions also requires the See Through Redactions right. This right implicitly grants the See Annotations and Read entry access rights.
- **See Through Redactions**: Grants the ability to see through redactions. This right does not grant the ability to see other types of annotations. This right implicitly grants the See Annotations and Read entry access rights.
- **Access Control:** Grants the ability to assign access rights on an entry.
- **Write Metadata**: Grants the ability to edit metadata assigned to an entry. This right implicitly grants the Read entry access right. This right allows a user to change a document's template as well as edit field values. This right grants the ability to edit document links, and document versions. This right also grants the ability to assign informational or security tags to documents and folders. The available security tags are limited to those granted to you.
- **Create Documents:** Grants the ability to create documents in a folder. This right implicitly grants the Read entry access right.
- **Create Folders:** Grants the ability to create folders. This right implicitly grants the Read entry access right.

Privileges

Privileges are special account rights that grant the ability to perform operations dealing with the management of a Laserfiche repository. Typically, privileges cover administrative activities that only need to be performed by specially designated individuals in an organization.

Privileges should not be granted to regular users. Privileges should only be granted to "trusted" users tasked with carrying out administrative tasks. Standard tasks such as filing, viewing, and modifying documents do not require any privileges, only the necessary access rights.

The privilege security mechanism is a separate security mechanism from the access right security mechanism. Certain privileges grant capabilities that overlap with entry access rights. In these cases, by having the appropriate privileges, these users can bypass the access rights security mechanism.

The following is a list of available privileges.

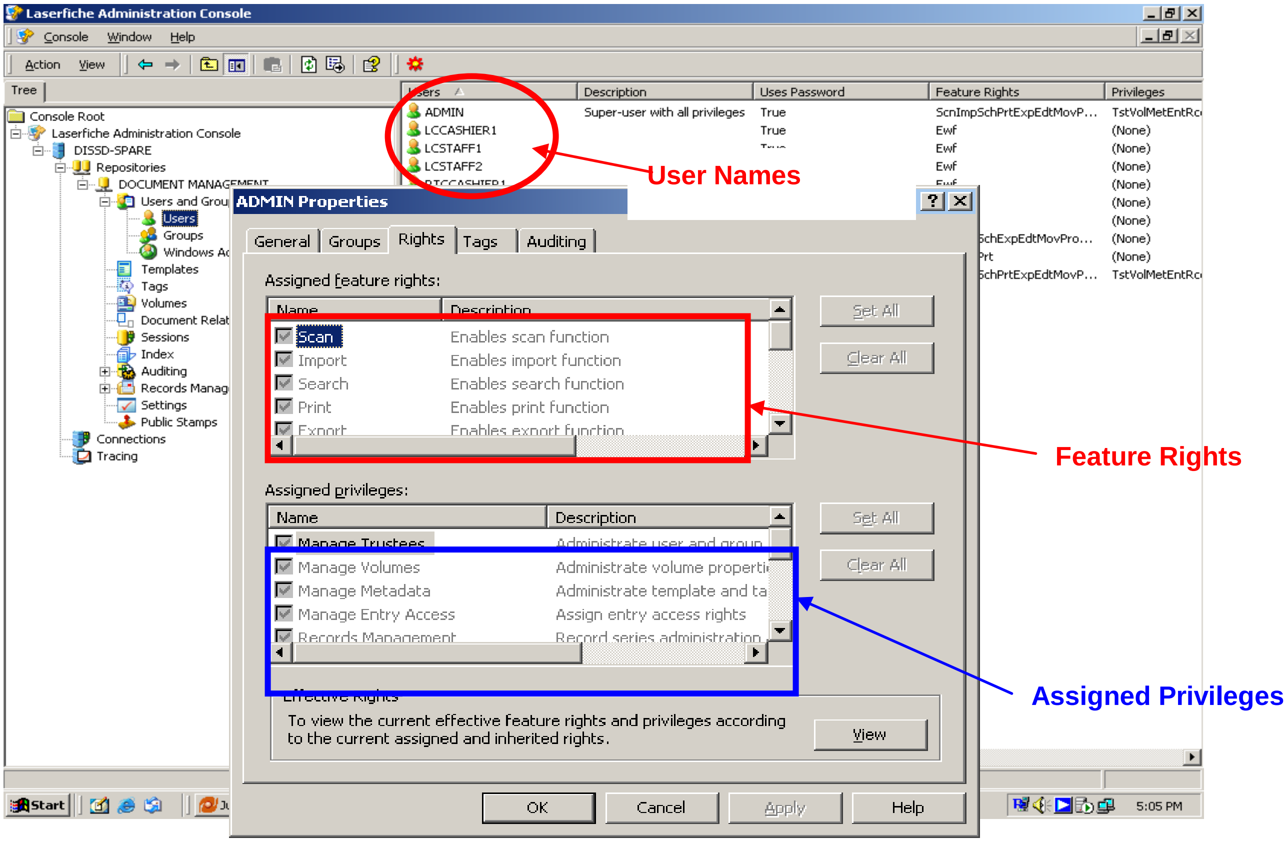
- **Manage Trustees:** Grants the ability to create/delete users and groups, add/remove members of groups, edit the descriptions of users and groups, set a password for a user without knowing that user's original password, set feature rights, and enable/disable an account. This privilege does not allow a user to grant/revoke privileges.
- **Manage Volumes:** Grants the ability to create/delete a volume, attach/detach/export a volume, create logical volumes, limit volume size, grant/deny volume access rights, change the volume name, and change the volume paths.
- **Manage Metadata:** Grants the ability to create/delete a template, modify template settings, grant/deny field access rights, create/delete tags, and modify tag settings. This privilege grants the ability to assign tags to users and groups, but not the ability to assign tags to documents and folders. This privilege does not grant the ability to view or set the field data assigned to a document or folder.
- **Manage Entry Access:** Grants the ability to grant/deny entry access rights to all documents and folders in a repository. To smoothly perform this task, this privilege bypasses several security mechanisms. This privilege bypasses the Browse and Access Control entry access rights. This privilege bypasses the Read entry access right on folders. This privilege also allows a user to browse through documents and folders associated with security tags that have not been assigned to him/her. This privilege does not grant the ability to assign volume access rights, nor does it grant the ability to assign field access rights.
- **Manage Connections:** Grants the ability to view all active connections to a repository and to disconnect a currently connected user.

Setting Up Security

When CLIENT creates a database, an administrator named ADMIN with no password and a group named EVERYONE are automatically added to the CLIENT’s database. Security will not be enabled until one of the following occurs:

- ➢ ADMIN is given a password.
- ➢ Security will be disabled if ADMIN’s password is removed.
- ➢ Setting up security is done through several dialog boxes:
  - In Administration console, Users and Group dialog box allows you to create, modify, and delete users and groups, and assign users to groups. It also permits the setup of the feature rights to users and groups.
  - The Access Rights dialog box shows the rights a user or group has to a particular document or folder, and can display the Assign Rights dialog box to let you modify those rights.
  - The Assign Rights dialog box lets you assign access rights to a document or folder for a user or group.

Below are the example screenshot of Access rights, Feature Rights and Priveleges:



Users	Description	Uses Password	Feature Rights	Privileges
ADMIN	Super-user with all privileges	True	ScnImpSchPrtExpEdtMovP...	TstVolMetEntRc
LCCASHIER1		True	Ewf	(None)
LCSTAFF1		True	Ewf	(None)
LCSTAFF2			Ewf	(None)
RTCCASHIER1			Ewf	(None)
				(None)
				(None)
			SchExpEdtMovPro...	(None)
			Prt	(None)
			SchPrtExpEdtMovP...	TstVolMetEntRc

Assigned feature rights:

Name	Description
☑ Scan	Enables scan function
☑ Import	Enables import function
☑ Search	Enables search function
☑ Print	Enables print function
☑ Export	Enables export function

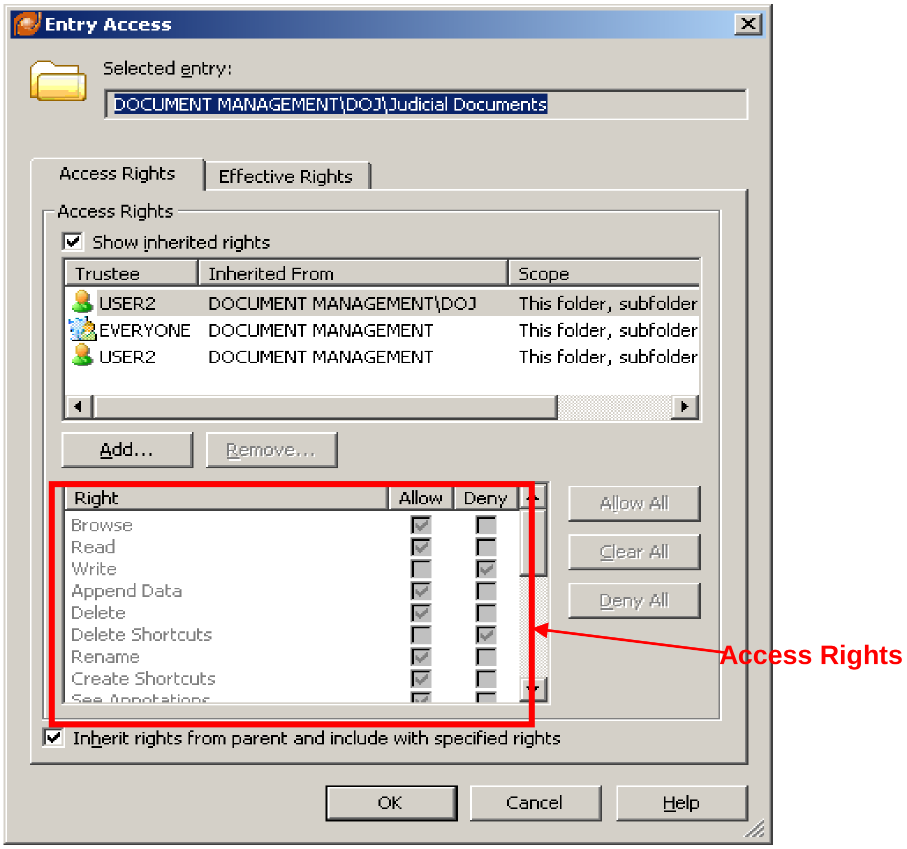
Assigned privileges:

Name	Description
☑ Manage Trustees	Administrate user and group
☑ Manage Volumes	Administrate volume properti
☑ Manage Metadata	Administrate template and ta
☑ Manage Entry Access	Assign entry access rights
☑ Records Management	Record series administration

Effective Rights

To view the current effective feature rights and privileges according to the current assigned and inherited rights.

Feature Rights and Privileges



Selected entry: DOCUMENT MANAGEMENT\DOJ\Judicial Documents

Access Rights

☑ Show inherited rights

Trustee	Inherited From	Scope
USER2	DOCUMENT MANAGEMENT\DOJ	This folder, subfolder
EVERYONE	DOCUMENT MANAGEMENT	This folder, subfolder
USER2	DOCUMENT MANAGEMENT	This folder, subfolder

Right	Allow	Deny
Browse	☑	☐
Read	☑	☐
Write	☐	☑
Append Data	☑	☐
Delete	☑	☐
Delete Shortcuts	☐	☑
Rename	☑	☐
Create Shortcuts	☑	☐
See Annotations	☑	☐

☑ Inherit rights from parent and include with specified rights

Access Rights