

What's New in Security for Laserfiche 8

White Paper

June 2008

Laserfiche®

The information contained in this document represents the current view of Compulink Management Center, Inc on the issues discussed as of the date of publication. Because Compulink must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Compulink, and Compulink cannot guarantee the accuracy of any information presented after the date of publication.

This chapter is for informational purposes only. COMPULINK MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

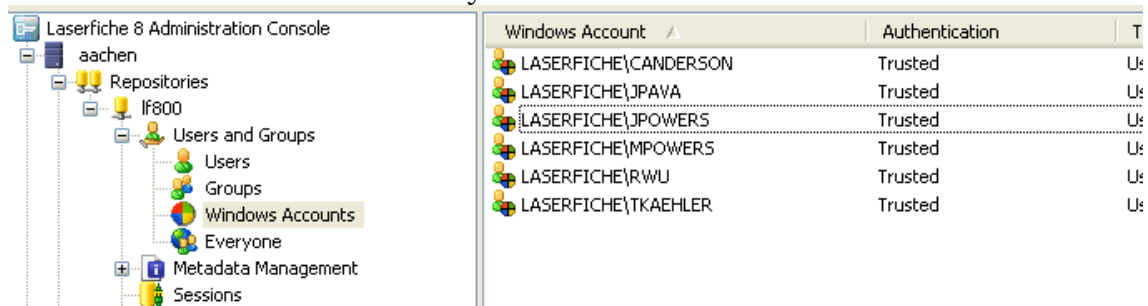
Table of Contents

Windows Accounts	3
Default Security.....	4
Folder Tunneling	5
Entry Ownership.....	5
Template and Field Security	6
Folder Filter Expressions	6
Groups Within Groups	7
New Entry Access Rights	8
New Privileges	8
Purge Entries.....	8
Manage Filter Expressions.....	9
Bypass Browse and Bypass Filter Expressions.....	9
Distributed Metadata Privileges.....	10
Retrieve Audit Data.....	10
System Managers.....	10

Laserfiche 8 introduces several new security features that allow you to manage your security more flexibly. These new features are outlined below. For information on general new features for Laserfiche 8, see [What's New in Laserfiche 8](#).

Windows Accounts

In Laserfiche 8, you can treat domain users and groups like any other user in Laserfiche. Thus, administrators can grant rights directly to these domain users and groups, configure auditing for them, configure trustee attributes, and otherwise treat them exactly the same as Laserfiche trustees.



This ability simplifies user and group administration and maintenance. It is not necessary for an administrator to create new users manually; if a Windows account for a new user has been created on the domain, that user can simply be added to Laserfiche (either individually or as part of a Windows domain group) and administered normally, without needing to tie them to Windows trustees. If a user leaves the organization, the administrator can simply remove their Windows account. Users can also authenticate directly to Laserfiche based on their Windows username. They do not need to remember an additional username and password for the repository – and reducing the number of passwords a user needs to remember also reduces the chances that the user will write the password down to remember it, thus compromising security.

If you add a Windows domain group, you do not need to add users who belong to that group to Laserfiche individually. If the groups to which a user belongs are permitted to log in to Laserfiche, then the user will inherit that ability to log in. Similarly, a Windows domain user's feature rights, access rights, privileges and other security information will be inherited from the group. This allows administrators to take advantage of Windows Accounts without adding each individual Windows account to Laserfiche. Simply adding the relevant Windows domain groups, and then either setting security for those groups on adding them to Laserfiche groups, will allow those users

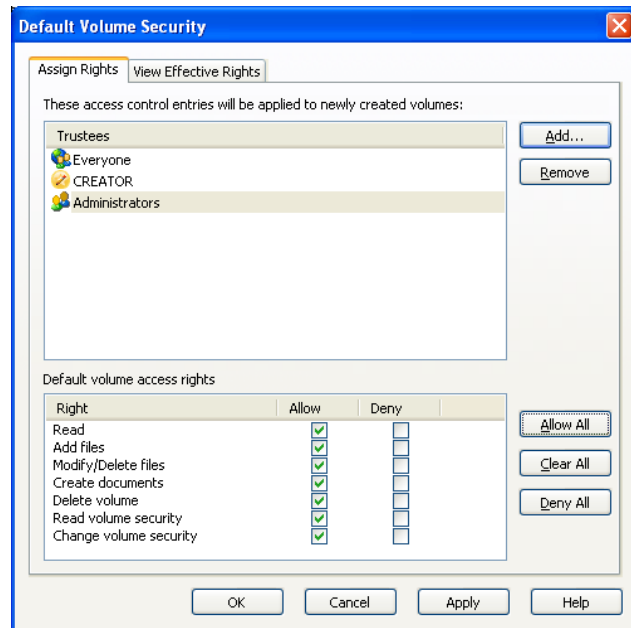
to log in and control their access. This both makes the task of adding users faster and easier for the administrator and falls in line with the Laserfiche best practice of configuring security by group rather than by individual user.

Windows Accounts are useful for any site that takes advantage of Windows domain users and groups to organize its users, and the Windows Accounts features are particularly useful for large organizations, for whom it would be unwieldy or time-consuming to add many users to Laserfiche.

Default Security

Whenever you create a new volume, template or field, Laserfiche creates a starting set of security for that new object. You can customize the starting default security for your volumes, templates and fields. Laserfiche will then automatically apply your default security to all objects of that type that are created after that point. (Default security won't affect volumes, templates or fields that have already been created.) You can configure default security by user, group or Windows account, just like regular security. You can also grant special rights to the object's creator.

For example, by default you might want to grant the Volume right **Read** to all users, the rights **Read, Create documents** and **Append Data** to the Scanner Operators group, and all rights to the user who created the volume (the Creator user) and the Administrators group. Then, whenever you created a new volume, these rights would be the default starting rights for the volume. You could still customize the security for individual volumes – Default security simply allows you to customize the starting security configuration. Any user with the **Manage Templates and Fields** privilege can set default security for templates or fields, and any user with the **Manage Volumes** privilege can set default security for volumes.



Default security makes it unnecessary to modify every new volume, template or field's security to match a general security policy. This saves time for

administrators and users, and also helps ensure that security will be consistent for these objects.

Folder Tunneling

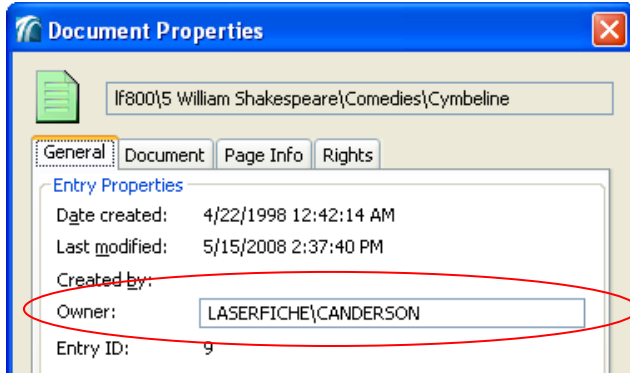
In some cases, you might want to grant users or groups access to folders that are 'buried' beneath folders to which they don't have access. For example, you might want users to be able to access their own personal folder, but not the rest of the department folder in which it resides. You can do this by creating a shortcut to that folder. You will need to place the shortcut in a folder to which the user *does* have sufficient rights, so they can navigate to it. They will also need to have the rights to access the folder to which the shortcut points, but they don't need rights to the folders in between.

For example, you might want to create a folder for Jane Smith's retirement fund information within the Human Resources folder, but only grant Jane Smith the ability to see her own folder, not the Human Resources folder itself. You could restrict Jane Smith from the Human Resources folder but grant her rights to the Jane Smith folder. You could then create a shortcut in another folder to which Jane Smith does have access. Even though she couldn't browse to her folder within the Human Resources folder, she could both search for it and access it by clicking the shortcut within the folder she could see. This configuration is useful because it doesn't necessitate explicitly denying her access to all the other folders within the Human Resources folder, which in turn simplifies the security policy.

This adds great flexibility in setting up repositories. Potentially complicated and time-consuming modifications to the overall security setup of the repository can be avoided in cases where certain users should be granted access to specific pieces of information in an otherwise confidential parent folder.

Entry Ownership

The Entry Ownership feature provides a mechanism by which users can manage their own documents and folders, without needing to call in an administrator or privileged user. An entry's owner can set security for that entry and can manage the entry's annotations. This gives entry owners the ability to configure security for and otherwise manage their documents, without granting them larger-scale rights over the repository. Since entry ownership is set at the time of document creation, it doesn't require you to separately grant additional rights to particular users to allow them to manage



their documents – they will be able to do so wherever they create the documents.

By default, the starting document owner for an entry is its creator. You can assign the starting document owner to another user or group, or you can configure your repository so that documents have no owner when

they are created. Additionally, a user with the **Change Entry Owner** entry access right can reassign entry ownership after document creation.

For example, if documents in your repository are generally created by the users who will be working with them the most, you may wish to keep the default entry owner set to the entry creator. Document creators will be able to easily manage and work with their own documents. However, if you have a handful of scanner operators creating the majority of the repository's documents, you may wish to switch the default document owner to a supervisor user, or to have no default document owner. In that case, an administrator could later grant document ownership to an appropriate user after the document was created.

Template and Field Security

In Laserfiche 8, fields exist in the repository independent of the template to which they belong. Template and field rights have accordingly also been separated. Furthermore, field and template rights can now control the ability to modify template and field definitions – it is no longer necessary to grant a privilege simply to change the ordering of a template or the name of a field. You can grant the ability to modify that field or template definition for a specific field or template, rather than using a privilege, which grants the ability for all fields and templates. For example, you might want to allow the Accounting department to manage the templates relevant to Accounting, and fields within that template – but not to be able to manage templates relevant to Human Resources. These rights will allow you to grant them the ability to manage their own templates only.

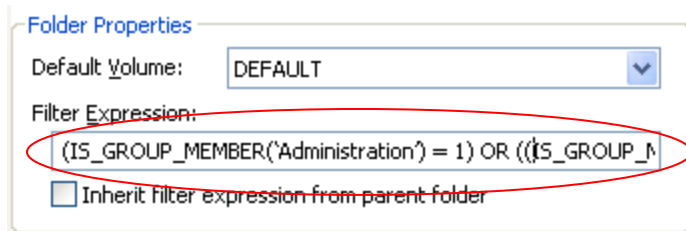
Folder Filter Expressions

Folder filter expressions allow you to determine dynamically which users can see which documents based on criteria you specify. Folder filter expressions

make it possible for administrators to specify conditions that must be met before a trustee can see a particular document. They use a regular expression string which will be interpreted by the Server to control access to entries within the folder.

For example, an administrator could set up a folder filter expression that controlled access to documents depending on the value set in a template field. The administrator might create a list field containing the projects to which a document can belong. He or she could then write a folder filter expression specifying that only users in particular groups can see documents in particular projects. When a document is created or imported, he or she could then set the field to the appropriate project. Users in the group or groups who should have access to the project will then be able to see the document, whereas users who are not in those groups would not have access to the document.

He or she could use a folder filter expression to make these changes – without ever needing to move the document from its folder, and without needing to constantly change the



security on the documents themselves. The folder filter expression would dynamically determine, based on the Status list field, which groups should have access to the documents. When the field is changed, the access would change automatically without additional configuration.

Folder filter expressions are created using an advanced regular expression syntax. This offers a great deal of flexibility for administrators who are willing to learn the syntax. See the Laserfiche *Administration: Reference* or Administration Console help files for syntax information and folder filter examples.

Groups Within Groups

In Laserfiche 8, you can add a group as a "member" of another group. This allows you to represent hierarchical security structures (where some groups are subsets of other groups) using Laserfiche security.

New Entry Access Rights

Laserfiche 8 introduces a new entry access right, **Delete Pages**. This right controls the ability to delete pages from within a document. Without this right, a user will not be able to delete individual pages. (If the user has the Delete Entry right, however, they will still be able to delete the entire document, even if they do not have the **Delete Pages** right; **Delete Pages** only controls attempts to delete specific pages from within the document.) A user must also have the appropriate Volume access rights to delete the pages from a document.

To complement the new Entry Ownership concept, there is also a new entry access right: **Change Ownership**. This right allows you to assign a new default owner to a document in that document's Properties dialog. (Since a document can only have one owner at a time, changing a document's ownership will remove the prior owner and replace them with the new owner.)

Additionally, entry access rights now support the ability to grant or deny rights to a Windows domain user even if that user has not been explicitly added to the Windows Accounts list in Laserfiche. If a user has been granted access to the repository – for instance, by adding a Windows domain group to which the user belongs to the Trusted Windows Accounts list – you can customize the access rights for that user from the same dialog in the Client that you would use to grant access rights to a user.

New Privileges

Laserfiche 8 introduces several new privileges to help you manage your repository more easily. Some privileges allow you to more easily distribute administrative tasks between multiple users, while others enhance performance for the users they have been granted to. In some cases, you may wish to grant some of these new privileges to regular users, rather than restricting them to administrative users.

Purge Entries

Laserfiche 8 includes a new recycle bin feature, which allows administrators and users to review the documents that have been deleted before they are permanently purged from the repository. Administrators with the **Manage Entry Access** privilege can restore and purge any deleted entries, and users with the new **Purge Entries** privilege can purge entries that they have deleted themselves. Granting this privilege allows users to manage their own deleted documents and determine whether they should be permanently removed. If

you would like a user to be able to decide whether a deletion should be permanent, you should give him or her this privilege.

Manage Filter Expressions

The **Manage Filter Expressions** privilege determines who can set filter expressions on folders in the repository. (The user must also have the Write Security entry access right for a folder to set its filter expression.)

Bypass Browse and Bypass Filter Expressions

As security grows more granular and complex, the Laserfiche Server must perform more security checks to determine whether a particular document should be displayed to a user. This does not generally impact performance when browsing a repository, but returning a search results list with many hits may be slower, as the Server must calculate security for each entry, as well as its parent folders and their parent folders up the folder tree, in the search results before they can be displayed. The **Bypass Browse** and **Bypass Filter Expressions** privileges speed up security calculations by allowing the Server to ignore the **Browse** right or the parent folder's filter expression for the user the privileges have been applied to.

Because these privileges ignore the **Browse** right and the folder filter expressions in the repository, they should only be granted if you are not using these security features to restrict access for that user. For instance, if a user has the **Browse** right for the entire repository, you should grant them this privilege in order to improve their performance, since it would not grant them access to any document they wouldn't be able to see anyway. Similarly, if you are not using folder filter expressions in your repository, you should grant the **Bypass Filter Expressions** privilege to the Everyone group, as it would improve performance without affecting access. However, if you do choose to use filter expressions, or if a user should have their **Browse** access restricted, they should not be granted these privileges.

In a new repository, **Bypass Browse** and **Bypass Filter Expressions** are granted to the Everyone group to begin. In a migrated repository, only **Bypass Filter Expressions** is granted to the Everyone group, since the folder filter expression feature was not present in Laserfiche 7 and therefore will not be relevant in a newly migrated repository. If you do want to use **Browse** and filter expressions to restrict access to documents, simply remove these privileges from the Everyone group.

Distributed Metadata Privileges

In Laserfiche 7, the ability to modify metadata types was controlled by a single privilege, **Manage Metadata**. In Laserfiche 8, **Manage Metadata** has been split into several separate privileges: **Manage Templates and Fields**, **Create Templates and Fields**, **Manage Stamps**, **Manage Tags**, and **Manage Links**. This allows you to distribute the ability to modify metadata to exactly the users who need particular rights. It is no longer necessary, for instance, to grant the ability to modify tags (which can be very powerful, in the case of security tags) along with the ability to create or modify a field. Additionally, due to new template and field rights, it is not necessary to grant the **Manage Templates and Fields** right simply to allow a user to modify a particular template or field. They only have to be granted the appropriate rights for that particular field or template.

Retrieve Audit Data

The Laserfiche 8 Audit Reporter logs in as a particular Laserfiche trustee in order to access the audit data on the Laserfiche server. That user must have the **Retrieve Audit Data** privilege in order to pull this information from the binary audit logs and load it into the audit reporter.

System Managers

In Laserfiche 7, system management operations (such as creating repositories, registering and unregistering repositories, performing traces, or monitoring license use) were controlled by a single system management password. To make system management more secure and flexible, Laserfiche 8 now allows you to specify which Windows domain users will be system managers. By default, members of the Local Administrators Windows group on the computer hosting the Laserfiche Server are system managers. You can add or remove additional Windows domain users and Windows domain groups as system managers. Note that system managers are only able to perform certain high-level Server maintenance tasks; setting a domain user as a system manager does not grant that account access to the contents of the repository itself.



What's New in Security for Laserfiche 8

June 2008

Author: Constance Anderson

Technical Editor: Justin Pava

Compulink Management Center, Inc.

Global Headquarters

3545 Long Beach Blvd.

Long Beach, CA 90807

U.S.A

Phone: +1.562.988.1688

www.laserfiche.com

Laserfiche is a trademark of Compulink Management Center, Inc.

Various product and service names references herein may be trademarks of Compulink Management Center, Inc. All other products and service names mentioned may be trademarks of their respective owners.

Copyright © 2008 Compulink Management Center, Inc.

All rights reserved