

# **Laserfiche<sup>®</sup> 7 Security: Notes on Best Practices**

*White Paper*

July 2005

**Laserfiche<sup>®</sup>**

*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

Authentication and Authorization .....	3
Authentication .....	3
Authorization .....	3
Order of Precedence and Inheritance .....	5
Setting Up Security.....	6
Starting Out.....	6
Using Groups .....	7
Entry Access Rights.....	7
Example: Setting Up a Repository.....	8

In considering a document management solution, security is a high priority, particularly if your company stores highly sensitive information. Laserfiche provides a powerful security system, fully compliant with DoD 5015.2, which allows detailed fine-tuning of repository security. Using Laserfiche security, you can control access from a repository-wide scope down to individual documents, grant rights to groups or to individuals, and select from several different ways of implementing your security system. This flexibility allows you to choose the system that provides the best security for you while still being easy to maintain.

This document will describe various aspects of the Laserfiche security system. It will also give ideas on how to set up your Laserfiche security to be as secure and maintainable as possible.

## **Authentication and Authorization**

Security consists primarily of two components: authentication and authorization. Authentication determines that users are who they claim to be. Authorization specifies which software functions and information they have access to. In Laserfiche, user and group accounts link authentication to authorization.

### **Authentication**

Laserfiche authentication uses three different methods. User accounts with a Laserfiche username and password authenticate a specific Laserfiche user. User accounts associated with a Windows account authenticate a Laserfiche user via that user's Windows username. Trusted Windows accounts allow Windows users to access Laserfiche even without their own user account.

Windows authentication allows a single sign-on system, so that users need not keep track of separate accounts and passwords for Windows and Laserfiche. Using Windows authentication for Laserfiche can simplify security setup, delegating some security operations to Windows so that the system administrator need only maintain a single authentication system.

Windows authentication for groups gives administrators an additional tool for easily associating different Windows groups with the appropriate Laserfiche groups. With Windows groups, you can add a single group to the Laserfiche Trusted Accounts list, then associate its subgroups with Laserfiche groups without having to add these to the Trusted Accounts list as well.

### **Authorization**

Laserfiche user accounts control several layers of security. Some types of security, such as Privileges and Feature Rights, determine what actions users may perform on the repository or using the client. Access rights, including Entry Access Rights, Volume Access Rights, and Field Access Rights,

determine a particular user's rights on a particular document, volume, or field. Security tags provide another form of security that is less dependent on the folder hierarchy than access rights.

**Privileges** confer the ability to carry out certain administrative tasks, such as granting rights to other users and groups, and should be granted to trusted users. They are generally not needed by ordinary users of the repository.

Privileges are granted to users or groups through the Administration Console, and apply across the entire repository. Since privileges are not inherited through the file structure, they can only be granted or not granted. This is in contrast to access rights, which apply to specific folders or documents through the client, and which can have three states: allowed, blank (inherited), or denied.

**Feature rights** allow administrators to control access to client functions such as search, import/export, scan, print and text editing. Since feature rights generally do not affect access to information in the repository, they are not as important to document security. Like privileges, feature rights are assigned to users and groups through the Administration Console and apply across the entire repository.

**Entry access rights** control access to documents and folders. These rights are applied through the client, since they are based in specific locations on the folder tree. They have three possible states: allowed, blank (inherited) or denied.

Entry access rights grant users and groups access to specific folders or documents, although they may apply to others through scope. Scope allows access rights on folders to apply to the items inside those folders as well, in a variety of combinations: documents only, folders only, immediate children only. The most common default scope applies as broadly as possible, to the folder on which the rights are granted and to all the subfolders and documents below it in the folder tree.

**Field access rights** can hide a particular field, or prevent users from modifying it. These may be particularly useful for fields which shouldn't be modified, such as identification numbers for specific documents, or for fields that contain sensitive information.

**Volume access rights** control access to the text, images and electronic files that are part of Laserfiche documents. These should be synchronized with entry access rights, so that users do not open documents only to find that they cannot access the images and text inside.

**Tags** act as supplemental markings for documents and folders. Security tags are primarily useful for enforcing different levels of classification. Tagging a document with a security tag ensures that only users who have that tag will be able to view it, so by assigning tags for different levels of security you can sort documents into the appropriate category without having to move them to another location in the folder structure.

Tagging documents with security tags provides a useful addition to access-rights based security. Tags may be applied by any other user who possesses the same tag.

## **Order of Precedence and Inheritance**

Laserfiche has several layers of security. With these interacting levels, it can be difficult to determine what will give a user the correct set of rights. Each type of security has its own set of rules governing what it can override, and what can override it.

0. Special case: A user with the "Manage Entry Access Rights" privilege is allowed the "Browse", "Read", and "Access Control" rights on all entries in the repository.
1. Blank rights will inherit rights from parent folders (unless this option is explicitly turned off).

**Example:** For user Bob, folder A has the right "Rename" denied with scope "This Folder, Subfolders and Documents." Subfolder B has the right "Rename" left blank. The right "Rename" will be denied on subfolder B.

2. Rights specifically assigned to an entry will override inherited rights.

**Example:** For user Bob, folder A has the right "Rename" denied with scope "This Folder, Subfolders and Documents." Subfolder B has the right "Rename" allowed. The right "Rename" will be allowed on subfolder B.

3. In the case of conflicting rights, where a user's rights are different from the rights of the group to which they belong, or when the user is in two different groups, the rights will be applied in the following order:
  - a. **Denied.** Denied rights always take precedence, so that if there is an accidental conflict in rights, documents will be less accessible rather than more accessible.

- b. **Tags.** If a users are unable to see an entry because they have not been assigned all of that entry's tags, they will still be unable to see it regardless of what rights they are allowed on that document.
- c. **Allowed.** Explicitly denied rights, or rights denied by tags, take precedence over explicitly allowed rights.
- d. **Blank.** If a right is left blank, neither allowed nor denied, then by default it is not granted. However, if there is a rights conflict between allowed or denied rights and blank rights, the rights that are specifically allowed or denied will take precedence.

In general, if there is any doubt or conflict in security settings, Laserfiche will choose whatever security configuration is most secure and allows the least access.

## Setting Up Security

Setting up security on your Laserfiche repository can be quite quick and simple or quite long and complex. Obviously, each repository will be different and will have different requirements. Here we have presented some information and ideas about setting up security on your repository.

### Starting Out

When your repository is first installed, it will have a few security items pre-arranged. By default, the repository is arranged for minimum security, so that anyone who isn't interested in learning about security does not have to worry about it. If you do want to make your repository secure, you'll want to change some of the settings.

When newly created, the repository will have one user, Admin, and one group, Everyone. The Admin user has all feature rights and all privileges. The Everyone group, by default, has no feature rights or privileges, but has access rights to all entries in the repository. You should remove these access rights from the Everyone group if you are setting up a secure repository, because all users will be part of the Everyone group. It should have the lowest level of security, so that a newly created user will not have rights until you grant them. Note that all users, including those logged in as trusted Windows accounts, will always be part of the Everyone group.

In creating your repository, it is best to start with a blank slate, with no rights granted. The most all-encompassing group, the Everyone group, and the most all-encompassing folder, the root folder, should have no rights or very limited rights. From this secure base, you should add rights for specific users on specific folders and documents.

## Using Groups

Laserfiche allows security rights to be granted both to individual Laserfiche users and to groups. Granting and maintaining rights for individual users quickly becomes time-consuming and error-prone in large organizations, so you will probably want to set up most of your security using Laserfiche groups. Defining access using groups allows you to make changes for a whole departments or job title categories at the same time, while still permitting you to fine-tune security if necessary by granting or denying rights to a few individual users.

In setting up groups, you can use either Laserfiche groups containing Laserfiche users, or Laserfiche groups connected to Windows groups. Using Windows Authentication for groups can save a great deal of time in setting up repository security by allowing you to make use of your pre-existing Windows user and group accounts, and avoid the hassle of making a Laserfiche user account for each user in your organization.

Group-based security can easily be modified by assigning rights to individual users if it is necessary to do so. If you are assigning rights to users so they can carry out administrative tasks, it is often simpler to assign rights to individual administrators rather than creating a group to contain only one or two people. On the other hand, creating a group for a specific job title, even if only one or two people hold the job at any one time, can simplify changing or adding administrators. Make sure you always have at least one user with administrative rights. This type of setup allows you to change or add administrators simply by adding them to or removing them from the group

Also note that it is possible for a user to be in more than one group at the same time, but this ability should be used carefully, since conflicting rights can make security administration confusing.

## Entry Access Rights

As with users and groups, applying entry access rights at the broadest level possible will simplify security administration. By making use of the default scope, "This Folder, Subfolders and Documents", you can easily grant or deny access to entire sections of your folder tree.

To take advantage of scope, use the folder tree to organize your security, with certain sections of the tree being accessible to certain groups. You can also create structures with restricted rights at higher levels and more permissive rights at lower levels of the folder tree. In general, you will want to set up your tree so that higher levels are more restrictive and lower levels less so; this simplifies the process of keeping the repository secure.

If inherited rights are in conflict, the lowest level always takes precedence: if folder A has one set of allowed and denied rights, and subfolder B located within folder A has a different set of allowed and denied rights, then folders within B will inherit their rights from B and not from A.

**Example: Higher to Lower Security**

Maureen Birnbaum sets up her repository so that her users have full access to the appropriate lower-level folders, but can't make changes to the root folder. For instance, user George only has Browse and Read rights to the root folder. In the folder for his department, one level below, he has rights that allow him to access all files, import and create new documents, add annotations, and otherwise contribute material. In his personal folder one level below that, he has full rights to move, delete, create and modify whatever he wishes.

If you want to change access rights for certain documents and folders without having to reorganize your folder tree, you can use security tags for access control that doesn't use scope. Note that because tags do not have scope, tags on folders do not apply to the contents of the folder. Users will not be able to browse to the folder if they do not have the appropriate security tag, but they will still be able to access its contents by searching unless the contents are also protected in some way.

**Example: Setting Up a Repository**

Consider Charlemagne, who is setting up a new repository for his company, Frank's Document Management. He wants his repository to be secure, and he wants his network administrator, Missy, to be able to maintain it easily. Frank's Document Management has three departments: Engineering, Sales, and Tech Support.

Charlemagne creates a new repository using the repository creation wizard. He logs in using the repository's Admin account and removes the access rights the Everyone group has on the root folder. In the Administration Console, he creates three groups, one for each of his three departments. He grants feature rights to each group as he feels appropriate. He creates a user account for the head of each department with appropriate administrator privileges, and super-admin account for Missy that includes extra privileges that will allow her to administrate all aspects of the repository.

Charlemagne has his departments organized as Windows subgroups, so he adds the top-level windows group to the Windows Accounts list of the repository, then associates each subgroup with the corresponding Laserfiche group so that his employees can log in using Windows Authentication. He also associates his departmental administrators' user accounts with their individual Windows accounts.

Each department has its own types of documents (invoices for Sales, case reports for Tech Support, technical specs for Engineering) so Charlemagne creates a folder under the root for each department. He adds an Access Rights entry for the Sales group on the Invoices folder, with scope "This folder, subfolders and documents" allowing the group basic rights on the folder. This way Sales can access the invoices folder, but Engineering and Tech Support cannot. He repeats the process with folders for the other departments.

With this basic security in place, Charlemagne feels his system is ready for use.

Obviously this example shouldn't be taken as the only right way to create a repository. For instance, Charlemagne could have created Laserfiche user accounts for all of his employees instead of using Windows group authentication. Rather than creating individual user accounts for department heads, he might have created a group called "DepartmentAdmins" and added the department heads to it as Laserfiche users.

This paper presents just a few examples of good ways to set up your repository security. Remember that these are guidelines, not inflexible rules. Every company and every repository is different, and Laserfiche Security's great flexibility allows it to cover a very broad variety of different situations and administrative styles. Use Laserfiche security to create a system that works best for your repository.



Security: Notes on Best Practices  
July 2005

Author: Regina Carns  
Contributing author: Gerren Wang

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](http://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 © 2005 Compulink Management Center, Inc.  
All rights reserved