Introduction to Security in Laserfiche® 8

White Paper

June 2010

Laserfiche®

Table of Contents

The Laserfiche Server provides a powerful set of security options that you can use to ensure that only the right users can access the information you store in your repository. Using Laserfiche security, you can control access on a variety of levels. You can determine what users can log in to your repository, collect them into groups to apply security consistently, and determine what folders, documents and metadata they can see. In addition, Laserfiche gives you the tools you need to quickly apply security even for very large or complicated systems.

Because Laserfiche security has many options and settings, it can seem quite complicated, especially to new users and administrators. This document will break down the various elements of Laserfiche security and help you understand which ones you should use and for what purposes. Once you understand the parts of Laserfiche Security and how they work together, you will be able to easily implement your security policy.

Authentication and Authorization

Laserfiche security has two separate but interrelated aspects: authentication and authorization. Authentication determines that users are who they claim to be; it answers the questions "who is this user?" and "can this user log in?" Authorization determines what elements of the repository the user has access to once he or she has logged in, and what they can do with those elements.

Authentication

When a user wants to enter the repository, they first need to log in. The administrator for the repository must provide them a way to log in. The method they use to log in is their *authentication method*.

There are four ways that a user can authenticate to a Laserfiche repository.

First, the repository owner can set up an open repository by setting the repository's "admin" user to have no password. Any repository in which the "admin" user has no password will allow users to log in without prompting them for authentication details. The users will be logged in as the admin user. (As a corollary, if you do not want to use open authentication, you must set a password for the "admin" user.) Open authentication is only recommended for very small sites that don't want to use Laserfiche security settings at all. It is not recommended for any sites with sensitive data.

Second, a user can log in using a Windows Account. This allows the user to log in simply by selecting the User Windows Account checkbox when they select their repository in the Client. Laserfiche will use their Windows credentials to identify the user and determine whether they should be able to log in. Once the user has logged in, they will have the rights in the repository

that were assigned to that Windows Account or to groups the account belongs to. More information on Windows Accounts can be found in the "Windows Accounts and LDAP" section, below.

Third, a user can log in using a Laserfiche-specific username and password. This will log them in as a particular Laserfiche user, and once they have logged in, they will have the rights in the repository that were assigned to that user or to the groups the user belongs to. More information on Laserfiche users can be found in the "Laserfiche Trustees" section, below.

Finally, a user can log in using an LDAP (Lightweight Directory Access Protocol) account. This allows users to log in using their credentials from directory accounts other than Windows Accounts—for instance, an administrator could use LDAP support to grand their Novell eDirectory users access to a repository. The users would need to type their Novell eDirectory username and password, but would not need to remember a separate username and password. Once logged in, they would have the rights in the repository that were assigned to that LDAP account or the group the account belongs to. More information on LDAP can be found in the "Windows Accounts and LDAP" section, below.

Windows Accounts and LDAP

In order for a Windows Account or LDAP user to log in to the repository using their directory credentials, an administrator with the **Manage Trustees** privilege must grant them Trusted access in the repository. This does not have to be done on a user-by-user basis, however. If a Windows domain or LDAP directory group has been granted Trusted access, its members will automatically inherit trusted access unless they have been specifically denied it. This allows you to quickly grant access to many people to your repository without having to add them all individually. You can further customize your authorization by granting Trusted status to specific users (thus allowing them to log in even if they don't belong to any Trusted groups), or granting Denied status to specific users (thus preventing them from logging in even if they do belong to Trusted groups).

If a user has not been granted Trusted status, and is not inheriting Trusted status from any groups, will not be able to log in.

We strongly recommend using Windows Accounts or LDAP membership to manage authentication to your repository. It simplifies security for users, who do not need to remember an additional username and password. Even more, however, it simplifies configuring and maintaining security for administrators, who only need to configure one set of users and groups. Furthermore, when users join or leave the company, or move from one group to another, the administrator needs only to make those changes on the

Windows domain or LDAP directory and Laserfiche will automatically use the new settings.

Windows accounts can be added to Laserfiche directly in the Windows Accounts node of the Laserfiche Administration Console. Adding LDAP accounts involves one additional step, since you first must register your LDAP server with your repository. Full instructions for adding Windows and LDAP accounts can be found in the Laserfiche Administration Guide help files, in the "Administering Users and Groups" section of the Security chapter.

Example

Malory, the system administrator at Castle Industries, wants to use Windows Accounts to allow access to their repository. Since he has already set up a Employees on his CASTLE Windows domain, he can simply add the CASTLE\Employees group to Laserfiche and grant it Trusted access. The users CASTLE\Gawain, CASTLE\Elaine, CASTLE\Lancelot and so on will automatically be able to log in, because they are members of the Employees group in Windows. If Malory decides that the user Mordred should *not* be able to log in to the repository, despite being a member of CASTLE\Employees, he can add CASTLE\Mordred to the repository but set that user's status to Denied.

When a new employee, Percival, joins the company, Malory only needs to create a Windows user for him and add that user to the Windows group Employees. After that, Percival will automatically be able to log into Laserfiche, without any additional configuration. And when Lancelot leaves Castle Industries, Malory can remove his access to Laserfiche simply by disabling his account on the Windows domain.

Laserfiche Trustees

In order for a user to log in as a Laserfiche trustee, an administrator with the **Manage Trustees** privilege must create a Laserfiche username and temporary password for them. They can then use the username and password associated with that trustee to access the repository.

An administrator can associate a Windows user name with a Laserfiche trustee, allowing that Laserfiche trustee to log in with their Windows credentials. While this allows the user to skip the step of inputting a username and password, it does not take advantage of the other benefits of using Windows accounts. Full instructions for managing Laserfiche trustees can be found in the Laserfiche Administration Guide help files, in the "Administering Users and Groups" section of the Security chapter.

Group Membership

Windows Accounts, LDAP trustees, and Laserfiche users all support collecting users into groups. A Laserfiche trustee group is created in

Laserfiche, and can be made up of Laserfiche users, other Laserfiche groups, and Windows Account users or groups. Windows Account or LDAP groups must be created and populated in Windows or in your LDAP management system, but then can be added directly to Laserfiche.

When calculating whether a user should be able to perform a particular task, Laserfiche will take into account both the security settings applied to the user and the security settings applied to a group. If a user has been denied the ability to perform a function or access a document—whether that deny was set directly on the user, or was inherited from a group—they will not be able to perform that task, even if they have also been allowed it in another setting. In other words, deny trumps allow.

Authorization

In order to allow you to customize your security settings for your particular repository and security policy, Laserfiche offers granular security with many security types and settings. This gives you a great deal of flexibility when setting up security, but can be complicated at first glance. This section will go over each type of security available in Laserfiche 8 and will explain what it controls and when you should use it.

For more information about authorization and permissions in Laserfiche, see the "Securing Your Documents" section of the Security chapter in the Laserfiche Administration Guide help files.

Granting Permissions to Users

In order to authorize a user to perform a particular task or make a particular set of modifications to something in the repository, you will grant those users rights. This does not need to be done (and in most cases, should not be done) on individual users, however. Rights granted (or denied) to a group will be inherited by the members of that group.

For information about what settings take precedence when more than one conflicting right has been granted, see "Precedence, Inheritance, and Scope," below.

Feature Rights

Feature rights control what functions are available in the various Laserfiche applications: whether a user can scan, for example, or whether they can search, or import or export a file. Feature rights determine what menu commands or toolbar buttons are available to a particular user in client applications. Feature rights apply to the entire repository: even if a user has the appropriate entry access rights to scan into a folder, if they do not have the **Scan** feature right, they will not be able to scan because the Scan button and menu command will not be available.

If a user should be able to perform a particular action anywhere in the repository, they should be granted the feature right that controls that action. For example, if a user needs to be able to print documents from their personal folder, they must have the **Print** feature right, even if they should not be able to print from any other folder. However, if a user should never be able to perform a particular action, they should not be granted the relevant feature right. If a user should not be able to export documents from anywhere in the repository, you should not grant them the **Export** feature right – this will make it clear to them in the user interface that they cannot export.

Feature rights are applied in the Administration Console, and are applied directly to users or groups (whether they are Laserfiche trustees or Windows/LDAP accounts).

Access Rights

Access rights control what a user can do with various objects in the repository. Unlike feature rights, which apply to the entire repository, access rights are specific to a particular part of the repository. There are four types of access rights, to control access to different parts of the repository: entry access rights, volume access rights, field access rights, and template access rights.

Access rights have three possible states: allowed, blank (inherited) or denied. For more information on these settings, and the way they interact, see "Precedence, Inheritance and Scope," below.

Entry Access Rights

Entry access rights control whether a user has access to documents, folders and shortcuts in the repository. These rights are applied through the Laserfiche Client or Web Access, since they are based in specific locations in the folder tree. There are a variety of entry access rights available, that control whether a user can perform actions from opening and viewing to modifying and deleting a particular entry or set of entries. Entry access rights allow you to control what users and groups can do with entries in the repository on a folder-by-folder basis.

When you configure entry access rights, you need to specify three things: what user or group you're configuring entry access rights for (the trustees), what section of the folder tree the rights should apply to (the scope), and what permissions you want to grant or deny (the rights themselves).

Volume Access Rights

Volume access rights control access to the parts of the document that are contained within the repository's volumes: image pages, text pages, and electronic document files, as well as thumbnails, word location data, and attachment annotations. If a user has the appropriate rights to open a

document, but not to view the pages in the document's volume, the document will open but only the metadata will be visible. Similarly, you could restrict a user's ability to add files to all volumes except their department's volume, to ensure that all documents belonging to a particular department end up in that department's volumes. It is therefore important to think of the volume access rights in addition to the entry access rights when determining who should have be able to view or modify documents.

Volume access rights are applied to volumes in the Administration Console.

Field Access Rights

Field access rights determine which users can view or modify fields that have been applied to a document – or modify or delete field definitions from the repository. If a user does not have the rights to view a field, they will not see that field if they open a document that contains that field, even if they can see the other fields applied to the document. For example, you might restrict the users who are able to view an employee's Social Security number. Similarly, if a user should not be able to change a particular field – for example, the filing date of a document – you could restrict the user's ability to modify that field, but still allow them to view it.

Field access rights are applied to fields in the Administration Console.

Template Access Rights

Template access rights determine which users can view entire templates. If a user does not have the rights to view a template, they will not be able to see the fields in that template if the template has been applied to a document – even if they have the rights to see all of the individual fields in the template. In addition, template access rights control who can modify the template's definition.

Template access rights are applied to templates in the Administration Console.

Security Tags

Security tags are security settings that apply to only the entry they were applied to. They are applied to entries and granted to users or groups; only the users who have been granted a particular security tag can see the documents that have had that tag applied to them. Security tags are the most restrictive form of security in a repository: no matter what other rights and privileges are in effect, a document that has been tagged with a security tag can only be seen by users who have that tag. Security tags are useful for documents whose access should remain restricted no matter where they are in the repository—for instance, for documents that are confidential but that may

pass through a number of folders with varying security settings based on your workflow.

Security tags are granted to users in the Administration Console, and to documents in the Client or Web Access.

Privileges

Privileges are a special form of security: they 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. Privileges may also allow users to bypass other forms of security: for instance, a user with the **Manage Entry Access** privilege can browse all entries in the repository, regardless of the entry access rights applied to those entries.

Privileges are granted to users or groups through the Administration Console, and apply across the entire repository.

Folder Filter Expressions

Folder filter expressions are a form of dynamic security that allow you to configure access to documents based on the properties of the individual documents. For instance, you could write a folder filter expression that would determine which groups could see a document based on the value in the document's fields. Folder filter expressions require writing a filter expression string, and are therefore considered advanced security; see the Administration Console help files for more information.

Precedence, Inheritance and Scope

Laserfiche has several layers of security, which can, in turn, be applied to individual users or to groups. 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, as well as what part of the repository the right applies to. This section will explain how these rights interact, and how to tell what part of a repository the right applies to.

Order of Precedence

In some cases, more than one security setting may apply to a particular document or user. For example, a particular document may inherit security from both its parent folder and its parent folder's parent folder, or a user may inherit different security settings from more than one group. The following order of precedence will help you determine which rights will apply in these circumstances.

0. Special cases: A user with the **Manage Entry Access Rights** privilege is allowed the **Browse**, **Read**, and **Access Control** rights on all entries in the repository. A user with the **Bypass Browse** privilege is allowed the **Browse** right on all entries in the repository. If a document has been tagged with a security tag, it will only be visible to those users who have been granted that tag, regardless of the other rights that it might inherit. (Note that a tag does not override entry access rights: a user must have both the appropriate entry access rights and the appropriate tag to open and view the contents of a tagged document.)

1. 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.

2. An access right that has not been explicitly set – in other words, a 'blank' right – will inherit rights from parent folders (unless this option is explicitly turned off).

   Example: For user Bob, folder A has the right **Rename** allowed with scope **This Folder, Subfolders and Documents**. Subfolder B has the right **Rename** left blank. 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 a conflict in rights, documents will be more secure rather than more accessible.
   b. **Tags.** If 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.

4. If a right has not been explicitly set, and is not explicitly set anywhere else (either higher in the folder tree or in another group setting), the user will not have that right.

> **Example:** For user Bob, the **Delete** right was not set on folder C. The Delete right was not set for Bob in folder' C's the parent folders A or B, or the repository's root folder. It was also not set for these folders for any group that Bob belongs to. Bob, therefore, does not have the **Delete** right, and will not be able to delete in that folder.

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

Scope

While entry access security is set directly on entries, it does not necessarily affect only the entries that it was set on. When you apply access rights to a folder, you can determine how far down the folder tree below the folder your rights will apply.

For example, you might have a Human Resources folder, containing subfolders for each employee. The Human Resources director should be able to see and open documents in all folders in the folder, but individual employees should only be able to see and open the main folder and their own personal folder. You could use scope to set up security in this fashion in the following manner.

First, you would grant the **Read** entry access right to the Human Resources manager on the main Human Resources folder, and then set the scope for that user to **This folder, subfolders and documents**. That **Read** right would then inherit to all of the documents, subfolder, subfolder's documents, and subfolders in those subfolders, all the way to the bottom of the Human Resources folder – appropriate, for the manager. However, individual users should not have such powerful rights. Instead, the Everyone group should have the Browse right set on the Human Resources folder with the **This Entry Only** scope, allowing them to open just that folder but not view or open its contents. Then, each user should be granted the **Read** right for his or her own folder, with the **This folder, subfolders and documents** scope for that folder only. Thus, each employee would be able to open the Human Resources folder, but under that folder they would be able to see, open, and read contents for their personal folder only.

Laserfiche®

Introduction to Security in Laserfiche 8
June 2010

Author: Constance Anderson
Technical Editor: Justin Pava

Description:
Because Laserfiche security has many options and settings, it can seem quite complicated, especially to new users and administrators. This document will break down the various elements of Laserfiche security and help you understand which ones you should use and for what purposes. Once you understand the parts of Laserfiche Security and how they work together, you will be able to easily implement your security policy.

Laserfiche
3545 Long Beach Blvd.
Long Beach, CA 90807
U.S.A

Phone: +1.562.988.1688
www.laserfiche.com