Introduction to Security in Laserfiche 8.3 and later

White Paper

November 2013

Laserfiche®

Table of Contents

Introduction

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

Because Laserfiche security has many options and settings, it can seem complicated, especially to new users and administrators. This white paper breaks down the various elements of Laserfiche security and helps 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 can easily implement your security policy.

Authentication and Authorization

Laserfiche security has two separate but interrelated aspects: authentication and authorization. Authentication determines 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 can access after logging in and what he or she can do with those elements.

Authentication

When a user wants to access documents in a repository, they first need to log in. The repository administrator must configure an authentication method that will let users log in.

There are four methods by which a user can authenticate to a Laserfiche repository.

- The repository administrator can set up an open repository. In an open repository, all users are automatically logged in as the admin user and they are never prompted for a password. We only recommend this method for very small sites that do not want to use any Laserfiche security. If your repository has sensitive data, you should choose a different method. To create an open repository, configure the repository's "admin" user to have no password. (As a corollary, if you do not want to use open authentication, you must set a password for the "admin" user.)
- A user can log in with his or her Windows Account by selecting the **Use Windows Authentication** checkbox when they select a repository in a Laserfiche client application. The user's Windows credentials serve to identify the user and determine if they can log in. Once the user has logged in, the user has the rights assigned to that Windows Account and also inherits rights from the group the account belongs to. More information on Windows Accounts can be found in the Windows Accounts and LDAP section, below.
- A user can log in using a Laserfiche-specific user name and password. The user has the rights assigned to the Laserfiche user he or she logged in as and to the groups the Laserfiche user belongs to. More information on Laserfiche users can be found in the Laserfiche Trustees section, below.
- A user can log in using an LDAP (Lightweight Directory Access Protocol) account. For instance, an administrator could use LDAP support to grant their Novell eDirectory users' access to a repository. The users can log in with their Novell eDirectory username and password, and they have the rights in the repository assigned to that LDAP account and 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

For a Windows Account or LDAP user to log in using their directory credentials, an administrator with the Manage Trustees privilege must grant them Trusted access to the repository. An administrator can grant access individually, or he can grant a Windows domain or LDAP directory group Trusted access. If a group is granted access, its members will automatically inherit the access unless they have been specifically denied it. You can further customize your authorization by granting Trusted access to specific users (allowing them to log in regardless of whether belong to any Trusted groups), or granting Denied status to specific users (preventing them from logging in even if they do belong to Trusted groups).

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 a Laserfiche user name and password in addition to their Windows or LDAP user name and password. Additionally, it simplifies configuring and maintaining security for administrators, who only need to configure one set of users and groups. When users join or leave the company, or move from one group to another, the administrator only needs to make those changes to 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. For full instructions on adding Windows and LDAP accounts, see Administering Users and Groups in the Laserfiche Administration Guide.

Example: Malory, the system administrator at Castle Industries, wants to use Windows Accounts to give employees access to the repository. Since he already has an Employees group in his CASTLE Windows domain, he can simply add the CASTLE\Employees group to Laserfiche and grant it Trusted access. Employees Gawain, Elaine, Mordred, and Lancelot can now automatically log into the repository, 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 his user status to Denied.

When a new employee, Percival, joins the company, Malory only needs to create a Windows account for him and add his user account to the Windows group Employees. After that, Percival can automatically log into Laserfiche. When Lancelot leaves Castle Industries, Malory can remove his access to Laserfiche simply by disabling his account on the Windows domain.

Laserfiche Trustees

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.

An administrator can associate a Windows user name with a Laserfiche trustee, allowing that Laserfiche trustee to log in with their Windows credentials. However, merely associating a Windows user with a Laserfiche trustee does not take advantage of the other benefits of using Windows accounts as described above.

Full instructions for managing Laserfiche trustees can be found in the Administering Users and Groups section of the Laserfiche Administration Guide.

Group Membership

Windows Accounts, LDAP, and Laserfiche trustees all support collecting users into groups.

- Windows Account or LDAP groups are created and populated in Windows or in your LDAP management system and can be added directly to Laserfiche.
- Laserfiche trustee groups are created in Laserfiche and can contain Laserfiche users, other Laserfiche groups, and Windows Account or LDAP users or groups.

When determining if a user can perform a particular task, Laserfiche takes into account both the security settings applied to the user and the security

settings applied to a group. If a user is denied access a document—whether the Deny status is set at the user level or inherited from a group—the user cannot perform that task, even if they are allowed permission elsewhere. In other words, deny trumps allow.

Authorization

To let you fully customize security settings to meet your needs, Laserfiche offers granular security with many security types and settings. This security model gives you a great deal of flexibility and precision when setting up security, but can be complicated at first glance. This section discusses each type of security available in Laserfiche and when you should use it.

For more information about authorization and permissions in Laserfiche, see the Securing Your Documents section of the Laserfiche Administration Console online help files.

Granting Rights to Users

Rights allow users to perform tasks or make changes in the repository. You do not need to grant rights to individual users (although you can), as rights granted to groups are 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 let users perform actions in Laserfiche applications. For example, feature rights determine if a user can scan, search, import, or export a file anywhere in the repository. Feature rights also determine what menu commands or toolbar buttons are available to a user. These rights apply to the entire repository. For example, users may have sufficient entry access rights to scan into a folder. But, if the users 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 needs to perform a particular action anywhere in the repository, they should be granted the feature right for that action. For example, if a user needs 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 perform a particular action, they should not be granted the relevant feature right.

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: 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 determine which users can access particular documents, folders and shortcuts in the repository and what a user can do with those entries. These rights are applied in the Laserfiche Client or Web Access, since they are based on specific locations in the folder tree. Each entry access right lets a user perform different actions from opening to deleting an entry or set of entries. These rights can be assigned to users 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 apply to (the scope), and what permissions you want to grant or deny (the rights themselves).

Volume Access Rights

Volume access rights determine which users can access the parts of documents contained in the repository's volumes: Image pages, text pages, electronic document files, thumbnails, word location data, and attachment annotations. If a user has the entry access rights to open a document, but not the volume access right to view the pages in the document's volume, the document will open but only the metadata will be visible. You can use volume access rights only let users add files to their own department's volume and not to any other volume. This configuration ensures that all documents that belong to a particular department end up in that department's volumes. It is important to consider volume access rights in addition to entry access rights when determining who can 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 applied to a document and if they can 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 who can view the Social Security number field. Similarly, if a user should not be able to change a particular field – for example, the filing date of a document –

you can 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 templates. If a user does not have the rights to view a template, the user cannot see the fields in that template – even if the user has the rights to see all 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 let you apply security to individual entries. These tags are applied to entries and granted to users or groups; only the users who have been granted a particular security tag can see the tagged documents. Security tags are the most restrictive form of security in a repository: no matter what other rights and privileges are in effect, a document 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, documents that are confidential but may pass through a number of folders with varying security settings as they are processed.

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 let users perform certain administrative tasks, such as granting rights to other users and groups. Privileges should only be given to trusted users as some privileges let users bypass other forms of security. For example, 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 let you configure access to documents based on the properties of the individual documents. For instance, you could write a folder filter expression that would control access to documents based on a specific value in the documents' fields. To create a folder filter expression, you must write a filter expression string—making this

an advanced security feature. See Folder Filter Expressions in the Laserfiche Administration Guide for more information.

VERS Classification Levels

VERS classification levels provide a way for an organization to ensure that documents remain in folders of a similar or higher level of confidentiality. In most Laserfiche scenarios, and according to Laserfiche best practices, most documents will inherit entry access rights from their folders. This security system provides many benefits in terms of consistency and convenience but can cause problems if documents are inadvertently moved to folders with less-restrictive security settings. Classification levels act as an extra check, preventing entries from being moved such that they inherit less-restrictive security than is appropriate.

Classification levels allow you to set a numeric level on documents and folders. Entries given higher classification levels are more restricted than documents with lower values. If you give an entry a classification level, it cannot be moved to a folder that has a lower numeric level. Unclassified entries have a value of zero.

Example: You have three classification levels: "Top Secret" (numeric value 10), "Classified" (numeric value 7), and "Standard" (numeric value 3). If a document is given "Top Secret" classification, it can be moved to any of the "Top Secret" classification level folders, but it cannot be moved to any of the "Classified" or "Standard" level folders or to any folders without classification levels set.

Example: If a document is given classification level "Classified," it can be moved to a "Classified" or "Top Secret" folder but not to a "Standard" folder or to folders without classification levels set.

See VERS Classification Levels in the Laserfiche User Guide for more information.

Precedence, Inheritance, and Scope

Laserfiche has several layers of security, which can be applied to individual users or to groups. With these interacting layers, it can be difficult to determine if a user has 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 explains how these rights interact and how to tell what part of a repository rights apply to.

Order of Precedence

In some cases, more than one security setting may apply to a document or user. For example, a 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 apply in these circumstances.

0. **Special cases**:
    - A user with the Manage Entry Access Rights privilege has Browse, Read, and Write Entry Security entry access rights for all entries in the repository.
    - A user with the Bypass Browse privilege can browse all entries in the repository, even if they do not have the Browse entry access right.
    - A user with the Bypass Filter Expression privilege will not have their access to entries restricted by folder filter expressions.
    - If a document is tagged with a security tag, it is only visible to those users who have that tag, regardless of the other rights it might inherit.

      Note: Security tags do 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: Bob has the Rename entry access right denied with scope This Folder, Subfolders and Documents for folder A. But he has the Rename entry access right allowed for subfolder B. Bob will be able to rename subfolder B.

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

> **Example:** Bob has the Rename entry access right allowed with scope This Folder, Subfolders and Documents for folder A. Bob neither is allowed or denied the Rename entry access right for subfolder B – the right is left blank. Bob will be able to rename subfolder B.

3. When a user has different rights than the group to which he or she belongs, 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. If rights conflict, entries become more secure rather than more accessible.
    b. **Allowed.** Explicitly denied rights, or rights denied by security tags, take precedence over explicitly allowed rights.
    c. **Blank.** If a right is left blank (neither allowed nor denied), by default, it is effectively denied. However, if allowed or denied rights conflict with blank rights, the rights that are specifically allowed or denied take precedence.
4. If a right is not explicitly set for a user and is not explicitly set anywhere else (either higher in the folder tree or in a group), the user will not have that right.

> **Example:** Bob does not explicitly have the Delete right for folder B. Bob also does not have the Delete right for folder B's parent folder or the repository's root folder. None of the groups Bob belongs to have the Delete right for folder B or its parent folder. Bob, therefore, cannot delete entries in folder B.

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

Scope

While entry access rights are set directly on entries, they do not necessarily affect only the entries they are set on. When you apply entry access rights to a folder, you can determine how far down the folder tree the rights will apply.

> **Example**: A Human Resources folder contains subfolders for each employee. The Human Resources director needs to see and open documents in all employee folders, but individual employees should only see and open the main folder and their own personal folder. You can use scope to set up security for this scenario the following manner:
>
> Grant the Read entry access right to the Human Resources manager for the main Human Resources folder and set the scope for this right to This folder, subfolders and documents. The manager's

Read right then applies to all of the documents, subfolders, subfolders' documents, and subfolders in those subfolders, all the way to the bottom of the Human Resources folder. Since employees should not have such powerful rights, grant the Everyone group the Browse entry access right for the Human Resources folder with the This Entry Only scope. This configuration lets employees only open the Human Resources folder but not view or open its contents. Additionally, grant each employee the Read entry access right for his or her own folder with the This folder, subfolders and documents scope. Now employees can open the Human Resources folder, but, under that folder, they can only see, open, and read the contents of their own personal folders.

For more information see the Scope in Laserfiche Security white paper.

Laserfiche®

Introduction to Security in Laserfiche 8.3 and later
November, 2013

Author: Constance Anderson
Editor: Sarah Seene, Sierra Jahoda
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