Laserfiche Advanced Security Training Manual

November 2010

Laserfiche Certified Professional Program. Not For Distribution or Resale.

Laserfiche®

Table of Contents

1.0 Introduction 4
1.1 Takeaways 4
2.0 Advanced Security Concepts 5
2.1 Designate Accounts as Read-Only 5
2.2 Privileges 5
2.3 Security Tags 6
2.4 Entry Ownership 7
2.5 Folders 8
2.6 System Managers 9
2.7 Encrypted Volumes 9
2.8 Exporting Briefcases 10
3.0 Annotations 11
3.1 Protected Annotations 11
3.2 Redactions 11
4.0 Troubleshooting 12
4.1 Basic Steps to Indentify/Solve a Security Problem 12
4.2 "I Can't Access Something" (Admin Login to Test) 12
4.3 Inheritance 13
4.4 Incorrect Use of Explicit Deny 14
4.5 Security Tags 15
4.6 Folder Filter Expressions 15
4.7 Access Rights 15
4.8 Privileges 16
4.9 Feature Rights 17
4.10 Windows Security 17
5.0 Best Practices 19
5.1 Entry Access Rights 19
5.2 Template and Field Security 19
5.3 Default Security 19
5.4 Using Groups 20
5.5 Domain Accounts 21

Laserfiche Certified Professional Program. Not For Distribution or Resale.

6.0 Security Outside of Laserfiche 22
6.1 Windows Operating System 22
6.2 DBMS 22
6.3 File Server 23
6.4 Web Server 23
7.0 Scenarios 25
7.1 Regulated Organization 25
7.2 Large Organization 25

Laserfiche Certified Professional Program. Not For Distribution or Resale

1.0 Introduction

In this course you will learn advanced methods for Laserfiche security configuration to address unique needs. We will also highlight best practices and address network security considerations that relate to Laserfiche.

> **Note:** This course builds on the security information and concepts reviewed in the Laserfiche Administrator I certification and is recommended for individuals who do, or are interested in, extensive configuration and maintenance of Laserfiche security.

This manual covers the following areas of Laserfiche Security:

- **Advanced Security Concepts:** Secondary, non-standard security features and concepts for specialized environments or implementations, and to further secure already secured Laserfiche systems.
- **Troubleshooting:** Common troubleshooting problems and suggestions for solving them to help keep your Laserfiche Security running smoothly.
- **Best Practices:** Best practices for setting up, using, and maintaining your Laserfiche Security.
- **Security Outside of Laserfiche:** Discussion of issues related to securing Windows, database, file server, Web server, and SSL.
- **Scenarios:** Two typical, real world examples of different-size customers, their security challenges, and how they met these challenges with Laserfiche security.

1.1 Takeaways

This guide 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.

Laserfiche Certified Professional Program - Not For Distribution or Resale.

2.0 Advanced Security Concepts

2.1 Designate Accounts as Read-Only

With Laserfiche 8, the Administration Console allows administrators to specify which users should be restricted from making changes to the repository by toggling a read-only setting in a user or group's properties. Setting groups as read-only immediately sets security such that its users are unable to move, modify, or delete documents. Of course, that is only one feature of security, as restricting sensitive information is equally important.

2.2 Privileges

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 privileges to regular users, rather than restricting them to administrative users. Be aware, however, that some privileges give additional rights within the Laserfiche repository and may supersede access rights.

2.2.1 Purge Entries

Administrators with the **Manage Entry Access** privilege can restore and purge any deleted entries, and users with the **Purge Entries** privilege can purge entries that they have deleted themselves. Granting this privilege allows users to manage their own deleted documents and determine if they should be permanently removed. If you want a user to be able to decide if a deletion should be permanent, give the user the **Purge Entries** privilege.

2.2.2 Manage Filter Expressions

The **Manage Filter Expressions** privilege determines who can set Folder 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.) For more information, see Section 2.5.2, Folder Filter Expressions.

2.2.3 Bypass Browse and Bypass Filter Expressions

As security grows more granular and complex, the Laserfiche Server must perform more security checks to determine if 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 in the search results, as well as its parent folders and their parent folders up the folder tree, before they can be displayed. The **Bypass Browse** and **Bypass Filter Expressions** privileges speed security calculations by allowing the Server to ignore the **Browse** right or the parent folder's filter expression for the user that the privileges have been applied to.

Laserfiche Certified Professional Program. Not For Distribution or Resale.

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 security features to restrict access for that user. For instance, if a user has the **Manage Entry Access** privilege for the repository, you should grant them the **Bypass Browse** 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.

> **Example:** Any user with the Manage Entry Access privilege can already browse the entire repository, therefore it's a good idea to give these users the Bypass Browse privilege so as not to slow down their system performance with unnecessary additional checks.

2.2.4 Distributed Metadata Privileges

Metadata management is 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. Additionally, due to 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.

2.3 Security Tags

Tags are a type of metadata that contain special handling and categorization instructions relating to documents and folders in a Laserfiche repository. You can apply more than one tag to a document to categorize or secure it multiple ways.

Documents with security tags can only be seen or accessed by users that have been assigned all of the security tags assigned to the document. Users not assigned a tag associated with a document will be unable to see the existence of that document, regardless of what other rights or privileges the user might have. For example, if a document is assigned two security tags, a user who is assigned only one of the security tags will be unable to access it.

Tags give you more flexibility in categorizing or securing documents. Since security tags are independent from the folder structure, you can use them to restrict access to specific documents without having to independently configure entry access rights for the document or move the document into another folder.

> **Note:** In addition to security tags, a user will still need the appropriate feature and access rights to view or work with a document or folder that has been secured using security tags. Tags do not grant additional

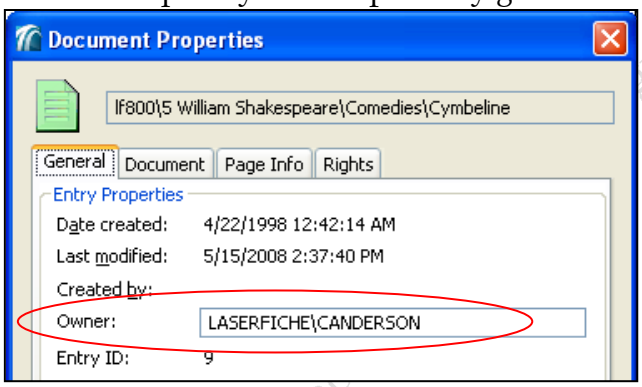
Laserfiche Certified Professional Program. Not For Distribution or Resale.

access to a document, they merely restrict who can access it. Entry Access Rights still determine what a user who has a tag can do with the document.

Creating, modifying, or deleting an informational or security tag, or assigning a security tag to a user account, requires the Manage Tags privilege. To apply a security tag to a document, a user must have been assigned that security tag and must have the Write Metadata access right on the document in question. Assigning a security tag to a user also allows him or her to work with documents that have been associated with the security tag in question, provided that the user or group has been granted sufficient entry, volume, and field access rights.

2.4 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.

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.

Laserfiche Certified Training Program. Not for Distribution or Resale.

2.5 Folders

2.5.1 Folder Tunneling

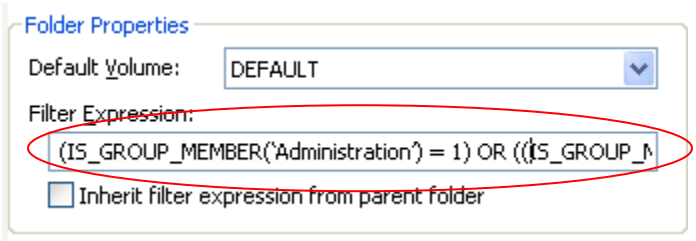
In some cases, you might want to grant users or groups access to folders that are "buried" beneath folders to which they don't have access. For example, you might want users to be able to access their own personal folder, but not the rest of the department folder in which it resides. You can do this 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.

> **Example:** You 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 in the Human Resources folder, she could both search for it and access it by clicking the shortcut within the folder she can see.

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.

2.5.2 Folder Filter Expressions

Folder filter expressions allow you to determine dynamically which users can see which documents based on criteria like group membership and field values. Folder filter expressions make it possible for administrators to specify conditions that must be met before a trustee can see a particular document.



For example, an administrator could set up a folder filter expression that controlled access to documents depending on the value set in a field. The administrator might create a list field containing the projects to which a document can belong, and 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, the scanner operator can set the field to the appropriate project. Users in the group or

Laserfiche Certified Professional Program Course Material. Distribution or Resale.

groups who should have access to the project will be able to see the document, whereas users who are not in those groups would not have access to the document.

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 Console help files for syntax information and folder filter examples.

2.6 System Managers

System management operations, such as creating repositories, registering and unregistering repositories, performing traces, or monitoring license use, are specific Windows domain users. 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:** 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.

2.7 Encrypted Volumes

Encrypting a volume protects the files in that volume in the Windows file system, using an encryption password to determine what users and applications should be able to access those files. Each of the files in the volume (image pages, text pages, and so on) will be encrypted; if they are opened from Windows, their contents will be unreadable or unavailable.

When a volume is first encrypted, it will be in an encrypted but accessible state. This means the files are encrypted on the Windows file system, but the Laserfiche Server has the encryption key. If a volume is encrypted but accessible, users can view files in the Client and other client applications normally (assuming they have the appropriate Laserfiche permissions to do so), but the files cannot be viewed directly through Windows. If a volume is encrypted but secured, however, it will be inaccessible both to users viewing documents through the Client and through the Windows file system.

A volume can be secured in two ways. When the Laserfiche Server is started, all volumes that were encrypted at the time the Server stopped will be loaded in a secured state. You will need to unlock these secured volumes to make them accessible. You can also secure a volume manually in the Administration Console.

> **Note:** Logical volumes cannot be encrypted or secured. Individual physical volumes within logical volumes, however, can be encrypted and secured.

Laserfiche Certified Professional Program. Not For Distribution or Resale.

Be aware that when a volume is secured, its contents are not accessible to anyone until it is made accessible again. Users opening a document stored in that volume will not be able to see the document's pages, text, or electronic files; instead, they will receive a message indicating that the document's volume is secured and therefore unavailable. Securing a volume is most useful for archival volumes that do not need to be available for routine repository access and for transferring volumes between Laserfiche systems.

> **Important:** Do not lose the password for a secured volume. Without the password, it cannot be unlocked, and there is no way to retrieve a lost password.

Volumes can also be encrypted when they are exported or detached. In this case, the volume's encryption password will be necessary when you want to attach that volume to a repository. Once the password has been provided, the volume will be attached in an encrypted but accessible state.

> **Important:** Encrypted or secured volumes can only be attached to repositories on Laserfiche Server 8.1 or higher. Previous versions of Laserfiche did not support encrypted or secured volumes.
>
> **Note:** In Laserfiche 8.1, encrypted volumes needed to be read only before they could be encrypted. As of 8.2, live volumes can also be encrypted.

2.8 Exporting Briefcases

Briefcases are designed to move content—folders and documents, including metadata and annotations—between repositories. There are a couple of security concerns to be aware of should sensitive information need to be transported with a briefcase. To begin with, Entry Access Rights (folder security) are not included in the briefcase. Instead, an imported briefcase will inherit security from wherever it is imported into a repository. One Entry Access Right to be particularly aware of in this situation is See Through Redactions, as this right also will be determined based on where the briefcase is imported. Therefore it is recommended that if sensitive information is being transported, you use the option to permanently burn redactions into the image. Of course, a user who cannot see through redactions can only export with the redactions permanently burned into the image.

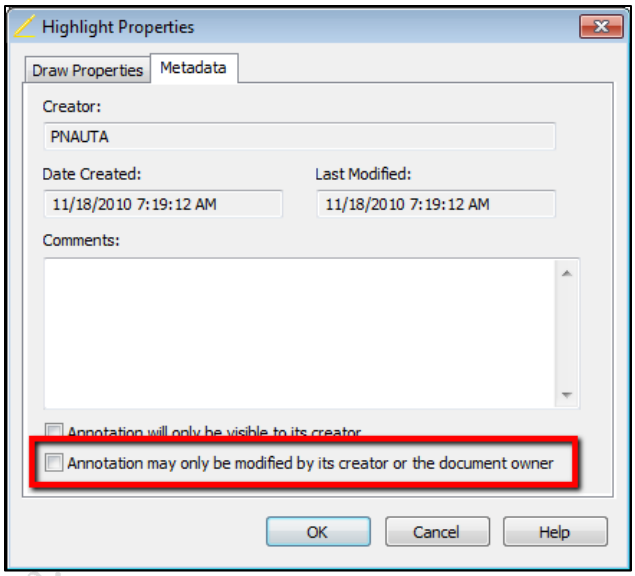
Laserfiche Certified Professional Program. Not for Distribution or Resale.

3.0 Annotations

Annotations, like highlights and text callouts, have security options to limit who can alter the annotation and even who can view the annotation.

3.1 Protected Annotations

An annotation marked as protected can only be modified by its creator or the document owner.



> **Note**: The annotation's creator or the document's owner are the only users who can mark an annotation protected.

3.2 Redactions

3.2.1 Redactions in General

Images and/or text associated with a document can be redacted, allowing you to hide sensitive material from unauthorized users. Only users with sufficient security rights can view redacted material, which will appear highlighted in gray. Users without security rights will see a black or white area, instead of the image or text behind it.

3.2.2 On Export Burn Them into Image/Text

You can specify whether to include redactions and other annotations such as highlights and stamps when documents are exported from Laserfiche.

Users who do not have permission to view redacted content on a document will always export secured images with redactions; the option only applies to documents for which a user has the right to see through redactions. When a document has been exported with redactions, the redaction will be burned in to the image. No user will ever be able to view the content behind the redacted portions of the image on the exported document.

3.2.3 Text and Image Layers

If you choose to export a Laserfiche document as a PDF file, remember that the PDF file can include the image and text from each page in the document. To secure the content stored in the PDF file, make sure that both the image and the corresponding text have been redacted in the Laserfiche document. By default, redacting an image in Laserfiche 8 will also redact the associated text.

Laserfiche Certified Professional Program

4.0 Troubleshooting

When problems are encountered in Laserfiche, they can be related to system configuration as opposed to improperly functioning software. One of the key configuration issues is security, as it affects what users can do in the system and even what functionality is available. While you might not approach the problem assuming that security is at its root, it is important to keep security configuration in mind as a possible culprit. This section introduces some of the problems that might result from improperly configured security and how best to address them.

4.1 Basic Steps to Indentify/Solve a Security Problem

In terms of figuring out whether a user's issues are due to software issues or security misconfiguration it is important to make sure you know exactly which rights the user has. Once you have done so, it is then a simple matter to map the user's rights to what they should and should not be able to do. To that end several of the factors below come into the process.

As with all software troubleshooting, start with the big picture then try to narrow it down.

- Was this something the user was able to do before? If so, what changed?
- Does this happen for all users or just one user?
- What about all users within a particular group?

With the number of security settings available your troubleshooting steps will depend on the nature/location of the problem. For example, a user may see a document in a particular folder, but not be able to see the pages upon opening it. This problem is likely related to volumes, which points to a couple of security items to be checked. First, the Volume Access Rights determine what rights a user or group has to a particular volume, including being able to see pages. Another concern would be the Laserfiche Server Service account, which needs to have appropriate rights to the drive or server hosting the volume.

The bottom line is to remember that issues related to security settings can show up in different areas, and they can be a bit tricky to track down.

4.2 "I Can't Access Something" (Admin Login to Test)

As a basic check, it is worth having a user with administrative privileges log in on the same machine and see if they can do what the user cannot. In this case, this should be a user with administrative rights on the Windows machine. If possible, the administrator should then log into Laserfiche as the original user. This will help determine if the issue is related to permissions within Laserfiche or a configuration on the local workstation. If the administrator is able to complete the action that the user was not, the issue is likely to be security related.

Laserfiche Certified Professional Program. Not For Distribution or Resale

Likewise, the admin can log in to Laserfiche with administrative privilege as a follow-up test. Again, being able to complete the action that the user could not points to a security problem. This time, however, it would be Laserfiche security as opposed to general Windows security. Testing for and tracking down a specific user or group's security configuration that is causing the problem may be tricky, depending on how the system is set up.

4.2.1 Considerations for Laserfiche Accounts (Username and Password)

Testing the security setup of a Laserfiche account is a bit easier than a user logging in with Windows credentials. For one, it does not matter which domain account is logged into the workstation; it is easy to log into Laserfiche with different accounts. Additionally, group membership is always a concern. From the Laserfiche Administration Console you can see which groups a particular user is a part of. When all else fails, effective rights are very informative. Anywhere that security can be set you can view the effective rights of a given user or group, in order to identify what Laserfiche thinks the user should be able to do.

4.2.2 Considerations for Windows Accounts

Testing Laserfiche security settings for users logging in with Windows accounts is a bit more complex. To begin with, it is harder to change who you are logged into Laserfiche as. Of more concern is tracking down issues related to conflicting group rights, since the Admin Console cannot be used to identify the user's AD groups. In this situation, it is best to start by identifying the effective rights the user has. If it looks like conflicting group rights may be causing the problem, you will want to identify all of the AD groups the user belongs to and check the effective rights for each of those groups.

Be aware that a Windows account can be assigned to a Laserfiche account—both user to user and group to group. In this case, your troubleshooting will need to focus on the Laserfiche accounts. This is most likely to show up on a system that has been migrated to Laserfiche 8 from a previous version.

4.3 Inheritance

Inheritance is the most common place to make mistakes in an otherwise solid security policy. There are really two types of inheritance: assigned rights inherited from group membership, and folder-level security (Entry Access Rights) inherited from a folder higher up in the folder structure. Group rights can be inherited from as high up as the Everyone group, and folder rights can be inherited from as high up as the root level of the repository. Since inheriting rights from the group was discussed in the previous section, this section will focus on inherited Entry Access Rights.

Entry Access rights are inherited through *scope*. When setting rights on a folder, scope determines how far those rights extend. The most common mistake with scope is to let the rights extend down the folder tree with a value of "This folder,

Laserfiche Certified Professional Program - For Distribution or Resale.

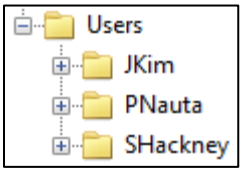
subfolders, and documents," which can lead to users having rights to inappropriate content. To restrict that access, administrators may end up denying rights on folders further down the tree, which can cause problems in several ways, including denied rights blocking out users that should have access and the administrative burden of having to set up denials on all newly created folders.

When looking at a folder's Entry Access Rights, it will show both inherited rights and rights explicitly assigned to the folder. Additionally, you can view any user's effective rights to see exactly what the combined effect is of inherited rights, explicit rights, and rights from any group memberships. If a user or group has rights that they should not, scope is a likely culprit and should be investigated.

Recommendations for avoiding problems with inheritance on Entry Access Rights:

- **Pay attention to scope** to ensure the rights you are setting do not extend further than intended.

  Example: Under the Users folder, there are subfolders for each employee in a department. For the people to get to their folders, they need access to the Users folder. The best way to accommodate this is to give the department's group rights on the Users folder with a scope of "This entry only." Then on each folder you can give rights to the appropriate user.



- **Any new repository gives the Everyone group rights on the root level** with scope that includes the entire repository. If this is not changed, users will have read only access to everything in the system.
- **Avoid using denies**. Denying a group access to a folder means that giving a member of that group access to the folder will have no effect. In Laserfiche, an undefined right is effectively a deny, so it is much better to leave rights undefined when access should be restricted.
- **Inheritance should remain *enabled***. Every folder in Laserfiche has the option of not inheriting the rights granted through scope. While this can be used as a temporary measure when troubleshooting a problem, it should generally not be used as a matter of policy, as it would require much more administration to assign rights on all the folders in the repository individually—not to mention introducing much more potential for configuration issues.

4.4 Incorrect Use of Explicit Deny

As previously mentioned, leaving an access right blank is effectively a deny, the difference being that a user can still be given access separate from the rest of the group. Again, explicitly denying a right is going take precedence over an explicitly allowed right. It must be pointed out that this applies to more than just Entry Access Rights. Volumes, templates, and fields all have rights that can be denied. When trying to track down why a user does not have rights to something they should, denies are an important place to look.

Laserfiche Certified Professional Training. Not for Distribution or Resale.

4.5 Security Tags

If one or more security tags has been assigned to a document, a user must be assigned each of those tags to access the document. Diagnosing an issue as being security tag–related, however, can be difficult because a user lacking appropriate tags will simply not see the document. This means that if there are concerns about documents "disappearing" from the system, security tags should be explored as the possible culprit. This can be identified if an administrative or other user with the appropriate tags assigned can see the document that has been reported as missing.

> **Note:** If a security tag needs to be assigned or removed for testing purposes, the user will need to log out and log back in after the change has been made. If the user remains logged in, it will appear that the change in tag assignment didn't do anything.

4.6 Folder Filter Expressions

Folder Filter Expressions (FFEs) hide content in much the same way that security tags do. If filter expressions are being used, they are another possible culprit when users complain of documents disappearing. Given the complex nature of FFEs, the possibility of a misconfigured expression should be investigated. Additionally there is a privilege called "Bypass Filter Expressions," which will make a user exempt to the restrictions imposed by FFEs, which can be helpful in identifying errors as being caused by filter expressions. If you give this to a particular user and the "missing" documents show up, FFEs are very likely the cause. Of course, you may not want to give the user Bypass Filter Expressions for security reasons. In that case, an administrative account can be used to determine if filter expressions are causing the problem.

On the other side of that coin, a situation may come up where a user can still see files that should be restricted by FFEs. Again, one option is the actual expression itself. Additionally, filter expressions will not have their desired result if the Bypass Filter Expressions privilege is given to a user or group that needs to have their rights restricted. You can see a user's effective privileges in the Administration Console and use it to determine if the right is coming from a particular group.

Note that the Everyone group has Bypass Filter Expressions by default. This privilege needs to be removed in order to secure content using FFEs.

4.7 Access Rights

In addition to Entry Access Rights there are three other types of Access Rights: volume, field, and template. The rights basically fall into the categories of read, modify, and manage. If a user thinks they should be able to set a field value but can only see and search on what other users have typed in, it is straightforward to check security settings. Note that the Write Metadata Entry Access Right is associated with editing field values.

Laserfiche Confidential Professional Proprietary Not For Distribution or Resale.

A trickier challenge is if a user cannot see something they should be able to, because they are less likely to notice the problem. Again, Effective Rights will tell you what a particular user can do with a given volume, field, or template.

Volume security can show up in interesting ways. For example, a user that has appropriate Entry Access Rights to get to a document will still see it even if they do not have appropriate volume rights. However, upon opening the document, they will be unable to see the image, text, or thumbnails. This shows that there is some problem with volume configuration, and Volume Access Rights is a good first step for tracking down the issue.

4.8 Privileges

The administrative abilities granted through Privileges do have side effects to be aware of. Since the goal is to be able to manage specific parts of the repository, those areas will be accessible to the user.

4.8.1 Manage Entry Access

This privilege gives users the ability to set up folder security through Entry Access Rights. What this means is that users will be able to see every folder and document in the system so that they can set security on it. Note that this does not include entries hidden by tags, which is a change from Laserfiche 7.

The other implication of this privilege is the ability to purge any entry from the recycle bin. This can be confused with the Purge feature right, but that just allows purging of a user's own deleted documents.

4.8.2 Bypass Browse

This privilege will ignore the "Browse" Entry Access Right and is designed to improve the speed of displaying folder contents and search results. With this right turned on, users will see the existence of folders they do not have access to. They will receive an "Access Denied" message when trying to open the entry, but generally Laserfiche security is configured so that users do not even see those things they do not have access to. This privilege is given to the Everyone group in newly created repositories and generally should be turned off.

4.8.3 Bypass Filter Expressions

This privilege is also given to the Everyone group on a new repository. The idea is that if filter expressions are not being used, it will improve performance because the Client will not even attempt to calculate rights from filter expressions. If FFEs will be used in the repository, this privilege needs to be turned off before they have any affect.

Laserfiche Certified Professional Program Not For Distribution or Resale.

4.8.4 Manage Volumes, Templates, and Fields

Similar to the effects of Manage Entry Access, users that can manage these items will see them, even if they have been denied access by another administrator.

4.8.5 Records Management

Records management privileges are required to manage the retention and disposition of records stored in Laserfiche when using the Records Management module. This can be a bit tricky because there are also Entry Access rights associated with records management. In order to actually cut records off, dispose of them, etc., the user must have the Records Management privilege *in addition to* the appropriate Entry Access Rights.

4.8.6 The ADMIN Account

It is important to note that while the default ADMIN account includes every privilege, this does not need to remain the case. This means that using the ADMIN account for troubleshooting purposes may not behave as expected. When additional accounts with administrative privileges have been created, you should verify that the ADMIN account indeed does have all privileges before troubleshooting a privileges issue.

4.8.7 Testing and Troubleshooting

An important note about privileges is that the user's rights are determined upon login. That means that if privileges are being tweaked in order to test or troubleshoot something, they will not appear to have an effect if the user has been and remains logged into Laserfiche. If a privileges is changed, the user needs to log out and back in before the results of the change can be tested.

4.9 Feature Rights

Feature Rights determine what functionality a user has, including the ability to delete or move entries. Without the appropriate Feature Right, a user will not be able to commit an action, even if they have been given the Entry Access Right. Additionally, a user lacking a particular Feature Right, like Search, will see that functionality disabled in the Client. In this case, the search button would be grayed out.

4.10 Windows Security

When troubleshooting odd behavior, another security-related concern is the account assigned to the Laserfiche Server service. This service requires access to your database server and file server, in addition to being an administrator on the Laserfiche Server machine. Generally this is not that big a deal for a fresh installation. However, it can become a concern after an infrastructure upgrade,

Laserfiche Certified Professional Program. Not For Distribution or Resale

specifically if all of the components were hosted on a single machine but then one got pushed to a separate server.

If the Laserfiche Server service account was running as a local system account, it will not have access to the separate machine. Additionally, issues like expired passwords or changes in Windows permissions can affect the Laserfiche system.

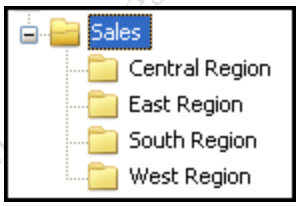
Laserfiche Certified Professional Program. Not For Distribution or Resale.

5.0 Best Practices

5.1 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 scope, 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 folder structure so that higher levels are more restrictive and lower levels less so; this simplifies the process of keeping the repository secure.

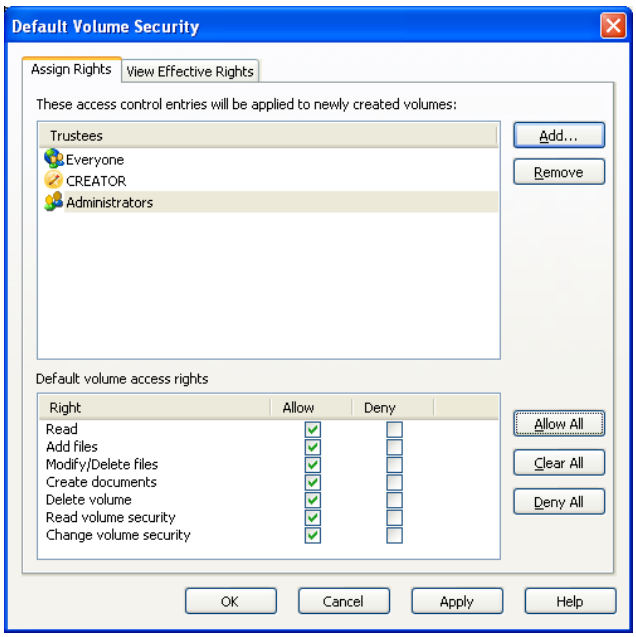


If inherited rights are in conflict, the lowest level always takes precedence: if the Sales folder has one set of allowed and denied rights, and the Central Region subfolder located within the Sales folder has a different set of allowed and denied rights, folders within Central Region will inherit their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

5.2 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. When security a field that will be assigned to multiple templates, be aware that security stays with the field. If you restrict a group's rights to the field, they will be restricted for that field on all the templates that house it.

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. 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 grant them the ability to manage their own templates only.



5.3 Default Security

Whenever you create a new volume, template, or field, Laserfiche creates a starting set of

Laserfiche Certified Professional Program. Not for distribution or resale.

security for that new object. You can customize the starting default security for your volumes, templates, and fields, and Laserfiche will automatically apply your default security to all objects of that type 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, and 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 create a new volume, these rights will be the default starting rights for the volume. You can still customize the security for individual volumes—default security simply allows you to customize the starting security configuration.

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.

5.4 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 department or job title at the same time, while still permitting you to fine-tune security if necessary by granting or denying rights to a few individual users.

Creating groups to reflect particular job titles or functions simplifies the process of adding additional users, which is particularly useful for employee turnover. It is much easier to create a Scanner Operator or Administrator group, configure security for it once, and add users to it than it is to individually configure security for each new scanner operator or administrator. Even if your site has only two administrators, security still only needs to be configured once instead of twice. More importantly, granting security by group ensures that all administrators will have consistent rights and reduces the likelihood of mistakes that accidentally grant or deny access inappropriately. If you do have users with genuinely unique security needs, however, you can also assign rights directly to those individual users.

It is possible for a user to be in more than one group at the same time. In this case, the user will inherit security from both groups, with Denied rights taking precedence over Allowed. You can also add groups directly to other groups.

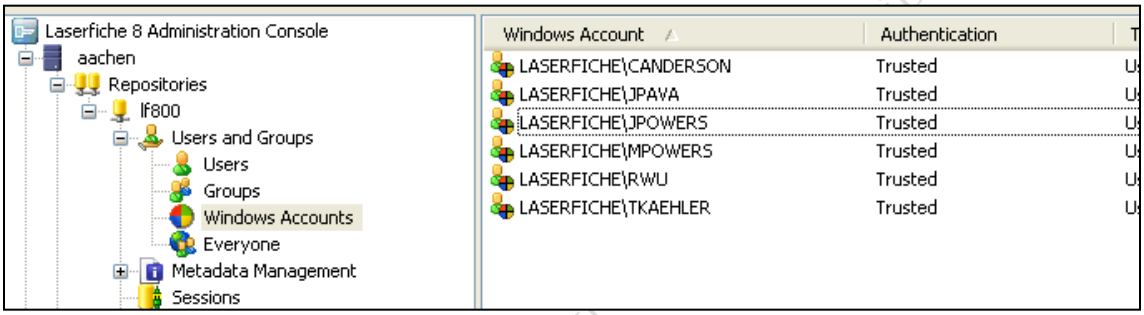
Laserfiche Certified Professional Portal. Not For Distribution or Resale.

5.4.1 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. This feature should be used carefully, since multiple conflicting rights can make security administration confusing.

5.5 Domain Accounts

In Laserfiche 8, you can treat domain users and groups—Windows Active Directory or Novel eDirectory—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.



If you add a domain group, you do not need to add the users who belong to that group to Laserfiche individually. If the group to which a user belongs is permitted to log in to Laserfiche, the user will inherit that ability. Similarly, a 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 domain accounts without adding each individual account to Laserfiche. Simply adding the relevant domain groups and setting security for those groups will allow those users to access Laserfiche. 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.

Note: After adding user and group domain accounts to Laserfiche, security rights can be applied directly to them.

6.0 Security Outside of Laserfiche

In addition to the security that gets established within a Laserfiche repository, there are also security concerns for the system in general. Most of these concerns relate to the account assigned to the Laserfiche Server and other services, as well as network communication concerns.

6.1 Windows Operating System

6.1.1 Domain Accounts

When Laserfiche is run in a distributed environment (server components on two or more machines), the Laserfiche Server service account will need to be assigned to a domain account. This way, it will have access to all of the server-side machines, not just the one it is installed on. While not necessary, it is easiest if this account is given admin rights on the relevant server machines. If this is not desirable, the account can be set up with fewer rights within the DBMS and on the file server (more information below). However, it is recommended that domain administrative rights be used during the initial configuration of a new system.

6.2 DBMS

Laserfiche uses a Database Management System (DBMS) to store document metadata, repository security settings, and a great deal of other information. The following are compatible versions of DBMS software and considerations that need to be made for each.

6.2.1 MSSQL Server

Microsoft SQL Server is by far the most common DBMS used with Laserfiche. There are many variations of this MSSQL Server, each with its own limitations and caveats, as discussed below. Laserfiche currently supports MSSQL Server 2000 (SP3) (and above), MSSQL Server 2005, and MSSQL Server 2008, with 2005 and 2008 being recommended.

6.2.1.1 Rights

Regardless of the MSSQL Server version being using, it is easiest to give the Laserfiche Server service account system administrator (SA) rights to the MSSQL Server instance. Of course, that is not always desirable. The database should initially be created through the Repository Creation Wizard, which requires the account to have System Administrator rights. After that, it can be scaled back to database owner (DBO) rights for the database supporting a Laserfiche repository. However, you should remember that during upgrades between Laserfiche versions, you may have to grant more rights again if you have scaled them back.

Laserfiche Certified Professional Program. Not for Distribution or Resale.

6.2.2 Oracle

Laserfiche supports the use of Oracle as the DBMS (Oracle 9i release 2, Oracle 10g, and Oracle 11g). For detailed help, please see the Oracle section of the Laserfiche Administration Console help file (LFAdmin.chm).

One key difference when implementing Laserfiche with an Oracle DBMS is the need to create the database schema manually (Laserfiche can automatically create the MSSQL database in the DBMS during repository creation). Instructions for doing so can also be found in the Oracle section of the Laserfiche Administration Console help file (LFAdmin.chm).

6.2.3 Regular Users Should Have No DBMS Access

In general, only administrators should be granted access to your Microsoft SQL Server or Oracle installation. Your Laserfiche database may contain sensitive information; if users are allowed to access the database directly, Laserfiche security cannot protect that information. Additionally, manual modifications to the database can cause corruption and data loss. Restricting DBMS access to administrative and other privileged users is important for protecting your data.

6.3 File Server

The Laserfiche Server service account will need access to the appropriate directories on the file server. This means it will need to be able to create folders and create, edit, and delete files within the Volume directory. This is most easily accomplished by granting the Laserfiche Server service account admin rights on the file server. However, if this is not desirable, permissions can be granted for the Laserfiche volume directory.

6.3.1 Regular Users Should Have No Access

The volume directories on the file server should be protected using Windows security to ensure that only authorized users can access those files. This protects your repository's contents—if a user can browse directly to pages in a volume in Windows, they will not be subject to Laserfiche security, and may therefore be able to access documents they have been restricted from. Furthermore, if they have the rights in Windows to modify those files, they can make changes that will not be controlled by Laserfiche security. It is a good idea to use Windows security to lock down volume directories such that only administrators or other privileged users can access them.

6.4 Web Server

Laserfiche Web products use Microsoft's Internet Information Services (IIS) to communicate with users. To make sure the Web Access or WebLink installation can communicate with the Laserfiche Server and with users connecting over a network, IIS needs to be appropriately configured. Most Laserfiche Web products will try to

Laserfiche Certified Professional Program. Not for Duplication or Resale.

do this when they are installed, but sometimes it may be necessary to configure IIS manually to cope with unusual situations or changes in the network setup.

Web Access and WebLink run as the application pool user in IIS. This user requires read and write access to the **tempDirectory** and **cacheDirectory** and read access to the **Config** subfolder inside the Web Files folder of the installation directory. Access to these specific locations is configured for you during the Web Access installation.

6.4.1 Securing Client-Side Communication

When using Web Access to distribute sensitive information across the Web, it is recommended that the connection be encrypted. Web Access can be secured with SSL just like any other Web site and can be configured with standard procedures

6.4.2 Securing Server-Side Communication

If the Laserfiche Server and Web Access server are hosted on separate machines, that traffic may need to be secured, too. The primary purpose for this is to encrypt username and password data from user logins. If typing in Laserfiche or domain credentials, that information is sent between the servers over HTTP as text. This communication can also be encrypted with SSL or TLS, but the procedure is somewhat different from the client-side version. Both server machines will have an X.509 certificate added to them in order to facilitate secure communication. Information can be found in an article on the Laserfiche Support Site. Note that as far as this article is concerned, Web Access is the client.

Laserfiche Certified Professional Program. Not for Distribution or Resale.

7.0 Scenarios

7.1 Regulated Organization

Carl Friedrich, CFP®/CEPF®, runs a small, fee-only financial services company called Friedrich Wealth Management with his wife, Marisa. They cater to many of their busy clients' needs by traveling to the clients' homes or places of work. "We have to coordinate all areas of our clients' financial lives, which is a pretty tall order," says Friedrich. "To be as dynamic as we wanted to be, we knew we needed a paperless office. And as much as we moved around, we needed a way to manage client information where security was bulletproof, but we could be mobile enough to capitalize on making the planning process exceptionally convenient. "

The Security Challenge

Freidrich required the flexibility of an office that fits in his car without sacrificing security or compliance. This meant that he needed to be able to pull up client records on a laptop, but to be sure that sensitive data would not be compromised even if hardware was stolen. Client data also had to be stored in a way that was compliant, but efficient and easily accessible.

The Laserfiche Security Solution

Software-as-a-service (SaaS) content management was simply not an option, as Friedrich Wealth Management could only guarantee the integrity of its data if it was housed on its own server, a key assurance Laserfiche Avante provided, as well meeting as other security, compliance, and mobility needs. System security is set-up such that Friedrich's own laptop is itself part of the firm's domain, accessing the Laserfiche Server via a VPN connection where all other traffic is blocked by a firewall and IP filters. Utilizing Windows Active Directory authentication, Friedrich himself is able to access the Laserfiche repository with a single sign-on using fingerprint biometric authentication. A pre-existing integration with Junxure, Friedrich's Customer Relationship Management (CRM) software, automatically saves a single, master copy of client documents and correspondence generated from Junxure directly to Laserfiche using Workflow. "It's iron-clad security and audit-proof compliance," says Friedrich.

7.2 Large Organization

Chesterfield, a county in Virginia with a history dating back to the 1600s and no shortage of records to manage, made the switch from paper documents to document imaging in 2001. Initially five pilot departments made the switch, all of which are still using Laserfiche. In 2005, Chesterfield upgraded to the Laserfiche Records Management Edition (RME) and has continued to expand its use of Laserfiche, including using WebLink to give access to PDF files for land parcels in their GIS system.

Laserfiche Certified Partner Program. Not for Distribution or Resale.

The Security Challenge

Chesterfield's Human Resources department was among those to make the switch to Laserfiche. Electronic document management held the potential to make the HR team's lives much easier, but it also posed potential security concerns given the sensitive nature of HR documents. Additionally, it was important to ensure that whatever security solution was established would continue to function properly after the upgrade to RME and the new file structure that the upgrade would entail.

The Laserfiche Security Solution

During their initial switch to a paperless environment, the HR department replicated their rigorous security policy for paper documents within Laserfiche. However, unlike in the paper system, implementing security in Laserfiche allows HR staff to group supporting documents and even personalized notes together with sensitive HR documents.

With the upgrade to RME, the HR department used Workflow to maintain their security policy despite switching to a disparate file structure to satisfy records management requirements. Staff used RME to manage the records retention schedule, assigning access restrictions and creating shared folders to replicate the existing security structure. Using Workflow, they then copied records to the shared folders. In the end, HR personnel who had used the old system barely noticed the interface had changed.

Laserfiche Certified Professional Program Not for Distribution or Resale.

Laserfiche®

Laserfiche Advanced Security Training Manual
November 2010

Authors: Pieter Nauta, Jennifer Dickson, Connie Anderson
Technical Editor: Justin Pava
Editor: Tammy Kaehler

Laserfiche
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 © 2010 Laserfiche
All rights reserved

Laserfiche Certified Professional Program - Not For Distribution or Resale.