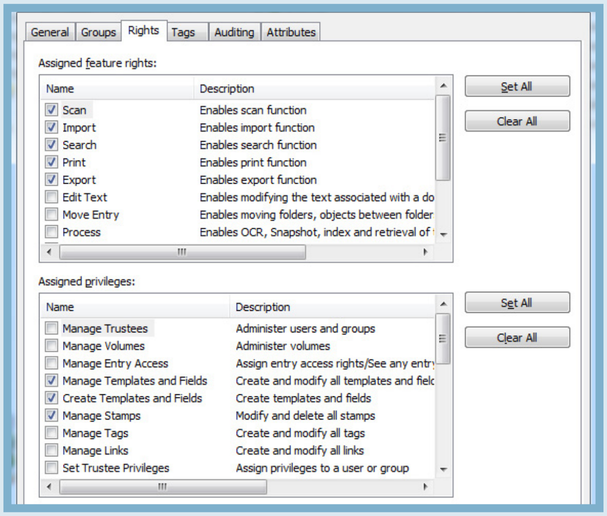
Laserfiche **Security**

Laserfiche provides incredibly granular security, ensuring that users will only see content they are allowed to see. This security is cumulative; users can only view content if they have all the appropriate rights. In addition, Laserfiche uses built-in Windows security and AES-256 encryption to ensure that data is secure when it is in transit and when it is at rest.

User-Level Security

- **Unique users.** The Laserfiche License Manager allows administrators to control the level of access users have to view, modify or delete documents or folders in your Laserfiche system. With Laserfiche, each user has unique security credentials, eliminating the risk of users sharing passwords and enabling leading security practices such as segregation of duties and the principle of least privilege.



Assigned feature rights:

Name	Description
☑ Scan	Enables scan function
☑ Import	Enables import function
☑ Search	Enables search function
☑ Print	Enables print function
☑ Export	Enables export function
□ Edit Text	Enables modifying the text associated with a do
□ Move Entry	Enables moving folders, objects between folder
□ Process	Enables OCR, Snapshot, index and retrieval of

Assigned privileges:

Name	Description
□ Manage Trustees	Administer users and groups
□ Manage Volumes	Administer volumes
□ Manage Entry Access	Assign entry access rights/See any entry
☑ Manage Templates and Fields	Create and modify all templates and fielc
☑ Create Templates and Fields	Create templates and fields
☑ Manage Stamps	Modify and delete all stamps
□ Manage Tags	Create and modify all tags
□ Manage Links	Create and modify all links
□ Set Trustee Privileges	Assign privileges to a user or group

The Laserfiche Administration Console provides total system control.

- **Single Sign-on.** Support for enterprise directory service systems (including Microsoft Active Directory and Novell eDirectory) helps ensure standard account policies such as password complexity and password expiration are enforced by the Laserfiche system, while using Active Directory groups to simplify security delegation and administration.

Document-Level Security

- **Data Classification.** Individual documents can be secured with security tags and Victorian Electronic Records Strategy (VERS)[1] classification levels. In order to see a document or folder with a security tag, a user must have been granted that security tag. VERS classification levels prevent users from moving high-security documents into lower-security folders.

- **Redactions.** The text and pages of a document within Laserfiche can be secured with black or white redactions. These redactions can be burnt into the document image on export, which helps ensure that the information is secure when it leaves the repository.

- **Secured metadata.** Field and template access rights allow you to control who can view sensitive metadata about documents.

- **Encrypted content transfers**. Laserfiche briefcases enable secure transfer of files from one repository to another.

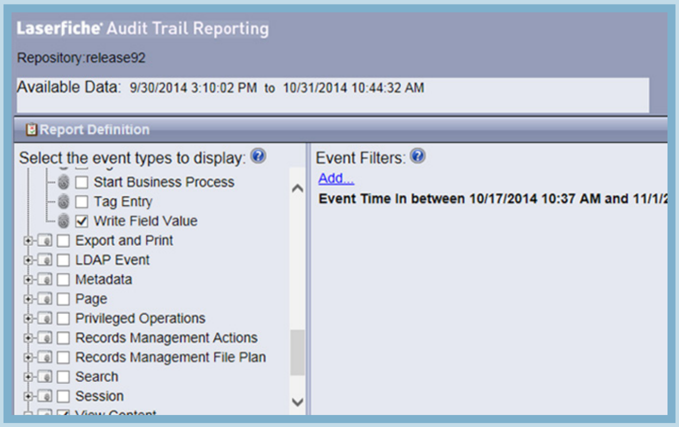
- **Encrypted exports**. Volume encryption and securing protect information for archival, backup and export.

- **Delegation of privileges.** Granular privileges allow distribution of administrative permissions across your organization.

[1] Developed by the Public Record Office in Victoria, Australia, VERS is the standard for reliably and authentically preserving electronic records over long periods of time. It is accepted and used as the backbone of e-Governance by archival institutions around the world.

System-Level Security

- **Database security.** Laserfiche leverages built-in Windows and DBMS (Microsoft SQL Server, Oracle) security to prevent users from accessing the DBMS, where metadata, security, user, and group information is stored.
- **Volume security and encryption.** Volume encryption prevents administrators from bypassing database security and viewing files directly. Each volume can be encrypted and secured, rendering it inaccessible from both the volume in Laserfiche and from Windows.
- **Data encryption.** Laserfiche offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to implement the methods that best meet their needs.
- **Data integrity verification.** Volume checksums verify that document contents have not been altered outside of Laserfiche.
- **SSL/TLS encryption.** Built-in SSL and TLS cryptography enables customers to encrypt communications between applications.
- **Secure web deployment.** Web products leverage built-in IIS access security and support multiple firewall configurations, including secure deployment in the DMZ.
- **Auditing.** All actions within the Laserfiche repository are audited and tracked, including viewing and modifying documents and any modifications to repository properties or security.
- **Watermarking.** Printed or exported information can be recorded and watermarked.



Repository:release92

Available Data: 9/30/2014 3:10:02 PM to 10/31/2014 10:44:32 AM

Select the event types to display:

□ Start Business Process
□ Tag Entry
☑ Write Field Value
□ Export and Print
□ LDAP Event
□ Metadata
□ Page
□ Privileged Operations
□ Records Management Actions
□ Records Management File Plan
□ Search
□ Session
☑ View Content

Event Filters:

Add...

Event Time In between 10/17/2014 10:37 AM and 11/1/2

Laserfiche Audit Trail tracks all activity within the Laserfiche repository.

Certificates and Compliance

- **Section 508 compliant.** Laserfiche is compliant with Section 508 standards of the Rehabilitation Act of 1973, providing equal access to electronic data in Laserfiche to people with disabilities.
- **Perpetual DoD 5015.2 certification.** Laserfiche is certified in the Department of Defense 5015.2 version 3 design criteria standard for electronic records management, the accepted standard for many state, county and local governments.
- **VERS v2-compliant.** Laserfiche is certified with the Victorian Electronic Record Strategy (VERS) requirements, a world-recognized standard for reliably and authentically preserving electronic records over long periods of time.
- **Integrated digital signatures.** When configured properly, digital signatures may help ensure compliance with a number of domestic and international regulations for e-Governance. Laserfiche provides an integrated solution that complies with FISMA, CFR Part 11 FDA, FIPS, VERS and Clinton E-Signatures Act standards.

YOUR NEXT STEP

Contact Us
(800) 985-8533

Get a Demo
laserfiche.com/demo

Read User Best Practices
laserfiche.com/solutionexchange