Xerox® DocuShare® Security Features

Security White Paper

Xerox® DocuShare Security Features

Businesses are increasingly concerned with protecting the security of their networks. Any application added to a network must support existing security policies and protect sensitive information. Xerox® DocuShare provides a range of security features to safeguard document content.

Security Layers

The network environment and the server(s) on which DocuShare is deployed provide several "layers" of security.

1. **Network or Operating System Security.** To access or manipulate the DocuShare data directories, network users must use login credentials (either Windows or Unix) to access the desktop or workspace on the server running DocuShare. If DocuShare is running on a private Intranet, not only are all network workstations and the DocuShare server itself password-protected, but the Intranet is protected from unauthorized access by the firewall (keeps unauthorized Internet users from gaining access to the company's private Intranet resources).

2. **Web Server Security. Web servers such as Microsoft IIS,** Apache, or Sun SunONE provide additional access security. DocuShare includes a Web servlet engine called Tomcat (the Java version of Apache) to handle browser, or http protocol, requests and to generate the user interface. IIS, Apache, and SunONE provide password protection to the Web server and can be enabled for Secure Sockets Layer (SSL). SSL encrypts all transactions over the Web between the server and browser and requires use of an https (secure http server) server connection instead of the http protocol. Businesses requiring a secure environment use SSL. DocuShare can be enabled to use the Secure Sockets Layer in conjunction with IIS, Apache, or SunONE.

3. **DocuShare Security.** DocuShare provides additional security through account types and user levels, password protection, access permissions, site access policies, content encryption, and administration tools. These security features are described in the following section.

DocuShare Security

DocuShare security features protect content from unauthorized access and modification. These features are available to both the site administrator and users, enabling them to apply the level of protection needed for their site.

DocuShare User Account Types

Each DocuShare installation can include four different user account types.

Guest	An anonymous user account that can view unrestricted content on the site; often used for public-facing sites.
Read-Only User	A registered user account on the DocuShare site that is able to search for, read, and download content. Read-Only users cannot add new content or change existing content on the site. Any number of Read-Only user accounts can access DocuShare content.
DocuShare User	A registered user account on the DocuShare site that is able to search for, read, download, add, update, or change content (subject to the access permissions set on content). Any number of DocuShare user accounts can access DocuShare content.
CPX User	A registered user account on the DocuShare site that is able to perform all DocuShare user tasks, plus certain activities that are restricted to CPX users (e.g., create collaborative workspaces and content rules). Any number of CPX user accounts can access DocuShare content.

DocuShare Administrator Groups

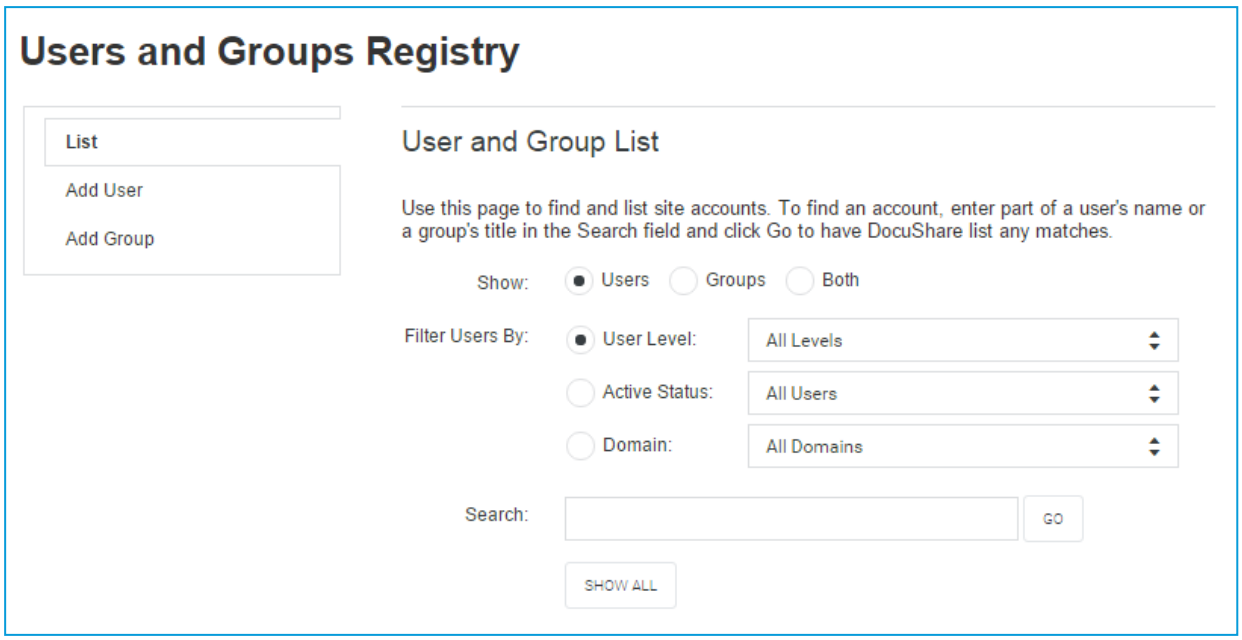
Site Administrators group (Group-1)—A group with a single member, the site administrator (User-2), whose account is created when DocuShare is installed. The site administrator can add other registered users to this group. Members of this group have full administrative access to the DocuShare site, including accounts, user objects, and site configuration.

Content Administrators group (Group-2)—A group of registered users that has content administrator privileges to the DocuShare site. Members of this group can view and change all content on the site, regardless of the access permissions. Initially, the site administrator and the Site Administrators group are members of this group. If a site has sensitive data that needs to be restricted to a few users, the Site Administrators group can be removed from the Content Administrators group.

Account Administrators group (Group-3)—A group of registered users that has account administrator privileges to the DocuShare site. Members of this group can create and manage user accounts (Read-Only, DocuShare, and CPX) and set site access policies. The site administrator assigns users to this group.

DocuShare Password Security

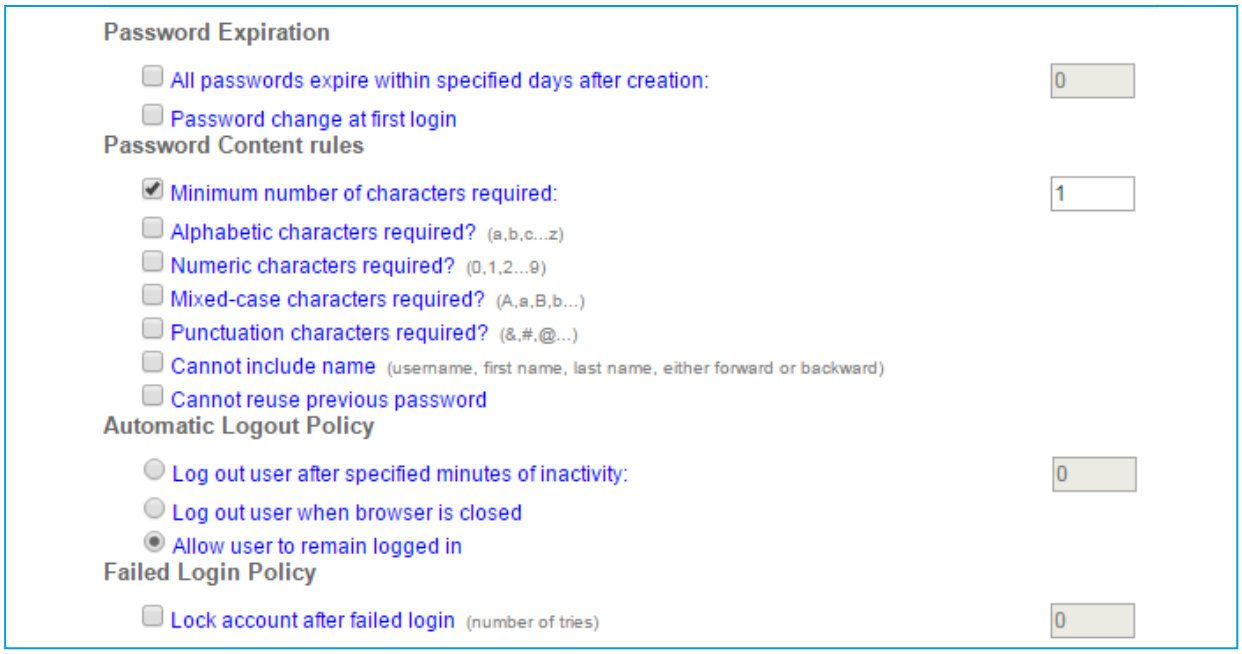
Access to DocuShare content is managed through user accounts (CALs), which can reside on the DocuShare server or on Lightweight Directory Access Protocol/Active Directory (LDAP/AD) server. Accounts created and managed within DocuShare's "internal" identity domain rely on DocuShare for password management, group membership, and authentication.



An administrator creates and manages user accounts in the DocuShare internal domain from the registry.

DocuShare ID/password data is validated using the MD5 Message Digest hash algorithm, which generates a 128-bit "fingerprint" for validating the input ID/password. It is this hash that is stored in DocuShare's database. For more information on the MD5 algorithm see http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html.

The DocuShare administrator determines the password policies for user accounts. The administrator can set an expiration period for passwords, specify a minimum password length, require the use of special characters, and set additional policies.



An administrator uses the Account Policies page to specify the password rules for a site.

Lightweight Directory Access Protocol and Microsoft Active Directory Support

DocuShare provides an LDAP connector, which enables a site to use a corporate LDAP or Active Directory server for account management and authentication. When using LDAP/AD, users log into DocuShare using their LDAP credentials (a separate login is not required). Additionally, network administrators can set password policies on their LDAP/AD server to enforce stronger security measures. It is possible to implement stricter authentication within DocuShare, such as RSA SecurID, by integrating such authentication into the LDAP/AD server.

DocuShare supports both internal and external domains. An administrator can use DocuShare to manage the accounts created on an internal domain and use an LDAP/AD server to create and manage separate sets of accounts on one or more external domains.

Authentication and User Identity Management

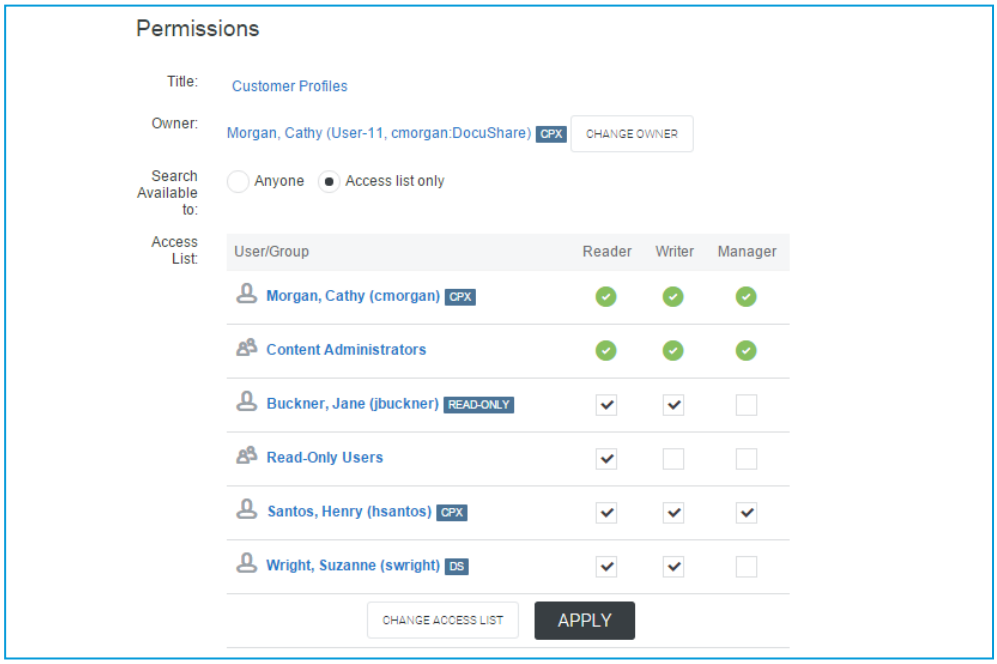
DocuShare uses cookies to authenticate a user's identity. For each request to DocuShare, via a browser, the DocuShare Client, the WebDAV Client, or Guest access, DocuShare distributes an encrypted authorization token to the client. DocuShare internally tracks the number of sessions per client.

Additionally, DocuShare supports persistent cookies (not recommended for security-conscious sites). The site administrator enables this feature from the Administration UI. When the feature is enabled, a retain login for future checkbox appears in the login area. When a user selects the checkbox, a DocuShare cookie is associated with that user's desktop. When logged into that desktop, the user does not need to log into DocuShare again, even after a restart.

DocuShare Access Permissions

Every DocuShare object has an access control list (ACL), which is assigned to the object when it is added to the site. The access control list identifies the users and groups who have access to the object and the type of access permissions each account has. An administrator can set up a site to use either three or six access permissions. The use of six permissions provides sites with more exact control over content.

Three Permissions	Six Permissions
Reader allows the user or group to read the content of the object, including its properties and permissions, and for documents, to download them.	Read Properties allows the user or group to read the object's properties and permissions.
Writer allows the user or group to change the object's properties and add new objects, including new versions of documents.	Read Content allows the user or group to read the content of the object.
Manager allows the user or group to delete the object, and change the object's permissions and owner.	Read History allows the user or group to read the object's change history.
	Write Properties allows the user or group to change the object's properties.
	Write Content allows the user or group to add new objects, including new versions of documents, and change the object, such as its location.
	Manage allows the user or group to delete the object, and change the object's permissions and owner.



Using the object's Permissions page, users can change the accounts in the access control list, the type of permissions each account has, and who can see the object in a search.

In addition, users can control whether or not the object displays in a search results list. By default, only accounts in the access control list with Reader/Read Properties permission (or greater) can see an object in a search results list. The object's owner or a user with Manager/Manage permission to the object can change the default setting to allow guests and users to see the object in a search.

DocuShare Site-wide Access Policies

DocuShare provides four site-wide access policies that the site administrator can change depending on the security needs:

1. **Site Access Authority**—Determines who can enter the site. Options are Guest, User, and Administrator. Setting this authority to User is a quick and easy way to disable site-wide Guest access.

2. **Registry Access Authority**—Determines who can view the users and groups registered on the site. Options are Guest, User, and Administrator.

3. **Account Creation Authority**—Determines who can create new user accounts (CALs) on the site. Options are Guest, User, and Administrator. Most sites will set the authority to Administrator. On sites that allow users to create accounts, users are able to create accounts at their user level or lower. For example, DocuShare users can create DocuShare and Read-Only user accounts, and CPX users can create CPX, DocuShare, and Read-Only user accounts. If the administrator chooses to allow Guest users to create user accounts, the administrator determines the user level assigned to the account (Read-Only, DocuShare, or CPX). Typically, if Guest users are allowed to create user accounts,

an administrator sets the user level to Read-Only (essentially creating a user self-registration process). The number of each type of user account that can be created is controlled by the CALs available on the site.

4. **Group Creation Authority**—Determines who can create new group accounts on the site. Options are User and Administrator.

An administrator uses the Access Policies page to set site and registry access and to specify who can create user and group accounts.

Protecting your Documents in the Document Repository

When configuring DocuShare, you can choose where your documents are to be stored, either on a local drive (recommended) or on a SAN or other external storage device.

- **Windows server**—To configure the minimum required NTFS permission for users accessing IIS, grant the anonymous Internet user account (IUSR_computer_name, by default) and any other accounts or groups that would need access to the Web server the following directory permissions:
  - DocuShare Directory—CHANGE (RWXD) (C:\Xerox\DocuShare\Documents and all subdirectories)

- **Solaris or Linux server**—Grant the system account DocuShare uses read, write, and delete permissions to the [DSHome]\Documents directory.

Additional Document-level Security

For added data security, DocuShare offers a Content Encryption add-on. This add-on module automatically encrypts the content of a document when it is uploaded to DocuShare. Document content is encrypted using a symmetric key cryptography algorithm before it is written to the content store. The encryption keys are stored in the relational database, with one unique key per document version and rendition.

Document content is decrypted when it is accessed through standard DocuShare interfaces. This prevents any system intruders from reading document content, even if they gain access to the storage server either remotely or physically. This also ensures that any backup tapes, which might fall into the wrong hands, are not at risk of disclo- sure. In the current release, DocuShare supports the Advanced Encryption Standard (AES) algorithm. The Java SDK shipped with DocuShare supports up to a 128-bit key size.

Like most encryption-based software technologies, sale of the DocuShare Content Encryption add-on is subject to export restrictions as defined by the U.S. Federal government. Therefore, the add-on module requires a separate installation disk and an update to the DocuShare server license key.

Using third-party software, document-level security can be added to documents before they are uploaded to DocuShare. For example, Adobe offers PKI (Public Key Infrastructure) protection of PDF documents. Individual documents can be encrypted, requiring a password to "unlock" certain view or print functions on the document. Other third-party applications extend this type of protection to other document formats, and are referred to as PGP or "pretty good protection."

Configuring the Web Server—Security Options

To a large extent, DocuShare security is dependent on network and operating system (server) security. However, there are other factors that are worth considering.

By default, when a client initiates a browser (HTTP protocol) session, DocuShare login information and passwords are transmitted in clear text, which can be a security issue. However, different server configurations provide varying levels of security.

- **Standalone** —DocuShare running under the Tomcat Web server. The Tomcat Web server does not provide any security. Usernames and passwords are sent in clear text. DocuShare listens to requests on TCP/IP port 8080. Users connect to DocuShare from a Web browser by typing a URL similar to: "http://mydocushare.mydomain.com:8080."

- **Bridged to IIS or Apache** —IIS or Apache handles the incoming Web requests and passes the requests to DocuShare via the Jakarta/Tomcat bridge (DocuShare installation option). Usernames and passwords are sent in clear text. Users connect to DocuShare from a Web browser by typing a URL similar to: "http://mydocushare.mydomain.com" or "http://mydocushare.mydomain.com:8080."

- **Bridged to IIS or Apache with SSL**—By adding a Security Certificate to IIS or Apache, you can enable SSL communication to DocuShare. With SSL enabled, all usernames and passwords are encrypted before they are sent. Users connect to DocuShare from a Web browser by typing a URL similar to: "http://mydocushare.mydomain.com," "http://mydocushare. mydomain.com:8080," or "https://mydocushare.mydomain.com."

- **Bridged to IIS or Apache with SSL only**—By adding a Security Certificate to IIS or Apache, you can enable SSL communication to DocuShare. With SSL enabled, all usernames and passwords are encrypted before they are sent. If this configuration is preferred, then the Web server must be configured to deny requests to TCP/IP port 80 and the Tomcat server must be configured to deny requests to port 8080. Users connect to DocuShare from a Web browser by typing a URL similar to: "https://mydocushare.mydomain.com."

These configurations apply to the Web server and DocuShare; they do not describe how to secure the operating system on which the Web server and DocuShare run.

Web Server Auto Login

The DocuShare auto login feature allows Windows domain authentication to handle DocuShare login authentication. To use auto login, you must configure your Web server and then enable the DocuShare auto login feature from the DocuShare Administration UI. For IIS, this feature is enabled with NTLM Challenge/Response.

With auto login, the browser client sends the user's desktop credentials to the Web server for authentication. If authentication succeeds, a REMOTE_ USER variable is set in the Request environment passed to DocuShare in the form of REMOTE_ USER=<domain>/<username>. For auto login to work with DocuShare, this username must match the DocuShare username.

If your site is restricted (Allow Anonymous disabled and access restricted for CGI commands), the Web server sets a REMOTE_USER variable to the value of the authenticated username. When auto login is enabled, DocuShare compares the value of that variable and checks if it matches a DocuShare username. If there is a match, the user is automatically logged into the site. If there is no match, the user is not logged in as a registered user, but instead is logged in as Guest. Auto login does not apply to either the Guest or DocuShare site administrator account.

About Xerox® DocuShare®

Xerox® DocuShare, a highly intuitive and secure Enterprise Content Management (ECM) application, enables document intensive organizations to dynamically capture, manage, retrieve, and distribute information easily, regardless of skill level or location. Part of the Xerox® DocuShare content management platform, DocuShare helps customers significantly improve productivity, streamline business processes, and reduce the time and cost of managing routine business documents and information. Leading the industry in speed of deployment and ease of administration and use, DocuShare significantly reduces installation and complexity, and flexibly extends into an existing infrastructure, resulting in lower total cost of ownership and faster return on investments. Tightly integrated with Xerox® WorkCentre® multifunction printers, DocuShare can manage both hard copy and electronic content with unsurpassed ease and convenience.

For more information, call **1.800.735.7749** or visit **www.docushare.com**