# Xerox® DocuShare® Private Cloud Service

Security White Paper

# Table of Contents

# Overview

Xerox® DocuShare Private Cloud Service is a highly intuitive and secure Enterprise Content Management (ECM) application. It enables document intensive organizations to dynamically capture, manage, retrieve, and distribute information easily, regardless of skill level or location.

As part of the Xerox® DocuShare® content management platform, DocuShare Private Cloud helps you to significantly improve productivity, streamline your business processes, and reduce the time and cost of managing your routine business documents and information. Leading the industry in speed of deployment, ease of administration and use, DocuShare Private Cloud significantly reduces installation complexity, and flexibly extends into your existing infrastructure. This results in lower total cost of ownership and faster return on your investments.

Tight integration with Xerox® multifunction printers and flexible access to content from office computers and mobile devices, DocuShare Private Cloud helps you manage your hard copy and electronic content with unsurpassed ease and convenience.

This paper is intended to present details and specifics of the security being employed by DocuShare Private Cloud. This paper is not intended to be a full disclosure of all security practices and policies, and therefore may not contain such disclosures.

# Adherence to Proven Security Practices

DocuShare Private Cloud follows industry best practices by incorporating security methods of the hardware and software manufacturers that are the foundation of the system itself. By default, DocuShare Private Cloud runs on Microsoft Windows Server technology. It follows current Microsoft security hardening guidelines with regards to registry, services, security settings, and NTFS permissions. DocuShare Private Cloud also has its own internal security best practices. These are described in the DocuShare Private Cloud Security Features section of this document. For a full technical description of the hardening settings from Microsoft, please refer to the links below:

http://technet.microsoft.com/en-us/library/cc771361(WS.10).aspx
http://technet.microsoft.com/en-us/library/dd560640(WS.10).aspx

In addition to following Microsoft security best practices, the following lock-down examples are a standard part of the server configuration:

- Disable AutoAdminLogon
- Remove the DefaultPassword registry value
- Disable 8.3 naming convention requirements
- Disable CD-ROM AutoRun
- Security-hardening the TCP/IP stack
- Disable anonymous network or local access to the registry

## Highly Secure Data Centers

All hosted instances of DocuShare Private Cloud are housed in Tier 3 compliant data centers. Key components of a data center are environmental controls (air conditioning, fire suppression, etc.), redundant/backup power supplies, redundant B2B and B2C network/internet connections, and high physical and information security.

## Three-Tier Architecture

A key strength of DocuShare Private Cloud is the way in which it integrates with your environments in areas such as user authentication, web user interface (UI), WAN suitability, and web services.

DocuShare Private Cloud leverages accepted Industry IT standards and follows the common three-tier architecture:

1. **Web or presentation tier:** Comprised of a single Internet Information Services (IIS) web server, or many IIS web servers, depending on the size of the DocuShare Private Cloud deployment. Microsoft IIS provides the web server capabilities that lie at the heart of DocuShare Private Cloud, and is the vehicle that provides the web user interface to the end-user. IIS is a reliable communications platform of dynamic network applications. It offers organizations significant advantages in terms of reliability, manageability, security, scalability, and performance.

2. **Application or business objects tier:** Comprised of a single or multiple Windows servers, depending on the size of the DocuShare Private Cloud deployment. This tier is used to run and manage the processes that load new data into the system from various types of intakes, such as electronic file feed, fax, email, or print spool feed. Microsoft Windows Integrated Authentication, using either the NTLM or Kerberos protocol, coupled with the ACL for managing NTFS permissions, allows the platform to restrict access to system data and applications through standard use of Active Directory groups and users.

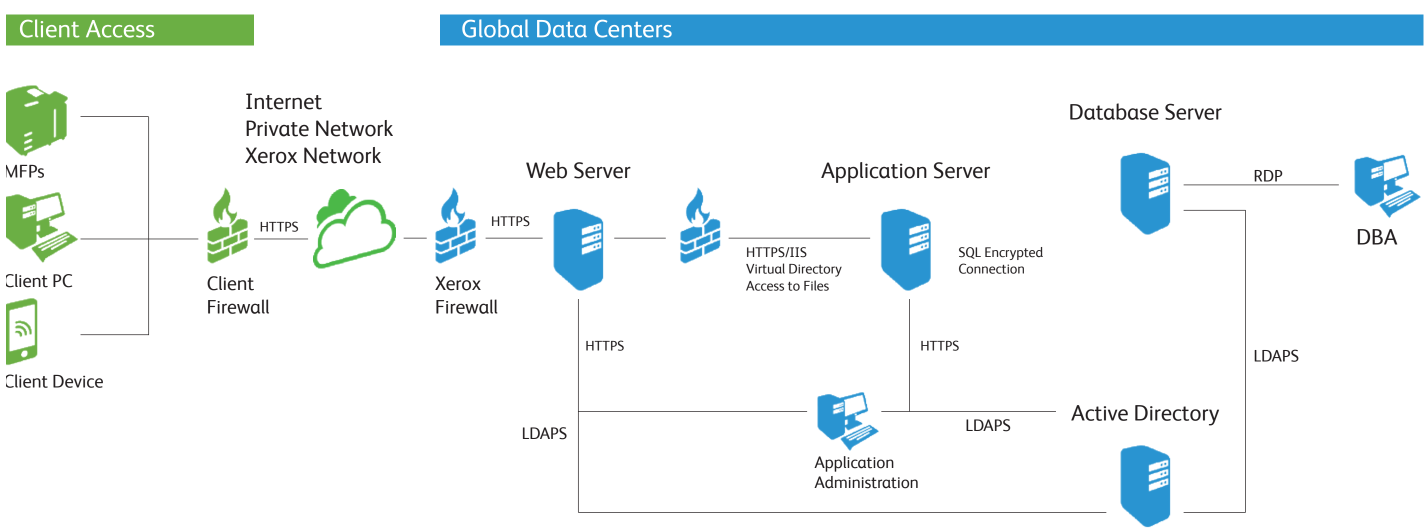
3. **Database or data access tier:** Comprised of a single database server or multiple database servers, depending on the size of the DocuShare Private Cloud deployment. This tier is used to run and manage the database architecture.

The following diagram depicts the different tiers.

**Xerox-hosted infrastructure provides global visibility with regional compliance**

**North America**
Canada
United States

**Europe**
United Kingdom
European Union



# Security Layers Safeguard Content

Businesses are increasingly concerned with protecting the security of their data. DocuShare Private Cloud provides a range of security features to safeguard your document content.

The network environment, the server(s) on which DocuShare Private Cloud is deployed, and the software application provide several layers of security.

1. **Cloud and Data Center Security:** Our production systems are located in our private data center facilities. Production web, application, file and database servers, along with network equipment are monitored and protected. Access to our data centers is monitored by video surveillance and controlled by the use of two factor authentication, such as card readers and biometric scanners, as well as on site security personnel. Access to our data centers is recorded, and requires approval along with confirmed identification.

   Cloud and data center features include, but are not limited to:

   – Secure data center
   – Encrypted user authentication
   – Internet firewalls
   – Network Address Translation and proxy services and servers
   – Secure Socket Layer (SSL) data encryption
   – Redundant, highly available routers and switches
   – Redundant, highly available, and secure servers
   – Redundant, highly available power management
   – Highly available data access via redundant circuits and carriers
   – Regularly scheduled backups, offsite storage and site replication
   – Hardened servers and operating systems
   – Regular vulnerability scanning

2. **Web Server Security:** Web servers use Microsoft IIS and provide additional access security. DocuShare Private Cloud includes the Apache Tomcat Java servlet engine to handle browser (http protocol) requests, and to generate the user interface. IIS provides password protection to the web server and is enabled for SSL. SSL encrypts all transactions over the web between the server and browser, and requires use of an https (secure http) server connection.

3. **DocuShare Private Cloud Application Security:** DocuShare Private Cloud 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 Private Cloud Application Security

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

## DocuShare Private Cloud Account Types

DocuShare Private Cloud provides the following account types:

1. **Guest (User-1):** An anonymous user account that can view unrestricted content on the site.

2. **Read-Only Client Access License (Read-Only CAL):** A registered user account on the DocuShare Private Cloud site that is able to search, read, and download content. Read-only users cannot add new content or modify existing content on the site.

3. **DocuShare Client Access License (DocuShare CAL):** A registered user account on the DocuShare Private Cloud site that is able to search, read, download, add, update, or change content (subject to the access permissions set on content).

4. **DocuShare CPX Client Access License (CPX CAL):** A registered user account on the DocuShare Private Cloud site that is able to perform all DocuShare CAL activities, plus certain operations that are restricted to CPX CAL users (e.g. create workspaces and content rules).

5. **Site Administrators group (Group-1):** A group with at least one member, the site administrator (User-2), whose account is created when DocuShare Private Cloud is installed. Members of this group have full administrative access to the DocuShare Private Cloud site, including accounts, content, and site configuration. The Xerox Cloud hosting and administration teams are members of this group and perform all site administration.

6. **Content Administrators group (Group-2):** A group of registered users that has content administrator privileges to the DocuShare Private Cloud 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.

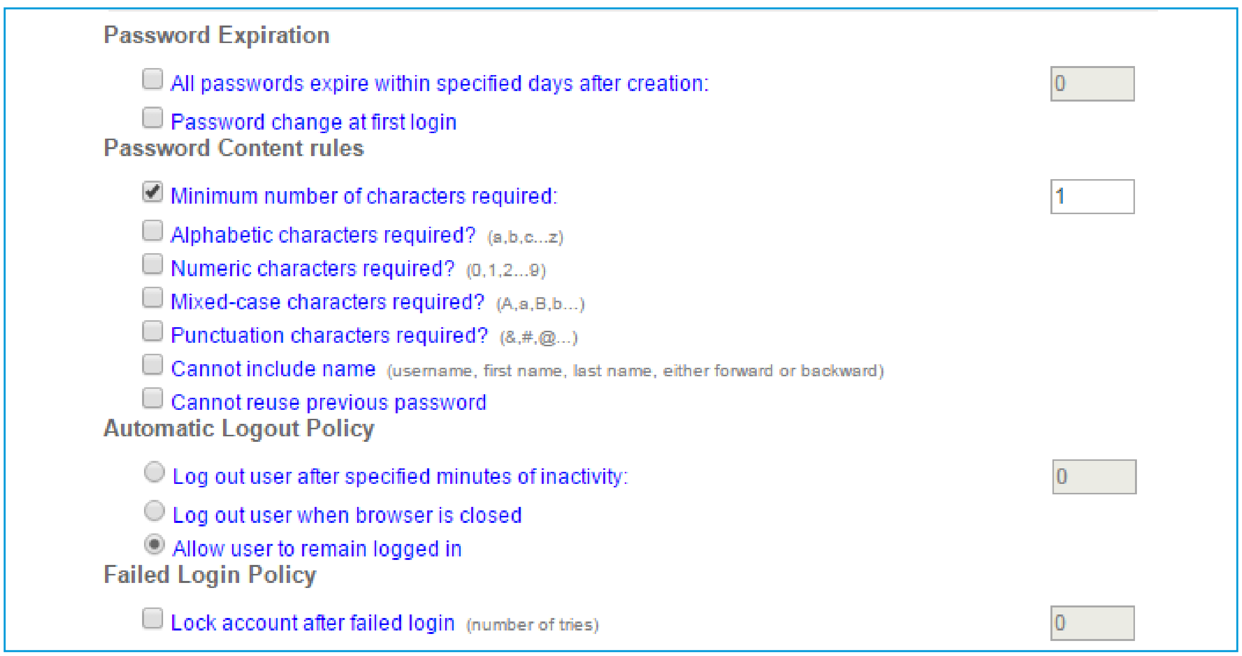
7. **Account Administrators group (Group-3):** A group of registered users that has account administrator privileges to the DocuShare Private Cloud site. Members of this group can create and manage user accounts (Read-Only CAL, DocuShare CAL, and CPX CAL), and set site access policies. The site administrator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

## DocuShare Private Cloud Password Security

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

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

The DocuShare Private Cloud 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.



## Single Sign-On

DocuShare Private Cloud 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 Private Cloud using their LDAP credentials; a separate login is not required. Additionally, network administrators can set password policies on the LDAP/AD server to enforce stronger security measures. It is possible to implement stricter authentication within DocuShare Private Cloud, such as RSA SecurID, by integrating such authentication into the LDAP/AD server.

DocuShare Private Cloud supports both internal and external domains. An administrator can use DocuShare Private Cloud 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 Private Cloud uses cookies to authenticate a user's identity. For each request to DocuShare Private Cloud via a browser, the DocuShare Private Cloud Client, the WebDAV Client, or Guest access, DocuShare Private Cloud distributes an encrypted authorization token to the client. DocuShare Private Cloud internally tracks the number of sessions per client.

Additionally, DocuShare Private Cloud supports persistent cookies, although this is 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 Private Cloud cookie is associated with that user's desktop. When logged into that desktop, the user does not need to log into DocuShare Private Cloud again, even after a restart.

## User Access to Content

Every DocuShare Private Cloud object has an access control list (ACL), which is assigned to the object when it is added to the site. The ACL 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.

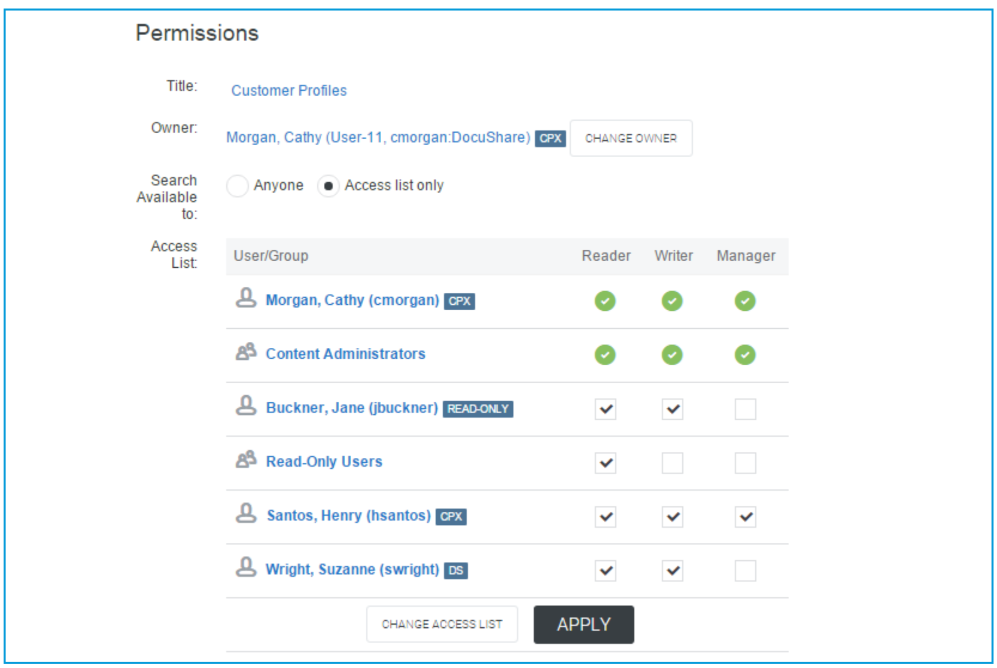
**Three permission site**

- **Reader** allows the user or group to read the content of the object and view its associated properties and permissions.
- **Writer** allows the user or group to change the object's properties and add new objects, including new versions of documents.
- **Manager** allows the user or group to delete the object, and change the object's permissions and owner.

**Six permission site**

- **Read Properties** allows the user or group to view the object's properties and permissions.
- **Read Content** allows the user or group to read the content of the object.
- **Read History** allows the user or group to view 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.

Additionally, users can control whether or not the object displays in a search results list. By default, only accounts in the ACL 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.



## Site-Wide Access Policies

DocuShare Private Cloud 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 Private Cloud 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.


Access Policies

- Use this page to select who has permission to access this site and who has permission to create new accounts on this site.
- Depending on the activity level of your site, changing access policies may take a while to complete. This operation closes all operations that are currently in progress and may generate failure messages for those terminated operations.

| Name | Value |
|---|---|
| Site Access Authority | Guest |
| Registry Access Authority | Guest |
| Account Creation Authority | Guest |
| Group Creation Authority | User |

Reset Apply

## Sophisticated Data Encryption

For added data security, Xerox uses state-of-the-art technology and industry best practices for data encryption during transit to and from the Xerox cloud, as well as while stored within DocuShare.

- Encryption at transfer with high-grade SSL and at rest with 256-bit AES
- Content Delivery Networks for transfer optimization and additional encryption cycle
- Encryption keys are securely stored in separate locations and frequently rotated



Document Version: 1.1 - 08/02/2016. BR12423

xerox®