# Table of Contents

1 Introduction ................................................................. 1
   Product Overview ........................................................... 1
   Xerox® Digital Alternatives Local Server Implementation Types ..... 1
   Xerox® Digital Alternatives End User Client Application ............. 2
   Xerox® Digital Alternatives Central Server .............................. 2
   Reporting Data Communicator ......................................... 2
   How to Use This Guide ....................................................... 2
   Intended Audience .......................................................... 3
   Limits to This Guide ......................................................... 3
   What’s New for Release 1.1 ................................................ 3
   Digital Alternatives Private Cloud Deployment Support ............. 3
   Software Licensing ............................................................ 3
   Compliance and Certification ............................................. 4
   Customer IT Organization .................................................. 4
   Xerox® Managed Print Services Delivery Organization ............ 4
   Ongoing Operational Roles and Responsibilities – Xerox® Digital
   Alternatives Server Maintenance ........................................ 4

2 Architecture ....................................................................... 5

3 Solution / Application Environments ................................. 7
   Hardware and Software Requirements ........................................ 7
   Local Server ........................................................................ 7
   Xerox® Digital Alternatives PC Client Requirements .................... 8
   Xerox® Digital Alternatives iPad Client Requirements ................... 9
   Local Server Deployment Models .......................................... 9
   Xerox® Digital Alternatives Local Server Requirements ................ 10
   Required Resources for All Deployments .................................. 10
   Private Cloud Implementation Considerations ........................... 11
   Establishing Business-to-Business (B2B) Connectivity ................... 11

4 Physical Security .............................................................. 13

5 Access Management ......................................................... 14

6 Access Control ............................................................... 15

7 Identification and Authentication ......................................... 17
8 Data Transmissions .......................................................... 19
9 Auditing and Logging ........................................................ 21
10 Application Timeout .......................................................... 23
11 Application Security .......................................................... 24
12 Business Continuity / Disaster Recovery .......................... 25
13 Data Management / Protection ......................................... 27
   Document Storage ..................................................................................... 27
Figures

Figure 1: Onsite Implementation......................................................................................... 5
Figure 2: Private Cloud Implementation.............................................................................. 6
Introduction

Product Overview

Xerox® Digital Alternatives is a software service supporting the reading, annotating, and sharing of documents digitally. Once a document enters a user’s Digital Alternatives client, it automatically replicates to all of the user’s PC and iPad devices on which the Digital Alternatives client is installed. Users can also share the annotated document with other users via the application as well as by email.

Digital Alternatives is composed of five main component areas.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Xerox® Digital Alternatives Local Server | • Performs authentication tasks  
• Replicates documents to user’s other devices and to other users |
| End User Client Application | • Installs on the end user’s PC and/or iPad  
• Displays documents for review and annotation |
| Internet-based Central Server | • Stores account information and licensing used by the local server and clients |
| User Analytics Reporting Data Communicator | • Transmits usage data to the Digital Alternatives User Analytics reporting platform hosted within Xerox. |
| Digital Alternative User Analytics Reporting | • Uses Digital Alternatives usage information obtained from the Digital Alternatives Local Server to provide analysis of usage benefits to the customer based on industry standard metrics. |

Xerox® Digital Alternatives Local Server Implementation Types

Onsite Implementation

The onsite implementation performs all authentication tasks with the customer’s IT Active Directory® on behalf of the Digital Alternatives user. The user supplies credentials through the Digital Alternatives End User Client Application. Another main task of the Digital Alternatives Local Server is to replicate documents to a user’s other devices as well as to other users with whom the document is being shared. The Digital Alternatives Local Server also performs Global Address Lookup on behalf of the Digital Alternatives End User Client Application when sharing documents with other customer Digital Alternatives users. Additionally, if a document is shared with a non-Digital Alternatives user, the Digital Alternatives Local Server sends the document through the customer’s email server for the Digital Alternatives End User Client Application. The Digital Alternatives Local Server interacts with the Internet-based central server to provide documents upon demand to users who are outside of the customer’s network infrastructure.
Private Cloud Implementation

Xerox hosts the Local Server within the Xerox private cloud network on behalf of the Digital Alternatives customer. In this case, no customer onsite server software installation is necessary and the customer is no longer responsible for managing the physical server, as Xerox assumes this responsibility. With the private cloud deployment, a dedicated VPN connection between the customer network environment and the Xerox private cloud environment is required. Access to the customer’s Active Directory and Exchange LDAP resources from the private cloud application server provided securely through the established VPN connection is also required. The private cloud implementation supports all the same functionality that exists with the onsite, local server implemented implementation.

Xerox® Digital Alternatives End User Client Application

This software, which can be installed on the end user’s PC and/or iPad, displays the document and holds a local copy of the documents being displayed within the user’s local Digital Alternatives document repository. Users go to the client when they want to access their documents.

Xerox® Digital Alternatives Central Server

This component houses the account information and licensing used by the local server and clients. The central server manages the Digital Alternatives customer account that includes the central server generated customer ID for each Digital Alternatives client implementation as well as the associated customer email domain(s) that customers use when accessing their Digital Alternatives accounts. Within this Digital Alternatives customer account, user seat licensing quotas for each implementation are managed. Consult the Xerox® Digital Alternatives Administration Guide for more details on how license management.

Reporting Data Communicator

The Reporting Data Communicator software component, which is separately installed on the Digital Alternatives Local Server, extracts customer user usage information from the Local Server’s reporting database and sends this information to the Digital Alternatives CompleteView User Analytics servers that are hosted within Xerox. The Reporting Data Communicator configuration does not allow the transfer of personally identifiable information to the Digital Alternatives CompleteView User Analytics servers. Consult the Digital Alternatives Data Communicator Installation Guide for more information on Reporting Data Communicator configuration for sending reporting data to Digital Alternatives CompleteView User Analytics servers.

How to Use This Guide

This guide is to help Xerox or Partner presales representatives provide their prospective customer’s IT organizations with security related information on Digital Alternatives, to help in the certification of the deployment of Digital Alternatives within the customer’s
environment. Customer and Xerox personnel can use the guide as part of the presales evaluation, post-sales testing, and acceptance process. Actual test plans and acceptance criteria are dependent upon the formality or required documentation of the customer. This document contains information related to Digital Alternatives’ potential impact to security, enterprise IT infrastructure, network traffic, resources, and required planning.

**Intended Audience**

The customer’s IT, security, and management will use this guide. Before certifying Digital Alternatives, customers, and appropriate Xerox personnel should have a clear understanding of:

- The IT environment at the site where Digital Alternatives will be installed,
  - If the private cloud hosting option is going to be utilized, an understanding of the nature of the VPN connectivity and its security aspects.
- Any restrictions placed on applications that are deployed on that network,
- The Microsoft® Windows Server® operating system, and
- The Microsoft SQL Server® database system.

**Limits to This Guide**

The Digital Alternatives solution is highly configurable and has many features. This guide covers standard implementations and a typical customer IT. If the customer’s IT environment differs from what this guide documents, then the customer’s IT team and the Xerox representative need to identify the differences and resolve any potential concerns.

The guide’s information pertains to the Digital Alternatives 1.1 release. Although much of this information will remain constant through the software’s life cycle, some of the data provided may be revision-specific, and will require periodic updates. IT organizations should check with the Xerox representative to obtain the appropriate version.

**What’s New for Release 1.1**

**Digital Alternatives Private Cloud Deployment Support**

This capability allows Xerox to host the customer’s Digital Alternatives Local Server on Xerox-furnished cloud servers instead of the customer having to furnish the host machines and all of the normal server maintenance responsibilities for this purpose.

**Software Licensing**

Software licensing is managed at the account level and stored in the customer account defined in the Digital Alternative’s Central Server. Neither the End User Client software
application nor the local server are specifically licensed, but rather when a new customer end user logs into their Digital Alternatives account for the first time, the overall available license seat count as managed in the central server is decremented. This initial login of a customer is known as Onboarding. Uninstalling the End User Client software does not increment the allocated license count within the Central Server. You must obtain additional license seats from Xerox once the onboarded customers deplete the available license count on the central server.

Compliance and Certification

Customer IT Organization

Ultimately, it is the responsibility of the customer’s IT organization to certify and accept the deployment and operation of the Digital Alternatives solution within their network environment. The customer may have an informal certification process, which is limited to the review of Xerox® Digital Alternatives documentation and a Xerox demonstration. Or, the customer may have a more formal process that requires actual installation and testing with defined test criteria and test plan. The customer needs to define the certification criteria and work with the Xerox team to define the required steps and timeline.

Xerox® Managed Print Services Delivery Organization

Xerox personnel may participate in the certification process and help determine which Digital Alternatives features and functions are required and the frequency of Digital Alternatives activities.

Ongoing Operational Roles and Responsibilities – Xerox® Digital Alternatives Server Maintenance

As part of the customer certification process, the Xerox account team, also known as the Operations Team, the field analyst who will be part of the initial deployment and ongoing maintenance, and the customer’s IT organization need to define the roles and responsibilities for the ongoing care of the Digital Alternatives software installation:

- Who will be responsible and what is the planned schedule for periodic backups for the SQL Server® database that Digital Alternatives uses in its operation? If the account is unstaffed with Xerox personnel, then the IT organization needs to include the Digital Alternatives database within their periodic database backup schedule, which they may perform on other systems.

- As the responsibility of providing the server hardware falls upon the customer IT management organization, installing periodic Microsoft operating system software updates will be the responsibility of the customer IT organization. Typically, the server that on which Digital Alternatives is installed will have to follow the server software update policies of the customer’s IT organization, but the two parties need to discuss and agree to this standard practice.
2 Architecture

The diagrams below show the two deployment scenarios for the Digital Alternatives local server components. In the onsite scenario, we implement the Digital Alternatives Local Server within the customer’s IT environment, where the customer furnishes the Windows servers, including Microsoft SQL Server. In the private cloud implementation scenario, Xerox provides the hosts and SQL Server within its private cloud network and a VPN connection between the Xerox private cloud network and the Customer’s IT network.

Figure 1: Onsite Implementation

Using the private cloud implementation, we establish a dedicated business-to-business VPN connection needs between the Application Server within the Xerox Services network and the customer’s network environment that provides access by the Application Server to the customer’s Active Directory and Exchange LDAP connections. The VPN connection also allows customer users who have the Digital Alternatives End User Client user software loaded onto their PC and iPad devices to connect to the Application Server when these devices are within the customer network environment.
Figure 2: Private Cloud Implementation
3 Solution / Application Environments

Hardware and Software Requirements

Detailed in the following sections are the software and hardware requirements for the local server and Client software components in the Digital Alternatives solution. In addition, the document focuses on the local server component, but it discusses the PC and iPad components as well.

Local Server

Supported Operating Systems

- Windows® 2008 Standard
- Windows® 2008 Enterprise
- Windows® 2008 R2 Standard
- Windows® 2008 R2 Enterprise
- Windows® 2012 Standard
- Windows® 7

Other Software Required

- Microsoft® .NET Framework v4.5.2
- Windows Task Scheduler

Hardware

- RAM: 8 GB
- CPU: AMD Dual Core 1.20GHZ
- Hard drive: 260GB

The installation requires 50MB of free space.

Install the reporting data communicator on a local server application node.
Xerox® Digital Alternatives PC Client Requirements

Installation

The following are the minimum system requirements for installation:

(Based upon specific system configuration and needs, additional hardware may be required.)

- Supported Operating System:
  - Windows® 7 (Professional, Ultimate, Enterprise)
  - Windows® 7 x64 (Professional, Ultimate, Enterprise)
  - Windows® 8
  - Windows® 8 x64
  - Windows® 8.1 (Professional, Ultimate)
- Office 2007 with SP3 to Office 2013
- Intel® Pentium® 4 Processor
- Physical Memory (RAM): 2 GB minimum (4 GB is recommended)
- Free hard disk space: 250 MB for the application only. Recommend 5 GB minimum for document storage too.
  **Note:** This may increase for users who have many documents.
- Microsoft ® .NET Framework 4.5.2 is required as a prerequisite for all supported operating systems.

Security

- The PC Client uses the customer’s Active Directory Domain Authentication.
- Users will use the same Windows Domain login as on their PC client.
- Requires user to have Internet Explorer configured for proxy server for installer to predetermine customer IT proxy settings for outside central server access.
- Requires that Digital Alternatives Local Server connect to the customer’s domain authentication server(s).

**Note:** After installation Internet access is required for users to:

a. Onboard the Digital Alternatives solution with their client for the first time.

b. Reauthenticate their Digital Alternatives client when their token or password expires.
   - Tokens expire every 8 hours.
Xerox® Digital Alternatives iPad Client Requirements

Installation
• iOS 7 or 8 operating system
• iPad 2 and newer, includes iPad mini™ (with and without Retina)

Security:
• The iPad Client uses the customer’s Active Directory Domain Authentication.
• Requires that Digital Alternatives Local Server connect to customer’s domain authentication server(s).

Note: After installation, Internet access is required for users to:
  a. Onboard the Digital Alternatives solution with their client for the first time.
  b. Reauthenticate their Digital Alternatives client when their token or password expires.
      – Authentication tokens expire every 8 hours.
  c. In order to sync and share you can use either the Internet or customer intranet.

Local Server Deployment Models

Pilot Deployment (1-20 Users)

Small Deployments (100 - 5000 Users)
# Xerox® Digital Alternatives Local Server Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
<th>Desired / Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server</td>
<td>IIS version 7.5</td>
<td>IIS version 7.5 for Server 2008 R2 or IIS version 8 for Server 2012</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>8 GB</td>
<td></td>
</tr>
<tr>
<td>Network COM+ Access</td>
<td>Not needed</td>
<td>Not needed</td>
</tr>
<tr>
<td>Network DTC Access</td>
<td>Not needed</td>
<td>Not needed</td>
</tr>
<tr>
<td>Access Components</td>
<td>Required (bundled w/Microsoft® .NET 4.5.2 Framework)</td>
<td>Required (bundled w/Microsoft® .NET 4.5.2 Framework)</td>
</tr>
<tr>
<td>Microsoft .Net Framework</td>
<td>4.5.2</td>
<td>.NET 4.5.2</td>
</tr>
<tr>
<td>Database Server</td>
<td>Microsoft SQL Server® 2008 R2</td>
<td>Microsoft SQL Server® 2008 Service Pack 3 R2 or SQL Server 2012</td>
</tr>
<tr>
<td>SQL Authentication</td>
<td>Required with admin account access</td>
<td>Required with admin account access</td>
</tr>
<tr>
<td>Server Administrative Rights</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>

## Required Resources for All Deployments

Customer IT needs to provide the following required resources for the Digital Alternatives Local Server.

**SMTP (outbound mail server):** Customer SMTP server information is required for Digital Alternatives Local Server to send share notifications. If the SMTP server needs user authentication, the credentials of the Service Account user credentials are used. The local server uses customer’s existing SMTP interface to customer’s existing MS exchange mail server. Port 25 is the most common setting for interacting with SMTP mail relays for Digital Alternatives, but can be overridden during configuration of the local server based upon customer mail server requirements.

**LDAP Connection for Global Address Lookup:** Primary customer user directory lookup server. This is used to access user email addresses for email owner verification during onboarding. This is also used for Global Address Lookup. By default port 389 is used, unless the customer’s IT department instructs us to use a different port ID.
LDAP Connection(s) for Authentication: Digital Alternatives users are authenticated using Microsoft® Windows Network Domain authentication. The Digital Alternatives Local Server can automatically detect membership in a given domain (using the provided service account), which allows domains and servers to appear automatically in the configuration screen. Otherwise, domains and LDAP connections can be added manually. By default port 389 is used, unless the customer’s IT department instructs us to use a different port ID.

Service Account: Customer IT needs to create a service account for the IIS app pools and the maintenance service to use on the local server. This account needs to be a domain account and have administrative rights on the Digital Alternatives Local Server node(s). If the SMTP server used requires user authentication, the username and password for the service account are used. This Service Account should be exempt from password expiration, as an expired password impacts the operation of the local server. Please refer to the Digital Alternatives Local Server Administration Guide for the correct configuration of the local server service account. This account is required at local server installation time.

Internet Access: Access to the Digital Alternatives Central Server is needed. The required https port is 443.

Private Cloud Implementation Considerations

Establishing Business-to-Business (B2B) Connectivity

With the private cloud implementation, we must establish a dedicated B2B connection between the customer’s network and the Xerox private cloud network in order to secure privacy. Typically this implementation occurs with, but is not limited to, an Internet site-to-site VPN solution establishing a NAT IP address connection between the customer’s firewall and the private cloud’s firewall.

IP Address and Port Number of Customer Active Directory Server

The Digital Alternatives Private Cloud server needs to present the credentials of an onboarding user to the Customer’s Active Directory server, using its Lightweight Directory Access Protocol (LDAP) interface through the B2B connection.

IP Address and Port Number of Customer Exchange Server LDAP Interface

When an end user views their company’s global address book within Digital Alternatives, the local server obtains this information by accessing the customer’s Exchange Server through its LDAP interface. By default port 389 is used, unless the customer’s IT department instructs us to use a different port ID.
Customer IP Address Network Address Translation Rule in Firewall

Because internal IP addresses used by the customer for their network devices may be similar to other customer networks as well as addresses within Xerox, the customer should provide a Network Address Translation (NAT) rule to map their outbound IP address communication to the Digital Alternatives Private Cloud Server. For example, it is common for the customer network devices to use 192.168.1.XXX or 10.10.1.XXX address ranges for internal addressing. Since each customer’s client application communicates to the private cloud server for document synchronization, all of the customer’s outbound traffic appears to Xerox as a single inbound IP source representing all of the customer’s traffic with which the private cloud server needs to interact.

Document Security within Cloud-Based Local Server

Documents imported into Digital Alternatives are stored within the local server as unencrypted PDF files within the local server’s document repository. Access to this document repository, along with the application and database server is restricted to Xerox private cloud IT personnel who require access to administer and maintain these servers. Direct access to the document repository by users or non-authorized Xerox private cloud IT personnel is prevented using Windows permissions specified on the directory containing the documents. Thus, we observe safe practices with respect to document security and personally identifiable information when storing sensitive documents in a cloud-based system.
4 Physical Security

Xerox uses multiple data centers to host its application and data, providing essential redundancy. All data centers employ physical security, strict access policies, and secure vaults and cages. First and foremost, Xerox takes every security measure to make sure confidential information stays that way. We provide administrative, technical, and physical safeguards to help ensure we meet your organizational compliance requirements.

- Data centers use two factor authentication methods, for example biometric entry authentication and secured with 24/7 security resources.
- Uninterruptible power and backup systems, plus fire/flood prevention at storage sites.
- The data centers that host Digital Alternatives Private Cloud are compliant with ISO 27001, HIPAA, PCI-DSS, and SOX guidelines.
- We constantly monitor our private network and perform frequent threat assessments to ensure data protection. Multiple Internet backbone connections provide routing redundancy and high-performance connectivity.
- Digital Alternatives Private Cloud instances are housed in Xerox data centers with secondary disaster recovery sites that are all ISO 27001 compliant:

<table>
<thead>
<tr>
<th>North American Data Centers</th>
<th>European Data Centers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Site</strong></td>
<td><strong>Secondary Site (Disaster Recover)</strong></td>
</tr>
<tr>
<td>Lexington, KY, USA</td>
<td>Sandy, UT, USA</td>
</tr>
<tr>
<td>North York, ON</td>
<td>Toronto, ON</td>
</tr>
</tbody>
</table>

- Secondary disaster recovery sites are activated when their primary sites are down. When activated, the secondary site is restored from the nightly backup of the primary site.
- No customer information or documents are housed in the Microsoft Azure™ environment. For Digital Alternatives Private Cloud, all customer information and documents are stored within Xerox-managed 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.
We constantly monitor our private network and perform frequent threat assessments to ensure data protection. Multiple Internet backbone connections provide routing redundancy and high-performance connectivity.

- Servers reside behind robust firewalls that selectively grant access to network resources on an as required basis.

- External penetration testing ensures system security and validation.

- Intrusion Detection System (IDS) monitors network traffic.

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
Access Control

Xerox private cloud maintains a strategic information security framework based on regular assessments of the threats, vulnerabilities, and business impact to protected information systems from a variety of attackers and contingencies. We review this framework at least biannually. The framework encompasses enterprise-wide information security as well as issues specific to the Digital Alternatives Private Cloud hosting environment. Xerox also maintains a comprehensive set of policies, procedures, and tools to ensure continuous compliance with internal and external security guidelines.

Our production systems are located in our private data center facilities. We monitor and protect production web, application, file, and database servers, along with network equipment. Video surveillance monitors access to our data centers. We use two-factor authentication, such as card readers and biometric scanners, as well as on-site security personnel to control access. We record access to our data centers and require approval along with identity confirmation. 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
7 Identification and Authentication

First and foremost, Xerox private cloud takes every security measure to make sure confidential information stays that way.

Digital Alternatives Private Cloud provides an LDAP connector which enables a site to use a customer’s corporate LDAP or Active Directory server for account management and authentication. When using LDAP/AD, users log into Digital Alternatives Private Cloud using their Windows credentials (domain, user name, and password); a separate login is not required. Additionally, customer network administrators can set password policies on the LDAP/AD server to enforce stronger security measures.
8 Data Transmissions

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

• Encryption at transfer with high-grade SSL and at rest with 256-bit AES using port 443

• Content Delivery Networks for transfer optimization and additional encryption cycle
9 Auditing and Logging

Xerox can provide reporting and audit trails for most actions or activities that occur within Digital Alternatives administration.
10 Application Timeout

Not applicable. When a user session expires on Digital Alternative Client Software, the user will need to reauthenticate.
11 Application Security

We constantly monitor our private network and perform frequent threat assessments to ensure data protection. Multiple Internet backbone connections provide routing redundancy and high-performance connectivity.

- Servers reside behind robust firewalls that selectively grant access to network resources on an as required basis.

- External penetration testing ensures system security and validation.

- Intrusion Detection System (IDS) monitors network traffic.
Xerox maintains backups of all your data as well as redundant hardware to minimize the business impact of hardware failures, site unavailability, natural disasters, or other contingencies. We annually test disaster recovery plans and tools on a live-reference installation of Digital Alternatives.
Data Management / Protection

Document Storage

All Digital Alternatives user documents are maintained on the Digital Alternatives Document Server. The Digital Alternatives Document Server, along with the Local Server and the Database Server, can be on-premise or securely hosted by the Xerox private cloud. Documents are stored unencrypted in the Digital Alternatives Document Server. The documents are stored in a configurable location, which can be any location to which the Digital Alternatives Document Synchronization Service has access. Access to the documents is protected by Windows and Server access on the customer’s domain. As an added layer of protection, actual documents are stored with an obfuscated file name and extension. Documents are not deleted automatically, but rather the users themselves delete documents. There is no automatic document cleanup. Each user has a specific amount of storage allotment for their documents on the Digital Alternatives File Server. No Digital Alternatives user documents are stored on the Digital Alternatives Central Server.