Xerox® Digital Alternatives
Security & Evaluation Software User Guide

October 2016
Version 2.0.xx

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Revision History

Date	Version Number	Description
October 2016	2.0.xx	• After release update regarding email addresses being encrypted
January 2016	2.0	• Includes Digital Alternatives 2.0 new features content
May 2015	1.2	• Includes Digital Alternatives 1.2 Private Cloud deployment capability
March 2015	1.1	• Major reorganization to comply with internal security documentation template • Updates for 1.1 Release, including introduction of cloud support.
August 2014	1.0	Initial Version

Table of Contents

Figures

1 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.

Xerox® Digital Alternatives is composed of five main component areas.

Component	Description
Xerox® Digital Alternatives Local Server	• Performs authentication tasks • Replicates documents to user's other devices and to other users
End User Client Software Application	• Installs on the end user's Windows® PC, iPad® or supported Android™ tablets or Apple Macintosh® computer • Displays documents for review and annotation
Xerox® CompleteView® Reporting Data Communicator	• Transmits usage data from Digital Alternatives local server to the Digital Alternatives CompleteView® reporting platform hosted within Xerox.
Digital Alternative CompleteView Reporting	• Uses Digital Alternatives usage information obtained from the Xerox® Digital Alternatives Local Server to provide analysis of usage benefits to the customer based on industry standard metrics. Hosted within Xerox network.
Internet-based Digital Alternatives Central Server	• Stores account information and licensing used by the local server and clients

Xerox® Digital Alternatives Local Server Deployment Methods

Onsite Implementation

With the onsite implementation method, this component performs all authentication tasks with the client's IT Active Directory® on behalf of the Xerox® Digital Alternatives user. The user supplies credentials through the Xerox® Digital Alternatives End User Client Application. Another main task of the Xerox® 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 Xerox® Digital Alternatives Local Server also performs Global Address Lookup on behalf of the Xerox® 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 Xerox® Digital Alternatives Local Server sends the document through the customer's email

server for the Xerox® Digital Alternatives End User Client Application. The Xerox® Digital Alternatives Local Server interacts with the Internet-based Central Server to provide documents upon demand to users who are outside of the client's network infrastructure.

Private Cloud Implementation

Xerox offers the ability to host 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 method, 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 between the two networks is also required. All Local Server functionality that exists with the onsite implemented local server is equally supported by the Private Cloud implementation method.

How to Use This Guide

This guide is designed 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 Xerox® 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 Xerox® Digital Alternatives' potential impact to security, enterprise IT infrastructure, network traffic, resources, and required planning.

Use this guide primarily during implementation and after contract signature; it can also be used during pre-sales and evaluation activities with a non-disclosure agreement (NDA).

Intended Audience

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

- The IT environment at the site where Xerox® Digital Alternatives will be installed,
  - If the private cloud local server 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 Xerox® 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 Xerox® Digital Alternatives 2.0 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 2.0

Digital Alternatives Version 2.0, offers a number of new capabilities.

- Several built-in document workflows enable customers to process common document workflow tasks such as document review, approval, and signing between Digital Alternatives users.
- The integration with DocuSign® eSignature service allows users to submit documents for signature using their existing DocuSign account for legally accepted digital signatures.
- Digital Alternatives now provides native integration with the Xerox® DocuShare® Content Management Platform that allows documents to be imported and exported from the DocuShare electronic content management solution.
- Additionally, the Digital Alternatives client software is now supported on two new host platforms, Google Android tablets and Apple Macintosh personal computers.

Digital Alternatives Document Processing Workflows

Digital Alternatives provides built-in document workflow management. Users can send documents within Digital Alternatives to another user for review, signing, or approval. Each workflow feature notifies the recipient of a new workflow request. Once the request recipient has completed the requested task, the processed document will automatically be returned to the request originator with a completion date stamp along with any comments from the recipient.

Workflows can be requested of someone outside of the Digital Alternatives system. In this scenario, the document will be sent as an email attachment but will not be returned within Digital Alternatives to the requester when completed.

Integration with DocuSign® eSignature Service

For those customers who have an Enterprise DocuSign electronic signature account, Digital Alternatives users can send a document to a recipient for signing using the sender's DocuSign account. The document will automatically be uploaded to the sender's DocuSign account, where the recipient will receive an email message from DocuSign letting them know of a pending signing request. Once the document has been successfully uploaded to DocuSign, all further processing with the signing request is performed within DocuSign. Once the recipient has processed the signing request, the signed document will not automatically be returned to the sender's Digital Alternatives account but will remain within DocuSign.

Integration with Xerox® DocuShare® Electronic Content Management System

Digital Alternatives can upload and download documents to a configured DocuShare system from within the Digital Alternatives client application. To access DocuShare, the user will need a native DocuShare user account that is independent from the user account used to access Digital Alternatives. Additionally, the Digital Alternatives client application needs to have direct network access to the DocuShare server for the integrated access to work. Thus, using this capability may not be possible for users outside of their corporate network unless their client devices have a VPN connection to their corporate network.

New Client Application Host Platforms – Google Android and Apple Macintosh

The Digital Alternatives client application supports the Apple Macintosh personal computer and certain Google Android tablets in addition to the current Windows PCs and Apple® iPad tablets. Details on which devices the Digital Alternatives client application supports can be found in the Xerox® Digital Alternatives Administration Guide.

Software Licensing

Software licensing is managed at the account level 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. When the available license count is depleted on the Central Server due to customers having onboarded, additional license seats must be obtained from Xerox.

Seat licenses can be reclaimed from one user to another by disabling a user's account in the local server which will prevent them from using Digital Alternatives. Once a user has been disabled, their license allocation for their account will be reclaimed into the available license set count that can be assigned to another new user within the customer account.

Application Compliance and Certification

Implementation - Customer IT Organization

Ultimately, it is the responsibility of the customer's IT organization to certify and accept the deployment and operation of the Xerox® 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.

User data stored within the local servers implemented within the customer's network will not be transferred to servers external to the customer's network, except for the usage data that is exported periodically to Xerox reporting servers, which is an optional component of the offering and is limited to the user data listed in Table 1: User Data Stored in Digital Alternatives.

Implementation – Private Cloud

Xerox is responsible for certifying and accepting the deployment of the Xerox® Digital Alternatives solution within the Private Cloud environment for a given Private Cloud customer. Upon request, Xerox can provide the procedure for this implementation certification and acceptance to customers.

User data stored within the local servers implemented within the Private Cloud network will not be transferred to servers external to the Private Cloud network, except for the usage data that is exported periodically to Xerox® reporting servers, which is an optional component of the offering and is limited to the user data listed in Table 1: User Data Stored in Digital Alternatives.

European customers that choose to use the Private Cloud implementation approach will have their servers located in one of two European hosting facilities listed in Table 2: Private Cloud Hosting Locations.

Implementation - Authorized Xerox® Digital Alternative Service Provider

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

Ongoing Operational Roles and Responsibilities

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 Xerox® Digital Alternatives software installation:

- System Administration Responsibility
  - The responsibility of supporting the server hardware belongs with the client IT management organization. Installing periodic Microsoft® operating system software updates will be the responsibility of the client IT organization.
- Local Server Database and Document Repository Backup Responsibility
  - The Customer IT department will be responsible performing periodic backups for the SQL Server® database that Xerox® Digital Alternatives uses in its operation. The Customer IT department will also be responsible for performing periodic backup of the Document Repository.
- Local Server Hardware Health Monitoring Responsibility
  - The Customer IT department will be responsible for monitoring the hardware and OS health of the local servers, including hardware failures, disk space capacity issues, network connectivity and Operating Systems issues.
- Local Server Software Updates
  - Authorized Xerox® Digital Alternative Service Provider will be responsible for scheduling with the customer IT and performing local server software upgrades as they become available.

2 Architecture

Xerox® Digital Alternatives is composed of five main component areas.

Component	Description
Xerox® Digital Alternatives Local Server	• Performs authentication tasks • Replicates documents to user's other devices and to other users
End User Client Software Application	• Installs on the end user's Windows® PC, iPad® or supported Android™ tablets or Apple Macintosh® computer • Displays documents for review and annotation
CompleteView® Reporting Data Communicator	• Transmits usage data from Digital Alternatives local server to the Digital Alternatives CompleteView® reporting platform hosted within Xerox.
Digital Alternative CompleteView Reporting	• Uses Digital Alternatives usage information obtained from the Xerox® Digital Alternatives Local Server to provide analysis of usage benefits to the customer based on industry standard metrics. Hosted within Xerox network.
Internet-based Digital Alternatives Central Server	• Stores account information and licensing used by the local server and clients

System Components

Xerox® Digital Alternatives End User Client Application

This software, which can be installed on a user's Windows PC, iPad, Android tablet or Apple Macintosh PC, displays the document and stores a local copy of the documents being displayed within the user's local Xerox® Digital Alternatives document repository. Users use the client when they want to access their documents. The local documents cannot be readily accessed without the use of the Digital Alternatives Client application. All documents stored in Digital Alternatives are converted to PDF files. Documents stored within the Client Application are automatically synchronized with the user's local server account. The user has visibility to their documents stored within their account along with document shared to them by other users.

Xerox® Digital Alternatives Local Server Application

The local server application that is installed by an Authorized Xerox® Digital Alternative Service Provider requires access to a SQL Server® database server and the Windows Internet Information Services web server. The Local Server coordinates document exchanges between a user's devices or to other users when a share document request

from one user to another occurs. Each Digital Alternative client application interacts with the Local Server application during user authentication as well as when a document is imported or modified. Hosting the application servers on separate virtual machines is supported.

As user accounts are defined and authenticated using the customer's Active Directory, the credentials a user provides to the client software to be authenticated with are transferred to the local server to authenticate with the customer's Active Directory. This communication between the local server and the customer's Active Directory server is through Lightweight Directory Access Protocol (LDAP).

Reporting Data Communicator Application

The Reporting Data Communicator software component, which is separately installed on the Xerox® 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, hosted within Xerox. The CompleteView reporting servers use this data to provide usage analytics reporting. The Reporting Data Communicator is configured to not transfer Personally Identifiable Information to the Digital Alternatives CompleteView servers. The Digital Alternatives Administration Guide has information on how the Reporting Data Communicator is configured to send reporting data to Digital Alternatives CompleteView User Analytics servers. All reporting for Digital Alternatives is accessed through the Digital Alternatives CompleteView reporting server hosted by Xerox. No reporting is available directly from the Digital Alternatives local server.

The Data Communicator can be configured to exclude Personally Identifiable Information (PII) about users in its upload to the CompleteView reporting server. The Data Communicator can be configured at the server implementation to obfuscate certain data elements considered PII. The table below shows what data elements are sent and which elements are obfuscated if no PII information is to be shared with the Xerox® Digital Alternatives reporting server.

Data Element	Digital Alternatives	Digital Alternatives with no PII
UserID	Sent as is	Sent as is
Username	Sent as is	Obfuscated
Email	Sent as is	Obfuscated
Documents	Sent as is	Sent as is
StorageUsed	Sent as is	Sent as is
Quota	Sent as is	Sent as is
DeviceID	Sent as is	Sent as is
ClientTypeID	Sent as is	Sent as is
Type	Sent as is	Sent as is
ActivityTypeID	Sent as is	Sent as is
ActivitySubTypeID	Sent as is	Sent as is
ActivityID	Sent as is	Sent as is
Key	Sent as is	Sent as is

Data Element	Digital Alternatives	Digital Alternatives with no PII
Value	Sent as is	Sent as is
DocumentName	Sent as is	Obfuscated
Pages	Sent as is	Sent as is
IsColor	Sent as is	Sent as is
DateUTC	Sent as is	Sent as is
Description	Sent as is	Sent as is
ActivityKeyValuePairID	Sent as is	Sent as is
OnboardDateUTC	Sent as is	Sent as is
RecType	Sent as is	Sent as is

Table 1: User Data Stored in Digital Alternatives

The servers are hosted within the Xerox® private cloud hosting facility. Communication to these servers from the Data Communicator is performed using HTTPS secure protocol using port 443. The CompleteView servers provide a secure web interface for authorized users to interact with the CompleteView reporting capability. Users can only view data from those Digital Alternatives accounts they are authorized to view. Data Communicator accounts can only send data to a specific CompleteView account for which they are set up.

Xerox® Digital Alternatives Central Server

The Digital Alternatives Central Server is hosted within the Microsoft Azure cloud network designated for Xerox. Only Xerox® MPS Application Support personnel who are responsible for creating and maintaining customer accounts within Central Server have access to the Digital Alternatives Central Server. All communication to the Central Server by the Local Server and client software is performed through the secure HTTPS protocol interface.

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 customer users use when accessing their Digital Alternatives account. User information held within the Central Server is limited to email addresses, which are encrypted, of those users that have installed the client software and initially logged into Digital Alternatives. No other user information is stored within the Central Server.

Within this Digital Alternatives Customer account, user seat licensing quotas for each implementation will be managed. Consult the Xerox® Digital Alternatives Administration Guide for more details on how license management is performed.

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.

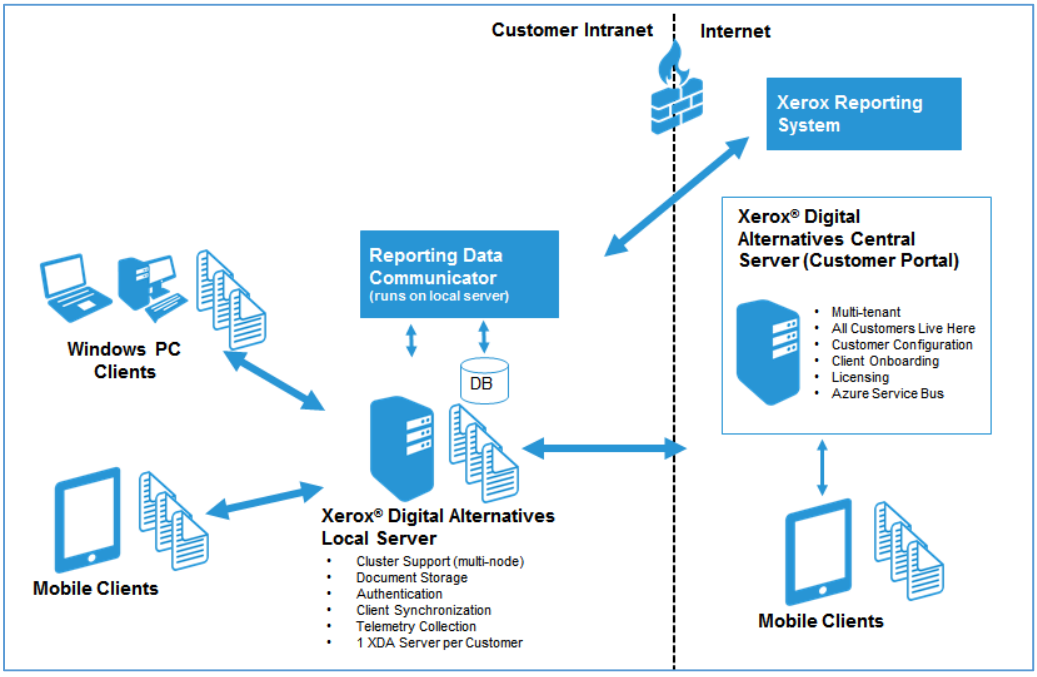

Figure 1: Onsite Implementation

Using the Private Cloud implementation, we establish a dedicated Business -to -Business VPN connection between the Application Server within the Xerox Services network and the customer's network environment that provides access for the Application Server to the customer's Active Directory and Exchange LDAP connections. The VPN connection also allows users who have the Digital Alternatives Client user software to connect to the Application Server from the customer network environment.

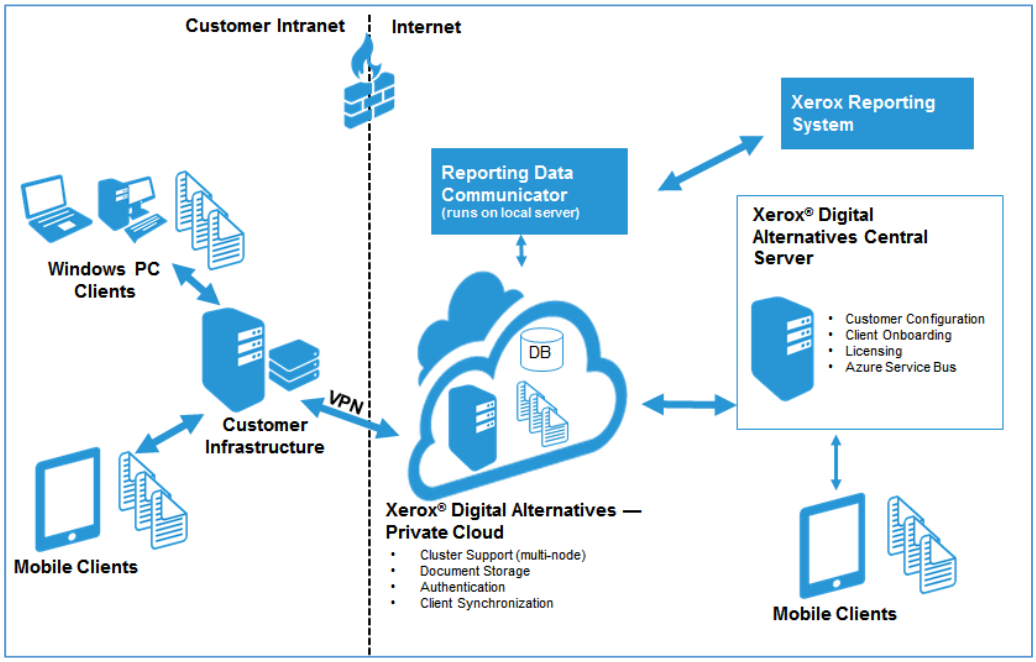

Figure 2: Private Cloud Implementation

Local Server Deployment Models

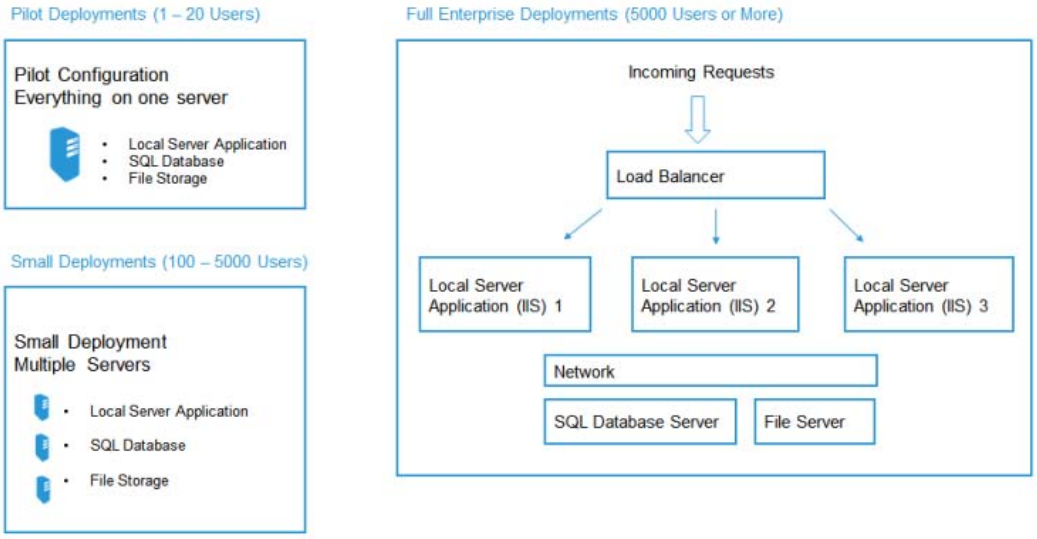

Figure 3: Local Server Deployment Model

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 Installation Requirements

Supported Operating Systems

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

Other Software Required

- Microsoft® .NET Framework v4.5.2
- Windows Task Scheduler
- Microsoft Message Queuing (MSMQ)

Minimum Hardware

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

The installation requires 100 MB of free space for the software, not including document repository storage. Application (web) server must have Server Certificate applied to the server's IIS web server to allow HTTPS protocol for Secure Sockets Layer (SSL) encrypted communication with client applications. All communication between Digital Alternatives application components is through HTTPS protocol.

The reporting data communicator can be installed on a Local Server application node.

Component	Minimum	Desired / Recommended
Operating System	Windows Server® 2008 R2	Windows Server 2008 R2 or Windows Server 2012
Web Server	IIS version 7.5	IIS version 7.5 for Server 2008 R2 or IIS version 8 for Server 2012
Virtual Memory	8 GB	
Network COM+ Access	Not needed	Not needed
Network DTC Access	Not needed	Not needed
Access Components	Required (bundled w/Microsoft® .NET 4.5 Framework)	Required (bundled w/Microsoft® .NET 4.5 Framework)
Microsoft .Net Framework	4.5.2	.NET 4.5.2
Database Server	Microsoft SQL Server® 2008 R2	SQL Server 2012
SQL Authentication	Required with admin account access	Required with admin account access
Server Administrative Rights	Required	Required

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 Xerox® Digital Alternatives Local Server to send share notifications. If the SMTP server needs user authentication, the credentials of the Service Account user are used. The local server uses customer's existing SMTP interface to customer's existing MS exchange mail server. Port 25 (TCP) 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. Default port 389 (TCP) is used unless instructed by the customer's IT to use a different port ID.

LDAP Connection(s) for Authentication: Xerox® Digital Alternatives users are authenticated using Microsoft® Windows Network Domain authentication. The Xerox® 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. Default port 389 (TCP) 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 to be used by the three application maintenance services on the local server as well as the IIS app pools. The three maintenance services that are installed with the local server application are:

- Xerox.Digital.MaintenanceService – responsible for periodically deleting documents marked for deletion by Digital Alternatives users
- Xerox.Digital.QueueService - responsible for interacting with MS Queuing for job execution
- Xerox.Digital.RelayService – responsible for interacting with Central Server for licensing information as well as interfacing with Central Server for remote client document updates

This account needs to be a domain account and have local administrative rights on the Xerox® Digital Alternatives Local Server node(s). If the SMTP server used requires user authentication, the username and password for the service account will be 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 Xerox® 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 Xerox® Digital Alternatives Central Server is needed. The required https port is 443.

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)
  - Windows® 10 (Home, Pro, Enterprise)
- Intel® Pentium® 4 Processor or greater
- 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 that have many documents.

- Microsoft® .NET Framework 4.5 is required as a prerequisite for all supported operating systems.

Security

- Digital Alternatives client application and local server use the customer's Active Directory Domain Authentication
- Users will use their Windows Domain login.
- For the PC client application, the user has Internet Explorer configured for proxy server settings to allow for initial external Central Server access interaction. Interaction between the PC client and the Central Server is through HTTPS protocol using port 443. The customer's proxy server must allow HTTPS protocol communication to the Digital Alternatives' Central Server during initial PC client software installation.
- Requires that Xerox® Digital Alternatives Local Server be connected to customer's domain authentication server(s). This is outlined in the Required Resources for All Deployments section.

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

- Onboard the Xerox® Digital Alternatives client software solution with the Central Server and with their installed Local Server for the first time.
- Reauthenticate their Xerox® Digital Alternatives client with their Local Server when external to their company's Network when their client's security token or password expires. If client application is external and without Internet access, such as in Airplane Mode, the client software will simply not open until Internet connectivity or internal customer network is restore for the client software.
  - Security Tokens expire every 8 hours.

Xerox® Digital Alternatives iPad Client Requirements

Installation

- iOS 7, 8 or 9 operating system
- iPad 2 and newer, includes iPad mini™ (with and without Retina). No iPhone support.

Security:

- The iPad Client uses the customer's Active Directory Domain Authentication.
- Requires that Xerox® Digital Alternatives Local Server be connected to customer's domain authentication server(s). This is outlined in a separate section.

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

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

b. Reauthenticate their Xerox® 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.

Xerox® Digital Alternatives Android Client Requirements

Installation

Supported Android tablet manufacturer and OS versions:

Device	OS Versions Supported
Asus Memo Pad 7	v4.4.2 (KitKat®)
Google (Asus) Nexus 9	v5.0 and v5.1.1(Lollipop)
Google (Asus) Nexus 7	v4.1(Jelly Bean), v4.4.2 (KitKat®), v5.0/5.1/5.1.1 (Lollipop)
Samsung Galaxy Tab 4	v4.4.2 (KitKat®)
Samsung Galaxy Tab S	v4.4.2 (KitKat®), v5.0/5.1/5.1.1 (Lollipop)

Security:

- The Android client application uses the customer's Active Directory Domain Authentication.
- Requires that Xerox® Digital Alternatives Local Server be connected to customer's domain authentication server(s). This is outlined in a separate section.

Xerox® Digital Alternatives Apple Macintosh Client Requirements

Installation

- Supported Apple OS versions: OS X 10.10 ("Yosemite") and OS X 10.11 ("El Capitan")

Security:

- The Apple Macintosh client application uses the customer's Active Directory Domain Authentication.
- Requires that Xerox® Digital Alternatives Local Server be connected to customer's domain authentication server(s).

4 Private Cloud Considerations

Private Cloud Implementation Considerations

Establishing Business to Business (B2B) Connectivity

With the Private Cloud implementation approach, we must establish a dedicated B2B connection between the customer's network and the Xerox® Private Cloud network in order for the customer's local server hosted within the Private Cloud to interact with the customer's Active Directory. Additionally, the Private Cloud VPN allows customer users to interact with the local server hosted in the Private Cloud as if it were installed within the customer's network. A typical implementation includes a site-to-site VPN solution which establishes a private connection between the customer's firewall and the Private Cloud's firewall. There are several considerations to address for an effective Private Cloud VPN implementation.

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. Normally the port number is 389 (TCP), but can be set to whatever the customer IT department has set.

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 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 should appear to Xerox as a single inbound IP source representing all of the customer's traffic to the Private Cloud server with which it 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.

Private Cloud 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. Xerox performs many security measures to make sure that customer confidential information stays confidential. Xerox provides administrative, technical, and physical safeguards to help ensure we meet the customer's organizational compliance requirements.

- Data centers use two factor authentication methods and include biometric entry authentication and 24/7 armed guards.
- Xerox has been issued an SSAE 16 Typle II report.
- Storage sites have uninterruptible power and backup systems, plus fire/flood prevention.
- 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 security and intrusion 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:

North America Data Centers		Europe Data Centers	
Primary Site	**Secondary Site (Disaster Recovery)**	**Primary Sites**	**Secondary Site (Disaster Recovery)**
Lexington, KY, USA	Sandy, UT, USA	Telford, UK	Newport, UK
		Paris, FR	Tours, FR

Table 2: Private Cloud Hosting Locations

- 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.
- The environmental controls employed in the Private Cloud data center are:
  - environmental controls (air conditioning, fire suppression, etc.),
  - redundant/backup power supplies,
  - redundant B2B and B2C network/internet connections.

Private Cloud Access Management

User accounts given access to Private Cloud servers are limited to those users who support the ongoing maintenance of the servers on a need to access basis. Xerox users who are responsible for maintaining the Private Cloud server request access to Private Cloud governance after they have secured approval from their manager. Once Private Cloud Governance has reviewed the request, an approval may be provided. All user access implementation is performed by the Governance-designated implementation team. Access to the customer's database instance and document repository is restricted to a subset of all users provided access to the customer's Private Cloud implementation.

Private Cloud Logical 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.

Customer users are not provided user accounts that would allow them to remote login into their hosted local servers. Only Xerox users who have been identified as needing access to maintain the private cloud servers are given login access to Private Cloud servers.

Private Cloud Identification and Authentication

Digital Alternatives Private Cloud provides an LDAP connector which enables the hosted local server to use a customer's corporate LDAP or Active Directory server for Digital Alternatives user authentication.

Customer users who authenticate into Digital Alternatives on their client software will supply their login credentials to the client software, which are transferred to the local server through the Private Cloud VPN connection. The local server, in turn, authenticates the customer's Active Directory LDAP interface with the supplied credentials through the Private Cloud VPN connection. Once the Customer's Active Directory server validates the credentials, the customer's client software is allowed to interact with the hosted local server.

Private Cloud Data Transmissions

For added data security, Xerox uses data encryption during transit to and from the Digital Alternatives Private Cloud.

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

Auditing and Logging

Upon request, Xerox can provide audit reporting for most actions or activities that occur within Digital Alternatives administration.

User access to local servers are logged within the private cloud servers using standard Windows User Access Logging which logs user access for up two years of history as a default. The user access data is stored locally on the local server and is expected to take less than 80 MB of disk space to store its records.

Upon request, Xerox can provide a text output of the user access logs to the customer.

Application Timeout

User authentication must be renewed every eight hours. When a user session expires on Digital Alternative Client software, the user will need to reauthenticate.

Application Security

Digital Alternatives was developed using Xerox software development standards that include design and code reviews and standard software libraries such as Microsoft .NET framework.

All communications between Digital Alternatives components utilize encryption to help secure customer data.

Business Continuity / Disaster Recovery

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. Disaster recovery includes the site fail-over mapping for each geography as defined in the data center table: Table 2: Private Cloud Hosting Locations.

5 Data Management / Protection

Document Storage

All Xerox® Digital Alternatives user documents are maintained on the Xerox® Digital Alternatives Document Server. The Xerox® Digital Alternatives Document Server, along with the Local Server and the Database Server, can be on premise, or securely hosted by Xerox in the cloud. Documents are stored unencrypted in the Digital Alternatives Document Server. Access to the documents is protected by Windows and Server access on the client's domain and restricted to limited number of personnel within the Xerox hosting facility. As a layer of protection, actual documents are stored with an obfuscated file name and extension. Documents are not deleted automatically, but rather by the users themselves. There is no automatic document cleanup. Each user is allotted a specific amount of storage for their documents on the Xerox® Digital Alternatives File Server (user quota setting in Admin UI). No Xerox® Digital Alternatives user documents are stored on the Xerox® Digital Alternatives Central Server.