

Software Version 1.0
Version 1.0
702P03957



Xerox[®] PrintSafe Software

Information Assurance Disclosure



Xerox® PrintSafe Software Copyright © 2015 Xerox Corporation. All rights reserved.
Xerox®, Xerox and Design®, Xerox Extensible Interface Platform® are trademarks of
Xerox Corporation in the United States and/or other countries.

Microsoft®, Windows® and SQL Server® are either registered trademarks or trademarks
of Microsoft Corporation in the United States and/or other countries. BR 16543

Contents

Introduction	1
Purpose	1
Target Audience	1
Disclaimer	1
System Workflows	2
Overview	2
Authentication Methods	3
Card Access	3
PIN Access	4
Confirmation Number Access	5
LDAP Access	6
Desktop Printing	7
Print Queue Submission	7
Document Release	8
Administrative Workflow	11
Auto Registration Workflow	11
Secondary PIN Logon	11
Confirmation Number Logon	12
LDAP Logon	12
Network Appliance Details	13
Models	13
External Authentication Details	14
Security Description	15
Component Communication	16
Protocols and Port numbers used by the system	17
System Components	20
Xerox® PrintSafe Software Services	20
Job Agent Service / PrintSafe Client	20
Xerox® PrintSafe Software Database	22
Email Server	22
Printer	22
Xerox® PrintSafe Software User	22
LDAP Server	23
System Component Interfaces	23
Users and Xerox® PrintSafe Software	23

User and Email Server Communication	23
Email Server and PrintSafe Server Communication.....	24
PrintSafe Server and Printer Communication.....	24
PrintSafe Server and Job Agent Service / Client Communication.....	25
User Workstation and Print Server Communication	26
Job Agent Service / Client and Print Communication.....	26
Administrator configuration and usage of the PrintSafe Server.....	26
Microsoft SQL Server Compact database deployment	26
Microsoft SQL Server external database deployment	26
PrintSafe Server Windows file structure	27
Print Server Communication.....	27
LDAP Authentication	27
Active Directory Import	27
Roles.....	29
Customer Supplied Network.....	29
Xerox Role	29
Customer Role	29

Introduction

Xerox® PrintSafe Software is a workflow solution that controls user access to a Xerox® Multifunction Printer (MFP). This solution also supports Desktop Printing, allowing printing to a common queue with the ability to release jobs to any printer. This reduces waste from uncollected jobs and provides security for sensitive information, since jobs are only printed when the user is standing at the printer.

Purpose

The purpose of this document is to disclose information for the Xerox® PrintSafe Software with respect to system security. *System Security*, for this paper, is defined as follows:

- How print jobs are received, accessed, and transmitted
- How user information is stored and transmitted
- How the product behaves in a networked environment
- How the product may be accessed, both locally and remotely

Please note that the customer is responsible for the security of their network and the Xerox® PrintSafe Software does not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the Xerox® PrintSafe Software relative to Information Assurance (IA).

This document does not provide tutorial level information about security, connectivity, PDLs, or Xerox® PrintSafe Software features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

It is assumed that the reader is familiar with the Xerox® PrintSafe Software workflows; as such, some user actions are not described in detail.

Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

System Workflows

Overview

The Xerox® PrintSafe Software supports two primary workflows / features.

- **Authentication** – Defined as customers who require validation of user access to MFPs before device usage is allowed at the “All Services” screen. Card-based is the most widely used authentication method. User name and PIN-based login at the device is an alternate method of login when card readers are not installed, or are not functional. Authentication as a standalone option provides device security access only, for the customer who does not require print jobs associated with their network login.
- **Desktop Printing** – Xerox® PrintSafe Software supports the Print / Release feature using two printer server models. One is a traditional printer server model, where jobs are printed to a network print queue and held there until the user authenticates themselves at a printer and releases their job(s). The other is a server “light” printer model, where jobs will be held / retained on the user’s client PC, until the issuer identifies themselves at a printer and releases their jobs, at which time the jobs are sent from the user’s PC directly to the printer.

Authentication methods:

- **Card Access** – User can scan or swipe a proximity card or magnetic stripe card using a card reader connected directly to the printer via USB.
- **PIN** – User can enter an assigned Primary PIN which may be the number read from their card, or an assigned number if the site does not use identification cards or card readers.
- **Confirmation Number** – User can optionally log in to the device using a system-generated confirmation number automatically created by the server and emailed to the user.
- **LDAP** – User can enter their LDAP Domain credentials (user name and password), for validation against the LDAP (Domain) server.

Optional - Secondary Authentication:

The PrintSafe Server supports the ability to enable a Secondary PIN feature, requiring the user to supply a second PIN in addition to their card, primary PIN, or confirmation number.

Desktop Printing:

- **Print Queue Submission** – There are two types of Print Queues used for Xerox® PrintSafe Software.
 - **Network Queues** – These are traditional print server queues. Jobs are sent to a network printer, where they are converted to a PDL (Postscript, PCL, etc.) and stored on the print server until they are released to a printer. A job ticket (descriptor) is sent to the PrintSafe Server.
 - **Client Queues** – Jobs are stored on the local user’s PC workstation and a job ticket is sent to the PrintSafe Server. This solution requires the end user to install the PrintSafe Client on their workstation.

- **Document Release**

- **Printer Client (EIP) App** – Users must access the PrintSafe Client Application (EIP) to release their print job.
- **Auto Release via Authentication** – Print jobs are automatically released to a printer when a user is authenticated. This feature also supports the option to prompt the user during logon, giving them the option to choose if they want to release all of their jobs, or leave them in the queue (for a subsequent logon session, or to manually release them via the Printer Client Application).
- **Auto Release via a Network Appliance** – Print jobs are automatically released to the printer associated with the network appliance and reader when the user scans their card. This feature is typically used with printers that do not support EIP, including non-Xerox devices.

The common link between the submission and release methods is the PrintSafe Server. Documents are stored in the solution until they are deleted, or until an administrative time-out has passed.

Installation, setup, and configuration of all tools are assumed to be similar to installing and configuring any other application and are not addressed in this document. Refer to the *Xerox® PrintSafe Software Installation Guide* and the *Xerox® PrintSafe Software Administration and Configuration Guide* for details.

Subsequent sections will detail the authentication methods, the print submission methods, document release, and document storage in the PrintSafe Server.

Authentication Methods

Card Access

The user is assumed to already be in the PrintSafe Server database, that is, they are an existing user.



Step 1: The user scans or swipes their card at the printer.



Step 2: The printer sends the card data to the server.



Step 3: The server initiates an authentication session with the printer.



Step 4: The printer asks the server to provide the initial screen data to be displayed as part of the logon session.



Step 5: The server validates the card data and informs the printer of the status—logon or failure.



Step 6: The printer displays the logon status. If the user is authenticated, then the user interface is unlocked and the user can access the features and pathways of the printer.

PIN Access

The user can enter an assigned Primary PIN.



Step 1: The user selects the Alternate Login button from the blocking screen on the printer.



Step 2: The printer tells the server to start a new session.



Step 3: The server initiates a new session with the printer.



Step 4: The printer asks the server to provide the first screen to be shown to the user during the logon session.



Step 5: The server sends over the details for PIN prompt.



Step 6: Print displays the PIN entry screen. The user enters the PIN and the printer sends the data to the server.



Step 7: The server validates the PIN and returns results to the printer.



Step 8: The printer displays the logon status. If the user is authenticated, then the user interface is unlocked and the user can access the features and pathways of the printer.

Confirmation Number Access

The user can optionally log in to the device using a system generated confirmation number.



Step 1: The user selects the Alternate Login button from the blocking screen on the printer.



Step 2: The printer tells the server to start a new session.



Step 3: The server initiates a new session with the printer.



Step 4: The printer asks the server to provide the first screen to be shown to the user during the logon session.



Step 5: The server sends over the details for confirmation number prompt.



Step 6: The printer displays the confirmation number entry screen. The user enters the confirmation number and the printer sends the data to the server.



Step 7: The server validates the confirmation number and returns the results to the printer.



Step 8: The printer displays the logon status. If the user is authenticated, the user interface is unlocked and the user can access the features and pathways of the printer.

LDAP Access

The user can enter their LDAP Domain credentials (user name and password).



Step 1: The user selects the Alternate Login button from the blocking screen on the printer.



Step 2: The printer tells the server to start a new session.



Step 3: The server initiates a new session with the printer.



Step 4: The printer asks the server to provide the first screen to be shown to the user during the logon session.



Step 5: The server sends the details for the Network User Name prompt.



Step 6: The printer displays the Network User Name entry screen. The user enters their user name and the printer sends the data to the server.



Step 7: The server sends the details for the Network Password prompt.



Step 8: The printer displays the Network Password entry screen. The user enters their password and the printer sends the data to the server.



Step 9: The server validates the network credentials with the LDAP Server / Domain Controller.



Step 10: The server sends the authentication results to the printer.



Step 11: The printer displays the logon status. If the user is authenticated, the user interface is unlocked and the user can access the features and pathways of the printer.

Desktop Printing

Print Queue Submission

Network Queues



Step 1: The user prints a document via their normal print mechanism (e.g., File > Print) from an application, selecting a PrintSafe printer (queue). Print job attributes, such as color, 2-sided, stapling, and so on, can be selected based on the capabilities of the driver installed and configured for the print queue.



Step 2: Using the Microsoft SMB Protocol, the job is sent to the print server hosting the print queue where it is converted to a PDL (e.g., Postscript or PCL) based on the configured driver. Then the PDL is sent to the PrintSafe port monitor attached to the printer, which stores the file on the server.



Step 3: The Job Agent Service running on the print server detects the new job and parses it to determine the job details, creating an XML description that is stored alongside the job. The Job Agent Service then notifies the PrintSafe Server of the existence of the new job along with the job details, such as number of pages, color, 2-sided, and so on.



Step 4: The PrintSafe Server updates its job list with the details of the new job. This includes the location of the print server where the job is stored.

Client Queues



Step 1: The user prints a document via their normal print mechanism (e.g., File > Print) from an application, selecting a PrintSafe printer (queue). Print job attributes, such as color, 2-sided, stapling, and so on, can be selected based on the capabilities of the driver that was installed and configured for the print queue.



Step 2: The job is converted to a PDL (e.g., Postscript or PCL) based on the configured driver. Then the PDL is passed to the PrintSafe port monitor attached to the local printer, which stores the file in the PrintSafe directory on the local workstation.



Step 3: The PrintSafe Client running on the workstation detects the new job and parses it to determine the job details, creating an XML description that is stored alongside the job. The PrintSafe Client then notifies the PrintSafe Server of the existence of the new job along with the job details, such as number of pages, color, 2-sided, and so on.



Step 4: The PrintSafe Server updates its job list with the details of the new job. This includes the location of the workstation where the job is stored.

Document Release

Printer Client (EIP) App



Step 1: The user authenticates themselves at the printer using Xerox® PrintSafe Software, or one of the printer-supported authentication mechanisms, for example, Network Authentication using LDAP.



Step 2: The user selects the PrintSafe Printer Client Application (EIP). The printer requests the EIP URL.



Step 3: The server responds with browser content.



Step 4: The Print Client (EIP) App queries the printer to determine the identity of the logged on user and sends the identity to the PrintSafe Server with a request to retrieve the user's job list.



Step 5: The PrintSafe Server retrieves the job list for the current user and sends the list to the Print Client (EIP) App to be displayed.



Step 6: The Print Client (EIP) App displays the job list.



Step 7: The user selects one or more jobs, modifies the desired job attributes (if applicable), and selects the "Print" button. The selected jobs and attributes are communicated to the PrintSafe Server.



Step 8: The server checks its job list and notifies the appropriate PrintSafe Client or Job Agent Service about the job to be released, any modified job attributes, and the identity (IP address) of the printer where the job is being sent.

Note: For jobs managed by the Job Agent Service, the PrintSafe Server will send a push notification of the job release request. For jobs managed by PrintSafe Client, the PrintSafe Server will queue up the notification for the next time the agent polls the server for any jobs to be released.



Step 9: The Job Agent Service receives the release notification, or the PrintSafe Client polls the server for jobs to be released. If the job attributes are to be changed, the print ready file is modified. Then the job is transferred to the requested printer via LPR or Port 9100 (Raw IP), and the job history is updated. If the job should be deleted, it is removed from the system.



Step 10: The job prints at the selected printer and the user retrieves their output. The user exits the Print Client (EIP) App and logs out of the printer.

Auto Release via Authentication



Step 1: The user authenticates themselves at the printer using Xerox® PrintSafe Software.



Step 2: At the completion of the authentication process, the server checks its job list for any jobs matching the user name of the logged on user. For all matching jobs, the server looks in its job list and notifies the appropriate PrintSafe Client or Job Agent Service about the job to be released, any modified job attributes, and the identity (IP address) of the printer where the job is being sent.

Note: For jobs managed by the Job Agent Service, the PrintSafe Server will send a push notification of the job release request. For jobs managed by PrintSafe Client, the PrintSafe Server will queue up the notification for the next time the agent polls the server for any jobs to be released.



Step 3: The Job Agent Service receives the release notification, or the PrintSafe Client polls the server for jobs to be released. If the job attributes are to be changed, the print ready file is modified. Then the job is transferred to the requested printer via LPR or Port 9100 (Raw IP), and the job history is updated. If the job should be deleted, it is removed from the system.



Step 4: The job prints at the selected printer and the user retrieves their output and logs out of the printer.

Auto Release via a Network Appliance



Step 1: The user scans their card at the USB reader attached to the network appliance.



Step 2: The network appliance sends the card data to the PrintSafe Server.



Step 3: The server receives the card data, and validates that the request is coming from a known (mapped) network appliance. The network appliance looks up the card number in the user database to find a matching PIN number and retrieves the associated user name for that PIN.



Step 4: The server checks its job list for any jobs matching the user name of the logged on user. For all matching jobs, the server looks in its job list and notifies the appropriate PrintSafe Client or Job Agent Service about the job to be released, any modified job attributes, and the identity (IP address) of the printer to which the job is to be sent.

Note: For jobs managed by the Job Agent Service, the PrintSafe Server will send a push notification of the job release request. For jobs managed by PrintSafe Client, the PrintSafe Server will queue up the notification for the next time the agent polls the server for any jobs to be released.



Step 5: The Job Agent Service receives the release notification, or the PrintSafe Client polls the server for jobs to be released. Then the job is transferred to the requested printer via LPR or Port 9100 (Raw IP), and the job history is updated. If the job should be deleted, it is removed from the system.



Step 6: The job prints at the selected printer and the user retrieves their output and logs out of the printer.

Administrative Workflow



Step 1: The administrator logs in to the PrintSafe Admin website. Administrators can configure solution behaviors and manage devices, users, and jobs.

Administrator functions:



- Configure solution
- Manage printers
- Manage users
- Manage jobs
- Manage licenses
- View audit log

Auto Registration Workflow

This mechanism controls whether the user can register their card themselves through an onboarding / validation process, or if the system administrator must do so through the PrintSafe Admin webpage. This feature can be found at: *Company > Policies > Security > Print Authentication > Basic > Auto Registration*. The supported values for this feature are:

- **Disabled** - The user cannot register their own card. It is expected that the system administrator has manually populated the user entries with the appropriate PIN / card number, added them via CSV import of the user database, or imported them via LDAP import.
- **LDAP Authentication** - If the PrintSafe Server is configured to access an LDAP server for user information, the user's card may be associated with their PrintSafe account by providing LDAP credentials at the PrintSafe-configured MFP the first time they swipe their card. On subsequent logon sessions, the user only needs to scan their card. They will not need to re-supply their LDAP credentials as part of accessing the printer using a card or badge.

Secondary PIN Logon

For environments that want a higher level of security when accessing a printer, the Xerox® PrintSafe Software provides the option to enable a Secondary PIN. This effectively enables a two-factor logon method. For instance, the user would need to first scan their badge, and then provide the Secondary PIN to gain access to the multifunction printer. This feature works in conjunction with the following authentication mechanisms:

- Card Access
- PIN Access (Alternate Login)
- Confirmation Number Access (Alternate Login)

The Secondary PIN feature does NOT work with LDAP Access, since the user is already entering two pieces of information.

The Secondary PIN is a numeric value with a minimum length of 4 digits. The administrator can modify the minimum length from 4 to 8 digits. There is no maximum length.

Users define their own Secondary PINs during the logon process. If this feature is enabled, the next time the user logs on to the multifunction device, they are prompted to create a Secondary PIN. This value is stored and used for subsequent logon sessions. Thereafter, the user is expected to supply the same Secondary PIN during the logon sequence. If the user forgets their PIN, or they would like a new one, the administrator can clear the current value; forcing the user to create a new Secondary PIN the next time they access the printer. Only the user knows the Secondary PIN. The administrator does not have access to view this value.

Confirmation Number Logon

The Alternate Login feature can be configured to support confirmation numbers as a logon mechanism. This is an auto-generated number that is emailed to the user. The length of the confirmation number is 1 to 10 digits, with the default set to 6 digits. In the event that all numbers for the configured length have been used, the system will generate numbers for the configured length+1. For example, if the configured confirmation number length is 3 and all numbers from 0-999 have been assigned to a user, the next auto generated number will be 4 digits long.

The Confirmation Number feature applies Card Swipe access, including Auto Registration. If a user scans their card and if the Confirmation Number feature is enabled, if that user does not have an assigned confirmation number, one will be generated and sent to the user. If that user does not have an email address, they are prompted to supply one as part of the logon sequence. If the user does not supply an email address, they are not allowed to proceed with the logon sequence.

Confirmation numbers are NOT generated when users are added via these methods:

- Manual User Creation using the PrintSafe Admin webpage
- CSV Import
- LDAP Import

The administrator has the option to manually create a new confirmation number for a user using the Action drop-down list on the Users tab. A new confirmation number is emailed to each selected user.

The confirmation number is never visible to the administrator. Only the user knows the value of their confirmation number.

Confirmation numbers can be configured to have a limited lifespan. This improves the security of the system. The enablement for confirmation number expiration can be found at: *Company > Policies > Security > General*. When enabled, the administrator can set the expiration period from 30 to 365 days. When a confirmation number expires, a new one is generated by the server and emailed to the user.

LDAP Logon

The Alternate Login feature can be configured to support LDAP credentials as a logon mechanism. This feature requires the user to supply their domain user name and password to

log in to the printer when using Alternate Login. This makes for a secure logon mechanism that is typical of many PC logon workflows at customer sites.

Note: The LDAP password is never stored as part of the Xerox® PrintSafe Software.

Network Appliance Details

Held print jobs are released automatically as soon as the user scans a card at a mapped network appliance associated with the printer.

Network appliances are small network boxes that attach to the network and permit the Xerox® PrintSafe Software to control the release of user documents to printers that do not support the use of Xerox® Secure Access / Convenience Authentication. A network appliance is configured on the network by the administrator, the appliance is associated with the particular printer in the PrintSafe Admin webpage, and the user can release their jobs at the printer by swiping their card using the card reader associated with the printer. One network appliance is required for each printer.

Models

Three network appliance models are supported by the Xerox® PrintSafe Software:

- RF Ideas Ethernet 241
- Elatec TCP Conv2
- Elatec TCP Conv

Each of these models is available by default on the PrintSafe Admin webpage at *Company > Settings > Network Appliances > Models*. If any or all of these models are not going to be part of your site installation, they can be disabled to turn the listeners off on the server.

The listeners use these default ports:

- RF Ideas Ethernet 241 - 2001
- Elatec TCP Conv2 - 7777
- Elatec TCP Conv - 7778

The default ports can be changed by the administrator if the network appliances on your system have been configured to use a different port. Any firewall on the PrintSafe Server must be configured to allow communication through the port(s).

By default, the network appliances support communication using non-encrypted channels. Therefore, card data is sent in plain text format when transmitting the card data from the network appliance to the PrintSafe Server. The RF Ideas Ethernet 241 is the only network appliance that supports encryption (using SSL) of the communication path.

Note: The Ethernet 241 supports SSLv3. It does not support TLS1.x.

External Authentication Details

The Xerox® PrintSafe Software supports the ability to work with other authentication solutions. When used with these other products, PrintSafe must be configured to support Desktop Printing and the Print Client (EIP) App must be installed. Authentication support should not be enabled, or it will interfere with the other solution.

Users can authenticate themselves at the multifunction device using the configured authentication mechanism. This is done using one of the multifunction device built-in authentication mechanisms (e.g., Network Authentication using Kerberos or SMB), or by using a third party solution. After identifying themselves, users can select the Xerox® PrintSafe Software Printer Application at the user interface, which queries the printer to obtain the logged on user's network user name, and then displays the user's set of pending jobs.

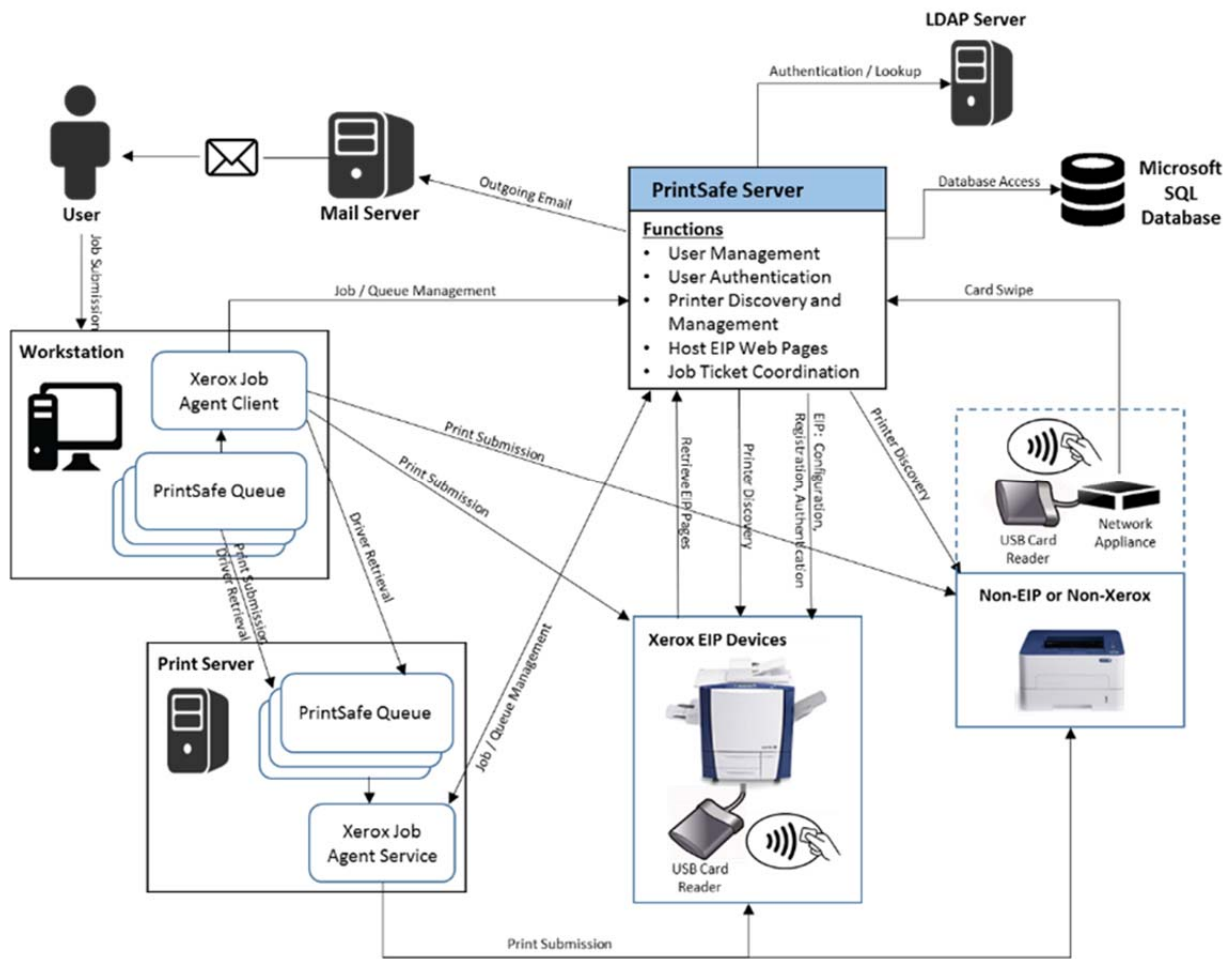
Note: The user name obtained from the session **MUST** match the user name sent to the print queue, that is, the network name found in the print ready files. If the user names do not match, the user will not see their print jobs.

Known issues:

- The use of Smartcard Authentication—done natively via the printer—is not supported as an external authentication mechanism.

Security Description

The architecture of the Xerox® PrintSafe Software incorporates technical controls to eliminate, where possible, information security risks from all information assets including software components, connected system components, and information owners. The figure below illustrates the relationship between the Xerox® PrintSafe Software and these other system components. The base of the arrows indicates the system or touch point that initiates the contact.



Xerox® PrintSafe Software Architecture

The following sections describe the components in the system and the interfaces between the components.

Note that this solution has been designed to offer flexibility and tailored account configuration while still maintaining a secure baseline configuration. Items that are configurable are reviewed in this document, while the methods regarding how to configure these items are not discussed in this document. From a system point of view, the administrator has control over which printers are enabled for Xerox® PrintSafe Software and which users are allowed to use Xerox® PrintSafe Software.

Component Communication

All communication between components is encrypted except where noted.

Communication	Encryption Details
PrintSafe Server and Printer	SNMPv1 and v2 are used by default and do not support encryption. SNMPv3 may be used if supported by the printer, which does use encryption. EIP webpages are retrieved by the printer using HTTP. EIP APIs for registration (HTTP) and authentication (HTTP/S). Raw TCP socket communication from network appliance to the PrintSafe Server containing card data. Uses ports 2001, 7777, and 7778. Encryption available only with the RFIdeas Ethernet 241 using port 2001.
PrintSafe Server and Customer Email Server	Email servers can be configured for both secured and unsecured connections. If the server supports secure connections, Xerox® PrintSafe Software can be configured for secure communication.
User PC and PrintSafe Server	HTTP/S communication with the print server to retrieve configuration and manage the queue.
User PC and Print Server	Uses Microsoft SMB File Sharing and Printing. Encryption depends on Microsoft file and print sharing settings.
User PC and Printer	LPR and port 9100 (RAW) printing do not support encryption.
Print Server and Printer	LPR and port 9100 (RAW) printing do not support encryption.
Print Server and PrintSafe Server	HTTP/S communication with the print server to retrieve configuration and manage the queue.
PrintSafe Server to Xerox Corporate Licensing System	HTTP/S communication using SSL over port 443.
PrintSafe Server and Customer LDAP Server	LDAP (Port 389 – default) or LDAPS (Port 639) communication for authentication and user import. Encryption is optional.

This section captures the security considerations and implementation of Xerox® PrintSafe Software in the following areas:

- Protocols and port numbers used by the system
- Individual system components
- Communication between system components
 - Email Server and PrintSafe Server communication
 - PrintSafe Server and Printer communication
 - PrintSafe Server administration
 - Microsoft SQL Server Express database deployment
 - PrintSafe Server Windows NTFS file structure permissions

Protocols and Port numbers used by the system

The following table lists the standard default ports used for many of the protocols with Xerox® PrintSafe Software. Some port numbers are configurable in the Xerox® PrintSafe Software such as the POP and IMAP ports. Other port numbers are non-configurable and cannot be changed. You may need to change some port numbers depending on the server you are communicating with or use the default ports if they cannot be changed. All ports used must be unblocked in the firewall used on the solution server.

Protocol	Default Use Port Value	Use	Option	Direction
Web Administration Communication Ports:				
HTTP	TCP 80	Hyper-Text Transfer Protocol. (Not encrypted)	Non-configurable	Inbound
HTTP/SSL	TCP 443	HTTP over SSL. If a certificate is already configured on the IIS default website, it will be used by the Xerox® PrintSafe Software. If no certificate is configured, the Xerox® PrintSafe Software will create a self-signed certificate. The administrator has the option to load a certificate from a trusted authority later, if needed.	Non-configurable	Inbound
Database Communication Ports:				
SQL	TCP 1433	Microsoft SQL Client to Server Communication for database queries and storing.	Non-configurable	Outbound
Email Communication Ports:				
Exchange Web Services	TCP 443	Exchange Web Services uses this port.	Configurable	Outbound
SMTP	TCP 25	Simple Mail Transfer Protocol is the foundation for all email transport in Exchange 2000. (Not encrypted)	Configurable	Outbound

Protocol	Default Use Port Value	Use	Option	Direction
SMTP/SSL (Secure SMTP)	TCP 465	SMTP over SSL. TCP port 465 is reserved by common industry practice for secure SMTP communication using the SSL protocol.	Configurable	Outbound
NRPC (Domino)	TCP 1352	Lotus Notes RPC. This is the API used between Lotus Notes and the Lotus Domino server. Communication between the Xerox® PrintSafe Software and Lotus Notes is via a local API on the same PC.	Non-configurable	Outbound
Printer / Printing Communication Ports:				
LPR	TCP 515	Fallback printing port if port 9100 is not accessible. From Xerox® PrintSafe Client or Service to Printer. (Not encrypted)	Non-configurable	Outbound
AppSocket RAW or Windows TCP-mon	TCP 9100	Common communications port used for RAW printing. (Not encrypted)	Non-configurable	Outbound
SNMP	161	Printer Discovery and Configuration. From PrintSafe Server to Printer. (SNMPv1/v2 not encrypted. SNMPv3 is encrypted)	Non-configurable	Outbound
SMB Print	TCP 445	Print submission to a network queue. Client Workstation to print server.	Non-configurable	
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download. From Workstation Print Queue to print server or from PrintSafe Client to print server.	Non-configurable	Outbound
HTTP	TCP 80	EIP Service Registration (between printer and PrintSafe Server)	Non-configurable	Outbound
HTTP/S	TCP 443	EIP Authentication (between printer and PrintSafe Server)	Non-configurable	Both
HTTP	TCP 80	EIP Application Webpage Retrieval	Non-configurable	Inbound
LDAP Server Authentication / User Import Ports:				
LDAP	TCP 389	Lightweight Directory Access Protocol uses this port. (Not encrypted)	Configurable	Outbound
LDAP with SSL	TCP 636	Lightweight Directory Access Protocol with Secure Sockets Layer uses this port. This service does not support a TLS configuration. (Encrypted)	Configurable	Outbound
PrintSafe Internally Used Ports:				
PrintSafe Server to Server	8800	Xerox® PrintSafe Software uses this port to communicate with other PrintSafe Servers. (Encrypted)	Configurable	Both

Protocol	Default Use Port Value	Use	Option	Direction
Network Appliance Used Ports:				
Card Data	2001 7777 7778	Card data sent from an associated network appliance and reader. (The RF Ideas Ethernet 241 can support SSL. Elatecau devices do not encrypt the card data).	Configurable	Incoming
Xerox Job Agent Client / Service Ports:				
HTTP	8800	Configuration, Job Information, Print Release	Non-configurable	Incoming (Client) Both (Service)

System Components

Xerox® PrintSafe Software Services

The PrintSafe Server is the foundational component of the Xerox® PrintSafe Software used to manage the system's behavior and the user's interaction within the system, from authentication to document submission to print. PrintSafe Server is a Windows® application running on a Windows® server. Xerox® PrintSafe Software will conform to the customer's existing security policies, using Windows authentication to access this application. Access to the server should be limited to system administrators and authorized Xerox personnel.

User's documents are received and stored for secure release on the PrintSafe Server. The PrintSafe Server monitors and works in conjunction any enabled print servers running the Job Agent Service, as well as any client workstations running the Xerox Job Agent Client.

Xerox® PrintSafe Software Administration Services

The Xerox® PrintSafe Software administration services run on the PrintSafe Server to provide configuration and authentication, as well as user, printer, and job management.

The administrator interacts with the administration services via a web browser interface to perform tasks such as configuring the system, managing users, and registering printers. Connection to the administration services is supported via HTTP (Port 80) or HTTPS (Port 443). By default, the PrintSafe Server uses a self-signed certificate for HTTPS communication.

Note: Most web browsers will generate a warning when using the self-signed certificate as it was not generated by a trusted authority. The administrator has the option to load and use a certificate from a trusted authority on the PrintSafe Server.

By default, the Xerox® PrintSafe Software supports auto-registration. If the customer site uses LDAP or Domain controllers, then auto-registration allows the user to scan their badge via a connected USB card reader at a PrintSafe-enabled printer. The user would then provide their LDAP authentication credentials to validate their identity, resulting in the addition of that user and their relevant LDAP information (name, email, network user name) in the PrintSafe user database. If auto-registration is not used, there are other options to create and manage users, including: Manual Updates, CSV Import, and LDAP Import.

All submitted jobs are stored and referenced based on the user's network user name and email address. The user's jobs are stored in the print server's Windows file system, or on the client with a randomized file name.

Unprinted jobs are deleted based on an administrator configured retention period. The default retention period is one day.

Job Agent Service / PrintSafe Client

The Xerox® PrintSafe Software is modular in design, leveraging a core PrintSafe Server component, as well as one or more additional components referred to as the Job Agent Service

and the PrintSafe Client. The Job Agent Service runs on the print server and is included as part of the install of the Xerox® PrintSafe Software. For customers who want to use an external print server, they can install the Job Agent Service on one or more external servers to create a distributed or regional system of print servers. For environments that want to forego a traditional print server, they can instead install the PrintSafe Client on each user's workstation.

Document Storage and the PrintSafe Port Monitor

All printers (queues) configured for Xerox® PrintSafe Software use the PrintSafe Port Monitor. Part of the Windows print path, this monitor accepts a print ready file (e.g., Postscript or PCL) and writes it to disk. The location where the file is written is configured using the PrintSafe Admin webpage of the PrintSafe Server. The print ready file and some descriptor files are temporarily stored to the print server or client workstation system disk while the files are active. Upon release to a printer, the Job Agent Service or PrintSafe Client removes the associated files.

As with any Microsoft server OS, the deleted documents follow traditional MS Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself, but are overwritten as the system reclaims the disk space. The Xerox® PrintSafe Software provides no facilities to erase the documents.

Job Agent Service

The Job Agent Service is a Windows service installed on a print server used in conjunction with Xerox® PrintSafe Software. The service can run on the same server running the Xerox® PrintSafe Software, or it can run on one or more external print servers. When installed on an external server, the Job Agent Service starts a listening service and waits for the PrintSafe Server to enable it to perform job management. The Xerox® PrintSafe Software administrator must add the print server IP Address to the list of print servers, effectively enabling the Job Agent Service to begin communicating with the PrintSafe Server. The messaging between the PrintSafe Server and PrintSafe Client consists of:

- Reporting of available printers (Queues)
- Enablement of printers (Queues)
- Job Information – Reporting of new jobs and their details
- Notification of job release to an enabled printer
- Results of job transfer to a printer
- Periodic job synchronization

PrintSafe Client

The PrintSafe Client is a Windows service installed on a client workstation used in conjunction with Xerox® PrintSafe Software. When installed on the client, the PrintSafe Client must be pointed to the PrintSafe Server via the inclusion of a configuration file or via a Service Registry setting which can be pushed to the workstation via the customer IT organization. The PrintSafe Client is responsible for managing print queues and print jobs on the client workstation. The messaging between the PrintSafe Server and PrintSafe Client consists of:

- Querying the server for configuration (e.g., polling intervals, timeouts, etc.)
- Querying the server for the list of printers (Queues)

- Installing or removing printers (Queues)
- Job Information – Reporting of new jobs and their details
- Polling for job release to an enabled printer
- Reporting of job transfer to a printer
- Periodic job synchronization

Xerox® PrintSafe Software Database

Microsoft SQL CE 4 database is used by Xerox® PrintSafe Software as the default relational data store. However, Xerox® PrintSafe Software can be configured to work with an external Microsoft SQL database.

Email Server

The email server is used to send emails to the Xerox® PrintSafe Software user. The preferred implementation is to leverage the client's established email infrastructure and email security in place; however, the mail server can be an internally or externally managed server. The email infrastructure is used if the administrator configures the Xerox® PrintSafe Software to support Alternate Login via confirmation numbers. When enabled, the server generates a numeric confirmation number for the user. This is an auto-generated number that is emailed to the user and can be used when accessing a printer in place of a badge or ID.

Printer

The printer can represent any printing device connected to your network. Throughout this document, we use a Xerox® multifunction device with an EIP control panel interface, unless otherwise noted.

Xerox Extensible Interface Platform® (EIP)

Xerox® multifunction devices introduce a flexible Xerox proprietary platform called EIP. This platform acts as a secure embedded web service that other applications can leverage to expose functionality and services to the user through the local control panel interface. Xerox® PrintSafe Software uses this platform to secure access (authenticate or identify a user) and present users with the Xerox® PrintSafe Software Printer Application.

Network Appliance

The network appliance, sometimes referred to as an ID Controller, is an external hardware device that supports the ability to plug in a USB keyboard mode card reader and transfer card information to a configured application. In this case, the Network Appliance is configured to send card data to the PrintSafe Server.

Xerox® PrintSafe Software User

The Xerox® PrintSafe Software user is an end-user attempting to print a document using the application from a mobile device, laptop, or desktop PC to a printing device on the corporate

network. It is assumed that the client's security policy and systems have already authorized the user to use corporate facilities.

LDAP Server

Xerox® PrintSafe Software can be configured to use an LDAP server (Domain Controller) to control user access. Interfacing with LDAP can occur in several different scenarios:

- Auto Registration of Cards – Users can register a new card with Xerox® PrintSafe Software by scanning it at a USB-connected reader and providing their LDAP login credentials. If the credentials are valid, the user is added to the system and their card number (PIN) is assigned to that new user.
- Alternate Login – The Alternate Login feature gives users the ability to provide their LDAP (Domain) login credentials to access the printer.
- LDAP Import – The Xerox® PrintSafe Software can be configured to import users from LDAP into the PrintSafe user database.

System Component Interfaces

Users and Xerox® PrintSafe Software

Users can be added, deleted, or modified in the Xerox® PrintSafe Software. Refer to the *Xerox® PrintSafe Software Administration and Configuration Guide* (latest version) for details.

The user interacts with the printer to:

- Authenticate and identify themselves
- Release documents to print
- Retrieve the printed documents

Note: For a description of any specific Xerox® printing device's Xerox Security Information, Bulletins, and Advisory Responses see www.xerox.com/information-security.

User and Email Server Communication

The PrintSafe Server communicates to the end user via email messages sent through the customer's email server. The PrintSafe Server creates a confirmation email message whenever a new confirmation number is generated for the user. The confirmation email message contains a personal confirmation number. The confirmation number is later used to authenticate the user at the multifunction device and / or to retrieve and print their documents at the printer.

Confirmation codes are configurable in length, and unique for each user. Once assigned, the confirmation code is reused for an authentication attempt by the user. Users can ask the administrator to reset their confirmation code at any time.

Email Server and PrintSafe Server Communication

Network communication between the email server and the PrintSafe Server is configured using the PrintSafe admin webpage.

For security:

- The PrintSafe Server requires a customer supplied user name and password to access the mail server. The credentials are stored within the SQL database.
- The communication port is configurable.
- Network communication between the servers can be configured to be encrypted using SSL.

Xerox® PrintSafe Software can send emails to the user and act as a standard email client.

The PrintSafe Server supports connectivity to the following:

- SMTP – Port 25 or 587
- Microsoft Exchange Web Services – Port 80 or 443 (SSL)
- Lotus Domino NRPC – Port 1352

Using the protocols above, Xerox® PrintSafe Software uses the outbound email configuration for sending email. Xerox® PrintSafe Software can connect to a MS Exchange Server 2007 or later using Exchange Web Services (EWS). This connection is made over the HTTPS protocol. When communicating with Domino, Xerox® PrintSafe Software communicates using a local API with Lotus Notes Client installed on the same PC as Xerox® PrintSafe Software, which in turn uses Notes RPC to communicate with the Domino server.

Xerox® PrintSafe Software can authenticate either using basic authentication or impersonation.

In the case of basic authentication, the user name and password are sent securely to the EWS server for authentication.

When impersonation is used, the Xerox® PrintSafe Software will log on as the impersonated user for the duration of the EWS connection. The impersonated user must have log on credentials to access the Xerox® PrintSafe Software.

PrintSafe Server and Printer Communication

Discovery

Discovery applies to all printers that are enabled to work with Xerox® PrintSafe Software.

The server connects to the printer via SNMP (Port 161) to retrieve printer configuration. The SNMP communication is done either via SNMPv1/v2 (no encryption) or SNMPv3 (encryption).

Printer (EIP) Application

The Printer Application is only supported by Xerox® multifunction devices that support the EIP browser.

Xerox® PrintSafe Software connects to the printer's web services to install the PrintSafe EIP application on Xerox® printers via port 80 over HTTP.

Xerox® PrintSafe Software can host webpages to the printing device's user interface commonly referred to as Xerox Extensible Interface Platform® (EIP). The device must be enabled to display these webpages and the webpages do not have any access to documents or any data residing on the printing device. All data exchanged is over port 80 via HTTP (default).

Authentication

Authentication is only supported by Xerox® multifunction devices that support the EIP Convenience Authentication API.

The server configures the authentication feature on the printer via SNMP (Port 161). The SNMP communication is done via SNMPv1/v2 (no encryption) or SNMPv3 (encryption).

During user authentication, the PrintSafe Server and the printer communicate using web service calls to initiate an authentication session, supply card data, and / or prompt the user to supply credentials or other data, and unlock the device for user access. All data exchanged is over port 443 via HTTPS.

Network Appliance

For those printers that do not support EIP or the Convenience Authentication API, release of print jobs must be done using a network appliance with an attached USB Card Reader.

The network appliance and the PrintSafe Server communicate via raw TCP sockets with proprietary data exchange based on the manufacturer of the appliance.

Elatec: The Elatec TCP Conv and TCP Conv2 use ports 7778 and 7777 respectively. The card data is sent in plain text.

RF Ideas: The RF Ideas Ethernet 241 uses port 2001. By default, the card data is not encrypted, but the option to use encryption is available.

PrintSafe Server and Job Agent Service / Client Communication

Job Agent Service Start Up

When the Job Agent Service is first installed, the software listens on port 8800 using HTTP for initial configuration information from the PrintSafe Server. Once the administrator adds the IP address of the external print server to its list of supported servers, the PrintSafe Server will push the communication endpoint to the Job Agent Service. This endpoint is used for all communication between the Job Agent Service and the PrintSafe Server.

Xerox Job Agent Client Configuration

The PrintSafe Client periodically polls the PrintSafe Server using the configure endpoint with HTTP on port 8800. This includes the retrieval of timers for job polling, configuration polling, and maintenance polling.

Job Management

Both the PrintSafe Client and the Job Agent Service communicate with the PrintSafe Server to communicate new jobs being added to the system, jobs to be released, job status, and job synchronization. This is done via web service calls using HTTP over port 8800. The Job Agent Service listens for notifications from the server about jobs to be released. Conversely, the PrintSafe Client polls for this information. The reporting of new jobs and job status is always initiated by the PrintSafe Client. For the Job Agent Service, communication is two-way.

User Workstation and Print Server Communication

The user workstation communicates with the print server in two ways:

- Print queue and driver install
- Print submission

Print queue install can be initiated via the PrintSafe Client, or via the Windows print install wizard if print queues are added manually. Printing is done via traditional shared network printers. These capabilities use DCE/RPC communication over port 1058 and SMB communication via port 445.

Job Agent Service / Client and Print Communication

When a job is released for printing, the Job Agent Service / Client submits a print ready file to the printer. The default submission method is port 9100 over TCP/IP. Port 515 (LPR) can also be used.

Administrator configuration and usage of the PrintSafe Server

Accessing the PrintSafe Admin webpage use the standard browser based NTLM protocol for web authentication. This access protocol requires a user name and password for client authentication and is supported by most browsers.

During installation of the Xerox® PrintSafe Software, the MPAdmin user group is created.

Windows user accounts that are members of the Administrator and / or MPAdmin groups on the PrintSafe Server have access to the PrintSafe Admin webpage, but not user accounts.

Microsoft SQL Server Compact database deployment

During the installation of the PrintSafe Server, an SQL Server CE database is created in the install location. Access to this database is restricted through file permissions.

Microsoft SQL Server external database deployment

During the installation of the PrintSafe Server, a database is created in the specified SQL database instance. In order to create this database, the user who installs Xerox® PrintSafe

Software must have permissions to create databases and database logins, and grant permissions. During the installation, Xerox® PrintSafe Software grants the PrintSafe system account “Domain\ComputerName\$” the rights to update the created database.

PrintSafe Server Windows file structure

The PrintSafe Server stores files in the install location: %ProgramData%\Xerox\XMP

Print Server Communication

When the Xerox® PrintSafe Software is configured to use multiple servers (e.g., a failover system), the servers communicate via TCP/IP over ports 8801 and 8802.

LDAP Authentication

When Xerox® PrintSafe Software is configured to enable Alternate Login using LDAP, the user is prompted to enter their credentials at the user interface of the printer. This is done using the EIP Convenience Authentication API. The credentials are sent from the printer to the PrintSafe Server over port 443. The PrintSafe Server performs an LDAP login using the supplied credentials. Passwords are temporarily stored in the SQL database in encrypted format during session creation, and are marked as deleted when the user logs out. They are then removed upon the next scheduled SQL data retention clean-up process. By default, the system uses SASL when doing an LDAP bind.

In order to communicate with Active Directory, Xerox® PrintSafe Software uses the Active Directory Services Interfaces (ADSI) technology available in all Windows operating systems supported by Xerox® PrintSafe Software. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if SSL is being used.

Active Directory Import

Xerox® PrintSafe Software can be configured to import users from Active Directory. This capability is an extension of the setup used for LDAP/ADS Authentication. The PrintSafe Admin has the ability to configure the type of LDAP access (Anonymous, Basic, Negotiate) required when connecting the LDAP server. By default, the system is configured to use the Negotiate setting, which instructs the PrintSafe Server to use SASL when doing an LDAP bind.

The administrator must supply user credentials to be supplied to the LDAP server when performing an import, assuming they have selected either Simple or Negotiate for the Usage Mode. The credentials are stored in the PrintSafe Server database (SQL), and encrypted using DES with MD5 hashing.

As part of the import, the PrintSafe administrator can define the LDAP containers that are queried as part of the import and map the fields within those containers to fields within the PrintSafe user database.

In order to communicate with Active Directory, Xerox® PrintSafe Software uses the Active Directory Services Interfaces (ADSI) technology available in all Windows operating systems

supported by Xerox® PrintSafe Software. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if SSL is being used.

Roles

Customer Supplied Network

Even the most secure systems are vulnerable to someone who has the right knowledge, access, and enough time. Threats include physical damage to the system and over networks, as well as damage caused by viruses. The goal is to minimize the security risks as much as possible, and have policies in place to detect and reduce the negative impact of a security incident. Examples of how to reduce risks include using logins and passwords properly, restricting network access, and using virus detection software.

Xerox Role

Xerox strives to provide the most secure software product possible based on the information and technologies available, while maintaining product performance, value, functionality, and productivity.

Xerox will:

- Run industry standard security diagnostics tests during development to determine vulnerabilities. If found, the vulnerabilities will either be fixed, minimized, or documented.
- Monitor, notify, and supply (when necessary) security patches provided by third party software vendors used with the Xerox® PrintSafe Software.

Customer Role

Although the Xerox® PrintSafe Software product support team tries to provide software that is secure, the customer is ultimately responsible for securing their environment to meet their specific security needs. Depending on the customer needs, the customer can increase security by installing a firewall, implementing a private network, and / or physically securing the hardware to a limited access area. The customer, depending on their needs, should use tools to monitor and log physical and network access to the PrintSafe hardware and software to determine if and when a security incident has occurred. The customer should also back up their data to ensure that it can be recovered in case of deletion or corruption.

In implementing a security strategy, customers must keep in mind that they should not modify the Xerox® PrintSafe Software system or its environment in any way that prevents it from functioning properly. If the customer performs such modifications, Xerox will not be able to support the product should problems occur. The customer may be responsible for returning the Xerox® PrintSafe Software product back to the original installed state. This may include uninstalling unsupported software, resetting configuration settings, or possibly reinstalling the Xerox® PrintSafe Software.

