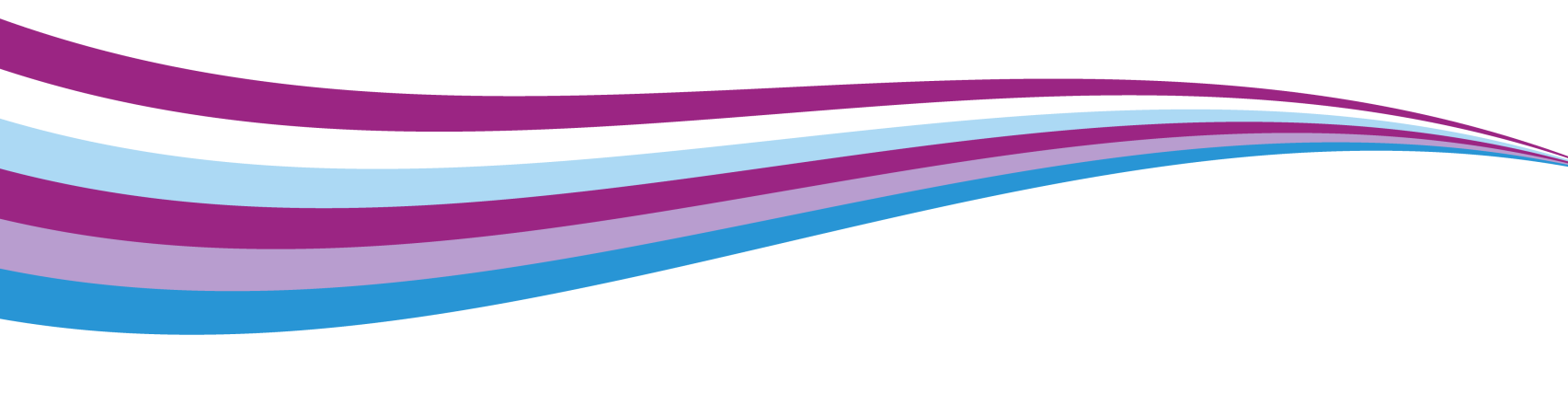
|  |
| --- |
| Xerox**®** MFP Connector for OnBase  Security Documentation Guide |



This document is a guide to help product management draft information security specifications sheets and marketing materials for internal and client distribution. This guide provides a list of general information security topics, features and functionality typical included as part of software applications and solutions.

This guide is not an all-inclusive list of security components, but has been put together to guide you through the high-level architecture and components that should be included in your documentation.

Introduction

The **Xerox® MFP Connector for OnBase** allows for convenient ad-hoc scanning of paper based documents into the Hyland OnBase, Electronic Content Management system.

The connector was built using Software Development Kits (SDK) currently available for Xerox Extensible Interface Programming (EIP) and Hyland OnBase, in order to tightly integrate Xerox Multi-Function Printers (MFP) with Hyland OnBase. The connector inherits Security Considerations and Best Practices as defined for each of the three key components, and the reader is encouraged to consult the appropriate documentation from the respective vendors for further detail. Security information for Xerox products can be found at <http://www.xerox.com/security> .

**Software suite and version**

This document applies to version 1.x of the **Xerox® MFP Connector for OnBase.**

**Type of solution**

The solution runs on a customer supplied windows server as a web service.

**Compliance & Certification**

The **Xerox® MFP Connector for OnBase** complies with all requirements of EAR99 classification

Architecture

* The application runs under IIS on a Windows 2008R2 or 2012 server
* Users do not directly access the application. It is accessed by a Xerox MFP
* The application may make use of ports 80 and/or 446 for communication with MFPs.
* The application may make use of ports 21, 22, and/or 445 for document image transport

**Application Architecture Diagram**

****

Solution / Application Environments

* The application runs under IIS on a Windows 2008R2 or 2012 server
* Users do not directly access the application. It is accessed by registered Xerox MFPs.
* The application may make use of ports 80 and/or 446 for communication with MFPs.
* The application may make use of ports 21, 22, and/or 445 for document image transport
* The application operates within the native Windows firewall system

Physical Security

This connector is installed within the customer’s environment behind their firewall.

Access Management

* User configuration is managed through the Hyland OnBase software and is subject to OnBase security

Access Control

* User access is managed through the Hyland OnBase software and is subject to OnBase security.

Identification and Authentication

* User authentication is managed through the Hyland OnBase software and is subject to OnBase security as configured by the OnBase administrator
* The application allows two different authentication techniques between the connector and OnBase:
  + Device Authentication  
    The device itself is registered as a user within OnBase. Any user authorized to use the MFP will select the onscreen button and have the ability to upload documents as the device user.
  + User Authentication  
    The individual is required to authenticate by entering a User Id and password that is configured within OnBase. The user Id may be entered by the onscreen keyboard or via a badge swipe.
* Each MFP can be configured to use one of the two configuration options

Data Transmissions

* Application information is transmitted between the MFP and the application server using either HTTP (port 80) or HTTPS (443).
* Image files are transferred between the MFP and the EIP connector server using either SMB, FTP or SFTP. The transfer protocol is configurable by the system administrator.
* The application may make use of ports 21, 22, and/or 445 for document image transport between the MFP and server.
* Image files and keyword data is transferred between the application server and the OnBase server using either HTTP (port 80) or HTTPS (443).

Auditing and Logging

Solution / application logging capabilities and describe how to configure to produce a security audit log

* A user audit log is enabled/disabled by the system administrator. When enabled, user audit logs are created daily and are managed by the administrator.
* The user audit log tracks the user access time, user name, scan queue, and document type transmitted to OnBase as well as a success/failure indicator
* An application debug log is enabled/disabled by the system administrator. When enabled, application debug logs are created daily and are managed by the administrator.

Application Timeout

Application timeout is managed by the Xerox Multi-Function Printer (MFP) and is configurable by the MFP administrator. Please reference the Xerox website: [www.xerox.com](http://www.xerox.com), and go to the product section.

Application Monitoring

Application performance is recommended to be added to customer’s monitoring practices.

Database Connections

This application does not connect to a database.

Application Security

* The application follows Xerox recommended secure coding practices
* The application makes use of industry standard .NET 4.0, C# programming procedures.
* The application contains no open source code.
* Other than the Hyland OnBase interface, the application contains no 3rd party source code.

Web Services

The application functions as a web service exposed to Xerox MFPs.

The application makes use of the Hyland OnBase MFP API.

Business Continuity / Disaster Recovery

Whereas the Xerox® MFP Connector for OnBase resides on a customer maintained server, it is subject to the customer Business Continuity and Disaster Recovery policies and procedures

Server Management

The application runs on a customer provided and maintained server

Data Management / Protection

* Data is passed to Hyland OnBase software for storage and archival.
* Scanned document images are retained in the temporary storage buffer for no more than 24 hours.
* The temporary storage buffer is secured by the administrator via server administration best practices.
* Exposure of transient storage data on Xerox MFPs can be managed through MFP features such as Disk Overwrite.
* The installation of OnBase Connect itself, adds no PI to an existing server or printer. Users are encouraged to check their own policies and procedures regarding the scanning of documents with PI.

