Xerox® ConnectKey™ Share to Cloud

Why Xerox for your cloud-based services and applications?

Xerox® ConnectKey™ Share to Cloud: Security Solutions

Product Overview

Xerox® ConnectKey Share to Cloud (STC) provides organizations with powerful document-scanning capabilities that connect multifunction printers (MFPs) to the most popular cloud-based services and applications. As a server-less application, Xerox® ConnectKey Share to Cloud requires very little software configuration or IT involvement, offers a user interface that sets a new standard for ease-of-use, and is priced and licensed to allow companies to instantly acquire and deploy the system.

Document capture products have a proven track record spanning more than 15 years in the document imaging industry and deploy solutions into markets with stringent security and compliance requirements, including financial services, legal, government and healthcare organizations worldwide. Xerox® ConnectKey Share to Cloud follows this best-in-class security legacy and has been designed to support enterprise-class security requirements for cloud-based applications.

Xerox® ConnectKey Share to Cloud security features focus on three key areas:

- User Authentication
- Cloud Server Security
- Transmissions to/from Cloud Servers

User Authentication

Xerox® ConnectKey Share to Cloud is deployed as an embedded application on the control panel of a networked MFP. As these devices are often accessible to a variety of people, authentication is required to identify the user and ensure only authorized users can access functionality at the MFP.

When a user accesses Xerox® ConnectKey Share to Cloud from the MFP or scanner control panel, the application retrieves the user's login information entered to unlock the device panel. Xerox® ConnectKey Share to Cloud is compatible with most of the popular login services that a user will find at the MFP or scanner panel—including PIN code, network credentials and ID cards. This allows organizations to leverage the security policies they already have in place to control user activity at networked MFPs and scanners.

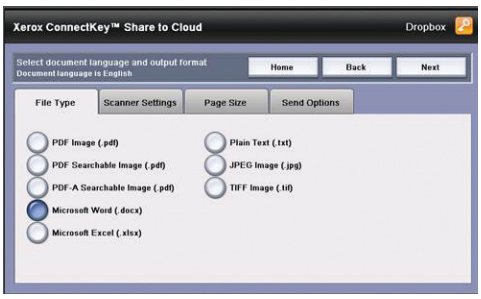
To summarize, Xerox® ConnectKey Share to Cloud takes advantage of the existing security policies already in place for using networked MFPs or scanners, while streamlining user workflows to provide the most intuitive experience possible.

Xerox® Share to Cloud and OmniPage® Cloud Service (OCS) Server Security

Xerox® ConnectKey Share to Cloud does not require any on-premise software installation and instead utilizes cloud server technology to deploy the application, execute Share workflows and convert scanned images into editable word processing documents, spreadsheets and searchable PDF documents. This powerful document conversion capability is performed using the OmniPage Cloud Service, a hosted optical character recognition (OCR) service. The Xerox® ConnectKey Share to Cloud Server connects the MFP or scanner to the desired cloud service, allowing for transmission of scanned images to popular cloud services such as Google Docs™, Evernote® and Salesforce.com®. The server also offers a number of helpful features—such as file splitting and quota notifications—to improve the user experience and make the scanning process even easier. Both the Xerox® ConnectKey™ Share to Cloud server and OmniPage® Cloud Service are hosted on the Microsoft® Windows Azure™ platform. Windows Azure runs in data centers managed and operated by Microsoft Global Foundation Services (GFS). These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24x7 continuity.

Supports popular cloud repositories.

Securely log in on the MFP directly to your preferred cloud repositiory.



Scan direct from the MFP to Word, Excel, PDF, image or plain text.

Windows Azure also incorporates security practices at the application and platform layers to enhance security for application developers and service administrators. For more information on Microsoft Azure security visit:
http://www.windowsazure.com/en-us/support/trust-center/security/

In addition to the server level security provided by Microsoft Azure, Xerox® ConnectKey Share to Cloud ensures that no user data is captured or retained by the application except at the user's request. Private information, such as "Remember Me" credentials that are stored on behalf of the user, is encrypted and stored using Microsoft Azure's secure table storage.

All temporary files are deleted from the OmniPage DCS and STC servers upon success or when they are attached as part of a failure notification. Furthermore, all data is purged by overwriting the disk locations multiple times with random characters permanently destroying its contents.

Transmissions To/From the Share To Cloud Server

As more and more data is exchanged via the Web, it has become more important than ever to transmit data over the Internet using secure connections.

There are three main routes that documents can take when using Xerox® ConnectKey Share to Cloud:

1.) MFP to Xerox® ConnectKey Share to Cloud

2.) Xerox® ConnectKey Share to Cloud Server to OmniPage Cloud Service Server

3.) Xerox® ConnectKey Share to Cloud Server to OmniPage Cloud Services or email

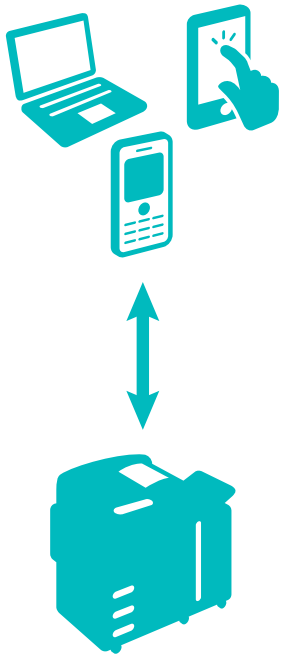
MFP to Xerox® ConnectKey Share to Cloud and OmniPage Cloud Service: All information transmitted between the MFP, Xerox® ConnectKey Share to Cloud and OmniPage Cloud Service is transmitted securely via Secure Sockets Layer (SSL). SSL is a commonly-used protocol for managing the security of data transmitted over the Internet using a public and private key encryption system to ensure all data is encrypted during transmission.

Xerox® ConnectKey Share to Cloud to Cloud Services or email: All information transmitted between Xerox® Share to Cloud and Connectors/Destinations use SSL encryption techniques as long as they are supported by the Service/Destination. If SSL is not supported, the security policies of the service/destination are used.

Note: Documents stored to the device's disk are deleted. If a Share process is disrupted, documents do not survive a power off cycle.

Complete Security for Complete Peace of Mind

Xerox® ConnectKey Share to Cloud is a completely secure solution that you can trust. User data is securely encrypted, so employees can rest assured that their information is kept completely confidential. In addition, all communications between the device and the cloud server are encrypted using SSL, including the documents sent from the MFP to Microsoft Azure. Additionally, temporary scanned files are deleted from the MFP when the data is transferred—a step that helps ensure the wrong users can't access confidential documents.



Xerox® ConnectKey™ Share to Cloud does not require any on-premise software installation and instead utilizes cloud server technology.