

Xerox[®] ConnectKey[®] for SharePoint[®] Administrator Guide



©2015 Xerox Corporation. All rights reserved. XEROX®, XEROX and Design®, and ConnectKey® are trademarks of Xerox Corporation in the United States and/or other countries. BR1001

Microsoft® and Microsoft SharePoint® are registered trademarks of Microsoft Corporation.

All trademarks used herein are the property of their respective owners.

Contents

1	Xerox® ConnectKey™ for SharePoint® Administrator Guide	1-1
	Purpose of This Document	1-1
	Glossary of Terms	1-1
	Version Compatibility.....	1-2
2	ConnectKey for SharePoint Configuration and Administration	2-1
	Global Settings	2-3
	Authentication Settings.....	2-4
	Configuring Xerox Secure Access to work with ConnectKey for SharePoint.....	2-7
	Network Setup Overview	2-7
	ConnectKey for SharePoint.....	2-7
	Xerox Secure Access.....	2-8
	Two Factor Authentication	2-10
	Configuring Native MFP Authentication	2-10
	Configuring the MFP with Native Mode Authentication using LDAP, Kerberos, or SMB authentication.....	2-11
	Configuring the MFP with Native Mode Authentication using the Device's Internal Database.....	2-11
	Reject Folder Settings	2-11
	General Failure Notification Options Settings	2-12
	Timing Interval Settings	2-14
	Debug Setting.....	2-14
	Retry Setting.....	2-15
	MFD Advanced Settings	2-15
	Web Server Port	2-15
	To Use SSL.....	2-15
	FTP Port	2-15
	Adding a Scan to Folder Workflow Button	2-16
	Creating a Scan to Folder Button on the MFP	2-16
	Adding a SharePoint Workflow Button.....	2-18
	SharePoint Routing Options.....	2-18
	Create a Scan to SharePoint Button on the MFP	2-20
	Scan Settings.....	2-22
	Notification Options Settings.....	2-24
	Scan to My Site	2-24
	Saving your Work	2-26
	MFD Summary View	2-26

	ConnectKey for SharePoint Toolbar Options.....	2-27
3	ConnectKey Service Manager.....	3-1
	Overview.....	3-1
	General Tab	3-2
	Log On Tab.....	3-3
	Service Accounts.....	3-3
	Recovery Tab.....	3-5
4	ConnectKey Status Monitor	4-1
5	ConnectKey License Manager	5-1
6	ConnectKey MFP Registration Tool.....	6-1
	Registration of MFPs with the ConnectKey for SharePoint Application.....	6-1
	Overview of Device Registration.....	6-2
	Setting the Parameters for the Default Registration Group.....	6-2
	Adding a Device to the Registration Group.....	6-4
	Registering Devices	6-5
	If a Device has not Been Successfully Registered (Indicated by a Red Icon)	6-6
	Adding Multiple Devices through CSV Import to the Registration Group.....	6-7
	Editing or Removing a Device in the Registration Group	6-9
7	Serial Numbers & Maintenance Contract IDs.....	7-1
8	Software Updates	8-1
9	General Administration Items.....	9-1
	ConnectKey for SharePoint Logs	9-1
	Log File Location Details	9-1
10	Basic Troubleshooting	10-1
	Troubleshooting Tips.....	10-1
	ConnectKey for SharePoint Application Button is not on the MFP or does not execute.....	10-1
	Document did not Reach Its Expected Destination.....	10-1
	No Email Notification has been Sent When a Scan Document Fails to Reach Its Expected Destination.....	10-2
	ConnectKey for SharePoint Service will not Start (or Stops Immediately)	10-2
	Document did not Convert to the Desired Output Format (PDF, PDF/A, XLS, DOCX) with Satisfactory Results	10-2
	Document Processing Time is Unsatisfactory.....	10-2
	ConnectKey for SharePoint does not connect to the SPS Server to display a list of libraries and folders	10-3
	Color Document Output was selected but the output file was black and white	10-3

Xerox® ConnectKey™ for SharePoint® Administrator Guide

1

Purpose of This Document

This document provides instruction for the basic configuration and administration of the Xerox® ConnectKey™ for SharePoint® software solution. The document is intended for use by the System Administrator for Xerox ConnectKey for SharePoint.

The ConnectKey for SharePoint solution consists of the following software:

- ConnectKey Process Designer (workflow administration user interface)
- Service Manager
- Status Monitor
- License Manager
- Device Registration

Note

The Status Monitor is not available in Canada.

Glossary of Terms

Term/Abbreviation	Description
Administrator	Technical resource supporting, configuring, and maintaining the ConnectKey for SharePoint software.
EIP	Extensible Interface Platform Xerox Platform for multifunctional device enablement and integration for custom software solutions.
Authentication	Refers to any method of authentication at the Xerox EIP MFP that is recognized by the ConnectKey for SharePoint service and that passes the user's Window Account.
ConnectKey for SharePoint	Xerox Application Solution for scan to folder and SharePoint.
Configuration File (CFG)	ConnectKey for SharePoint configuration file.
LAN	Local Area Network. Used to communicate between Xerox EIP MFPs, windows services, and servers at a customer location.

Multifunction Device (MFD)	Hardware scanning device running ConnectKey for SharePoint that has been enabled for document capture.
Multifunction Printer (MFP)	Any references to devices, multifunction devices, MFDs, printers, and MFPs should all be treated synonymously.
Scan User	Refers to the scanning user who will submit Scan jobs from the Xerox EIP MFP.
AutoStore	ConnectKey for SharePoint is powered by AutoStore™ Imaging technology from Notable Solutions, Inc.
SMTP	Simple Mail Transport Protocol is the standard protocol for email transmission.
LDAP	Lightweight Directory Access Protocol provides a way to look up email and user names from Active Directory.
SPS	Microsoft SharePoint server
Two factor Authentication	Refers to the process of enabling both Xerox Convenience authentication followed by a prompt for password.

Version Compatibility

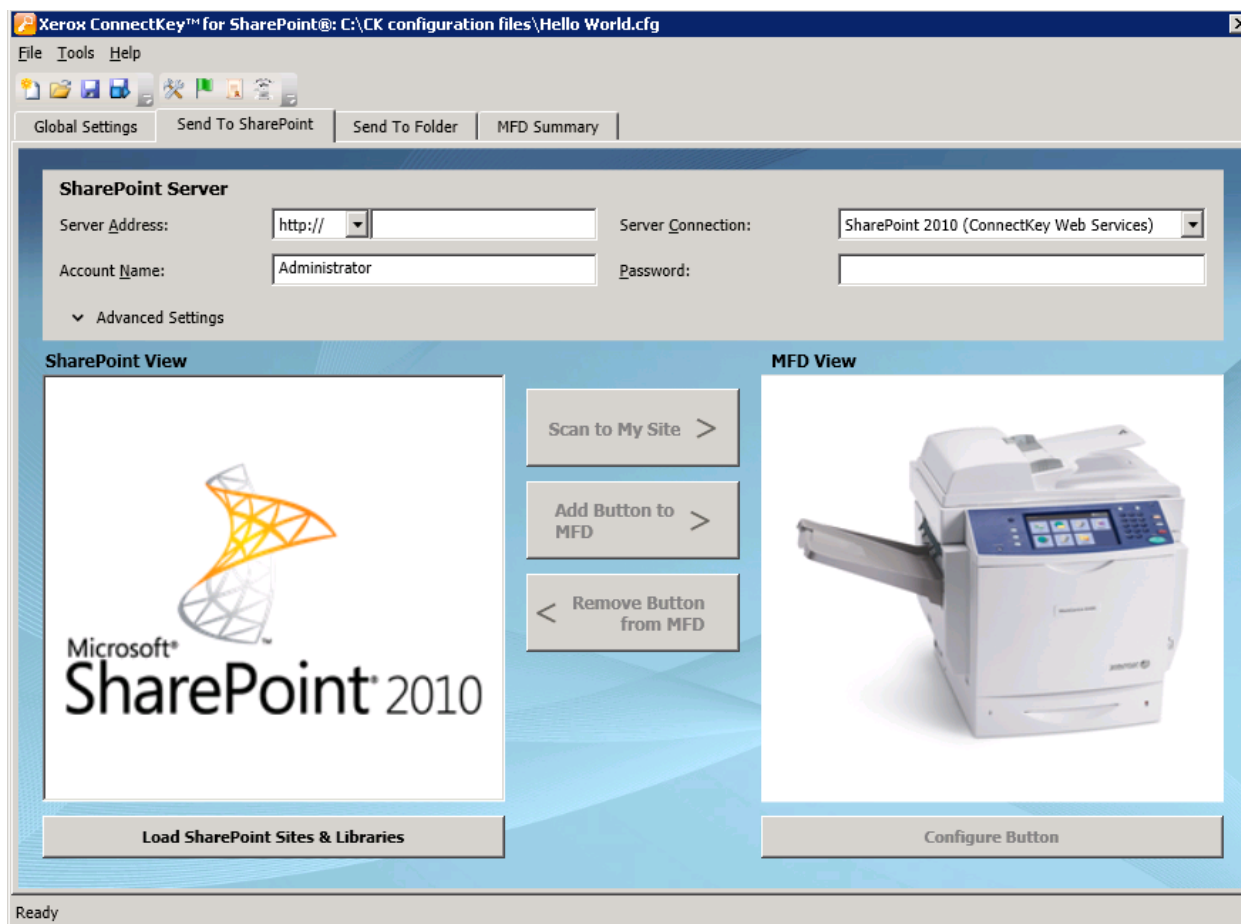
The information in this document applies to Xerox ConnectKey for SharePoint Version 1.2.

ConnectKey for SharePoint Configuration and Administration

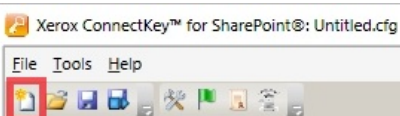

The ConnectKey for SharePoint administration application is designed to easily create workflow configurations (CFG). This configuration is for Xerox EIP device registration, document conversion, and content routing of the document and index metadata to a Microsoft SharePoint or a network folder destination. From the ConnectKey for SharePoint interface an administrator can create a new configuration, review or save changes to the details of an existing configuration, or launch additional tools for the overall application administration of the Xerox distributed capture solution. The following sections focus on the available workflow configuration options for handling content in this distributed capture software solution. In addition to this guide, ConnectKey for SharePoint has a built-in help system that will provide additional information.

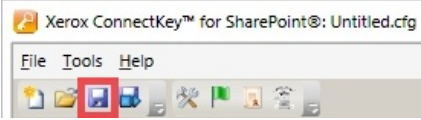
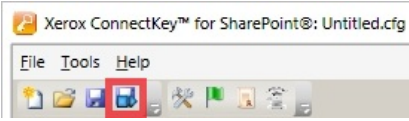
Take the following action to start the ConnectKey for SharePoint application:

From the computer where ConnectKey for SharePoint is installed, click Start > All Programs, select Xerox, select the ConnectKey Program Group, and then click on “ConnectKey Process Designer”.



Launching the ConnectKey for SharePoint application presents the administrator with a user friendly interface to manage the document workflow configuration, additional administrative tools, and some common features. The common features are available as icons in the menu bar, as well as the File or Edit menu options.

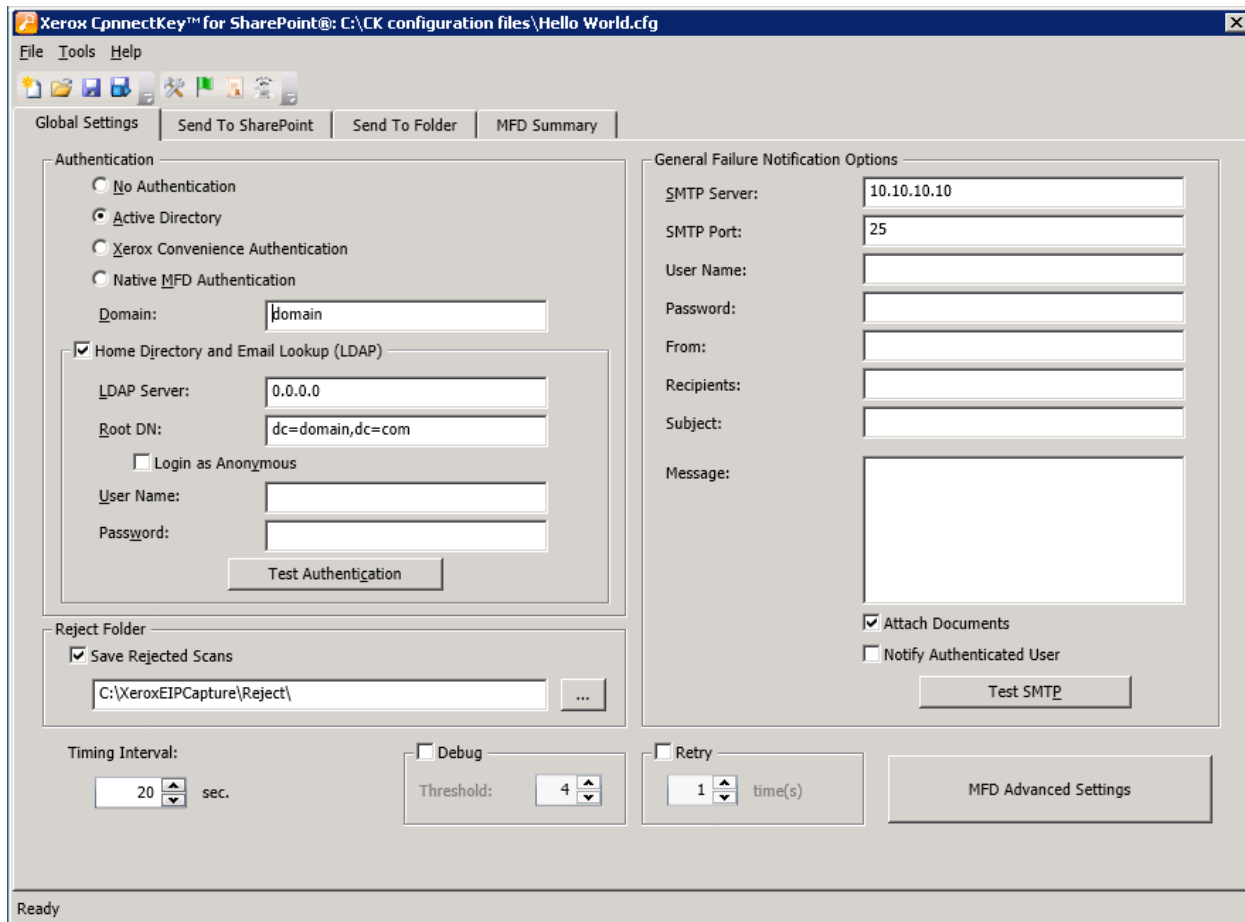
Name/Icon	Description
<p>Create a new configuration file</p> 	<p>File > New (or Ctrl+N)</p> <p>Creating a new configuration file generates a new CFG file, which an administrator can save and launch for document processing.</p>
<p>Open an existing configuration file</p> 	<p>File > Open (or Ctrl+O)</p> <p>Opening an existing CFG file, which an administrator saved in a location that is accessible by the ConnectKey for SharePoint server.</p>

<p>Save the current configuration file</p> 	<p>File > Save (or Ctrl+S)</p> <p>Saving any changes to the CFG file made in the ConnectKey for SharePoint application.</p>
<p>Save as...</p> <p>(Drop-down menu option under File)</p>	<p>File > Save as...</p> <p>Save as will create (or replace) a CFG file in process or previously saved.</p>
<p>Save and run service with the current Configuration file</p> 	<p>File > Save and Run</p> <p>Save and Run stores the changes to the CFG file and restarts the configured ConnectKey for SharePoint service with the recent changes to the configuration.</p> <p>Note</p> <p>In order for a configuration to deploy to your MFP, you must save your work and restart the service. This can be done either by clicking the Save and run option, or by Saving your configuration, then using the Service Manager to start the service with your new configuration.</p>
<p>Recent Files</p> <p>(Drop-down menu option under File)</p>	<p>File > Recent Files ></p> <p>Recent Files will provide quick links to open CFG files, which have recently been viewed by the ConnectKey for SharePoint administrator eliminating the need for the admin to browse to the CFG file through the Open a CFG file option.</p>
<p>Exit</p> <p>(Drop-down menu option under File)</p>	<p>File > Exit (or Alt+F4)</p> <p>Closes the ConnectKey for SharePoint administration interface.</p>

The tabbed interface gives administrators access to the configuration of Global Settings, Send to SharePoint, Send to Folder, and MFD Summary details. The following sections identify the details of each tabbed section and provide configuration options, which are available for document processing.

Global Settings

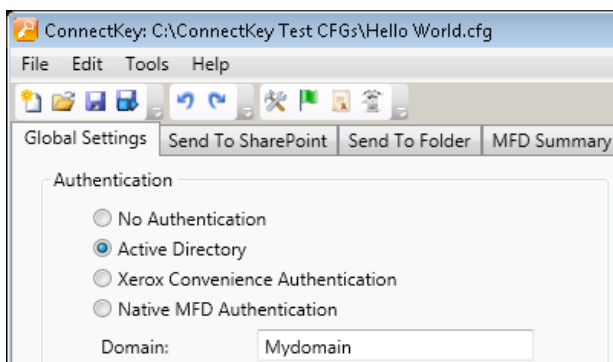
The “Global Settings” tab is positioned as the first configurable tab in the ConnectKey for SharePoint administrative interface. The general settings entered by a system administrator are global in nature and once saved are applied to the total solution and configuration file (CFG). To navigate to the general settings click on the “Global Settings” tab at the top of the ConnectKey Process Designer application tabbed dialog.



Authentication Settings

The administrator can set up an authentication method to control access by the scan user to ConnectKey for SharePoint on the MFP. There are four options to choose from, including “no authentication”. Based on the option designated by an administrator, other configuration options may be disabled. For example, choosing “no authentication” will disable the option to scan to a user’s home directory, because that information will not be available.

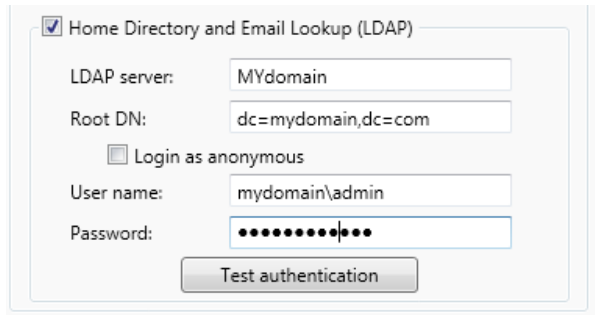
The following options are available as authentication methods for the workflow configuration:



Name	Description
No authentication	No MFP authentication will be required at the device panel, by scan users, to gain access to the configured scanning options.
Active Directory	<p>Users are prompted to enter their Active Directory username and password (LDAP lookup validated) at the MFP prior to accessing the ConnectKey for SharePoint Scanning options. Selecting this option requires the Domain field to be populated with the customer's domain name for the deployment.</p> <p>Note</p> <p>See the Home Directory and Email Lookup (LDAP) configuration settings.</p>
Xerox Convenience Authentication	<p>Users authenticate using a Xerox authentication method, such as card swipe, prior to accessing the ConnectKey for SharePoint scanning options. Refer to the section below, "Configuring Xerox Secure Access to work with ConnectKey for SharePoint" for more information on configuring Secure Access. Otherwise, refer to your Convenience Authentication product specific documentation or refer to the Convenience Authentication product support for further details on configuring convenience authentication.</p> <p>Note</p> <p>For SharePoint browsing options, two factor authentication is required</p>
Native MFD Authentication	Users authenticate using the native Xerox EIP authentication method (LDAP) prior to accessing the ConnectKey for SharePoint scanning options. Refer to the section below on "Configuring Native MFP Authentication". Otherwise, refer to your device product specific documentation or the device product support for further details on configuring Native MFP Authentication.
Domain	The Domain in which your ConnectKey for SharePoint server is configured is required for all Authentication options except, No Authentication.


Home Directory and Email Lookup (LDAP) Settings

While Home Directory and Email (LDAP) Settings are not required for authentication, they must be configured in order to obtain a scan user's home directory and email address. Those options will only be enabled when Home Directory and Email (LDAP) has been configured. For verification, the administrator can test the LDAP Settings using the test button in the ConnectKey interface.



The screenshot shows a configuration window titled "Home Directory and Email Lookup (LDAP)". It contains the following fields and controls:

- A checked checkbox labeled "Home Directory and Email Lookup (LDAP)".
- An "LDAP server:" label followed by a text box containing "MYdomain".
- A "Root DN:" label followed by a text box containing "dc=mydomain,dc=com".
- An unchecked checkbox labeled "Login as anonymous".
- A "User name:" label followed by a text box containing "mydomain\admin".
- A "Password:" label followed by a password box with 12 dots.
- A "Test authentication" button at the bottom.

Name	Description
Home Directory and Email Lookup(LDAP)	Activates the configuration of the LDAP settings, and is required if home directory and email attributes are desired.
LDAP server	Identifies the IP address of the Active Directory (LDAP) server in the deployment environment. The LDAP Server must be in the same domain as the computer where ConnectKey for SharePoint is installed. ConnectKey for SharePoint must be able to communicate with the LDAP server.
Root DN	In the Root DN field type the search base where the LDAP Query should start. For example: DC=Sales, DC=MyCompany, DC=com. This information should be requested from the network administrator.
Login as Anonymous	Select this option if your LDAP server does not require a secure connection.
User name	Unless the target LDAP Server allows anonymous access, ConnectKey for SharePoint requires a domain service account with rights to query the LDAP Server. Enter the domain user, which will be used to perform the LDAP Query.
Password	Enter the password for the domain user, which ConnectKey for SharePoint will use to perform the Active Directory authentication. (See User name above).
Test authentication 	To test the search settings, enter a domain account name in the field and click the Test authentication button. This must be a login id such as jsmith.

Configuring Xerox Secure Access to work with ConnectKey for SharePoint

This section will show you how to integrate the logins from Xerox Secure Access and ConnectKey for SharePoint to provide a seamless user experience.

Network Setup Overview

This example has a ConnectKey for SharePoint server installed on the SharePoint server, an Active Directory server, and a Xerox Secure Access server. These are all on the same domain.

ConnectKey for SharePoint

In the example below, ConnectKey for SharePoint is configured to use Xerox Convenience Authentication with the 'ck4sp' domain.

The LDAP server is also configured since it is used to authenticate from the Xerox Secure Access server and can provide a richer user experience by adding home directories and email lookup to the application.

The screenshot shows the 'Xerox ConnectKey™ for SharePoint: Untitled.cfg' window. It has a menu bar (File, Tools, Help) and a toolbar. The main area is divided into several sections:

- Global Settings** (selected tab):
 - Authentication**:
 - ☐ No Authentication
 - ☐ Active Directory
 - ☒ Xerox Convenience Authentication
 - ☐ Native MFD Authentication
 - Domain:
 - ☒ Home Directory and Email Lookup (LDAP):
 - LDAP Server:
 - Root DN:
 - ☐ Login as Anonymous
 - User Name:
 - Password:
 -
 - Reject Folder**:
 - ☒ Save Rejected Scans
 - Path:
 -
 - Timing Interval**: sec.
 - ☐ Debug
 - Threshold**:
 - ☐ Retry
 - Retry**: time(s)
 -
- General Failure Notification Options**:
 - SMTP Server:
 - SMTP Port:
 - User Name:
 - Password:
 - From:
 - Recipients:
 - Subject:
 - Message:
 - ☒ Attach Documents
 - ☐ Notify Authenticated User
 -

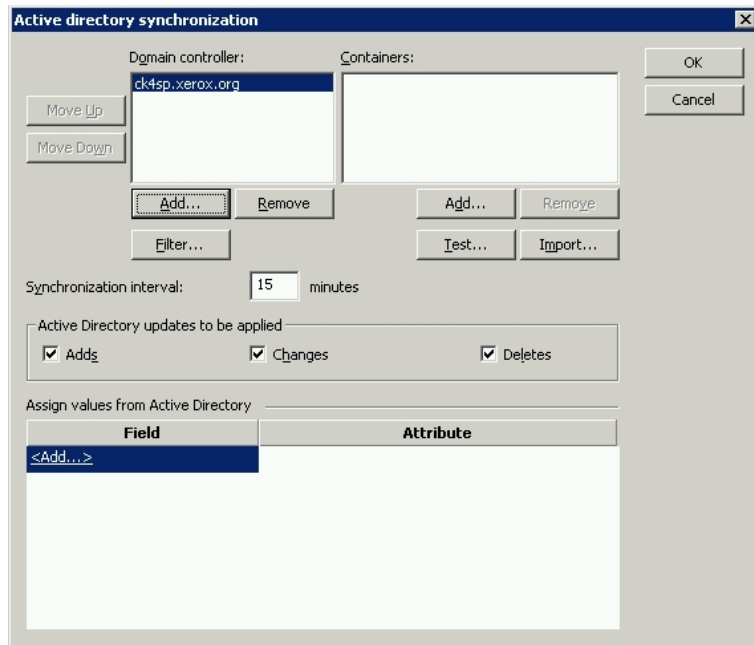
Xerox Secure Access

Xerox Secure Access should be configured to import the users from the Active Directory server. To do this from the main screen, click on **Configuration>Active directory synchronization**.

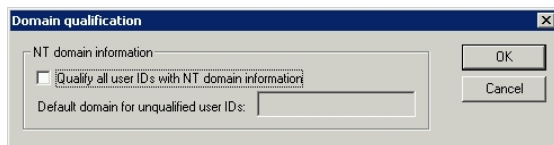
The screenshot shows the 'SIV-SECACCESS - Xerox Secure Access Unified ID System™ [Configuration]' window. It has a menu bar (File, Edit, View, Tools, Help) and a toolbar with a Refresh button. The main area is divided into two panes:

- Left Pane (Navigation)**:
 - SIV-SECACCESS - System**:
 - Configuration (selected)
 - Devices
 - Messages
 - Software
 - SIV-SECACCESS - Accounts**:
 - Users
- Right Pane (Content)**:
 - Active directory synchronization** (selected):
 - Domain qualification
 - Authentication device settings

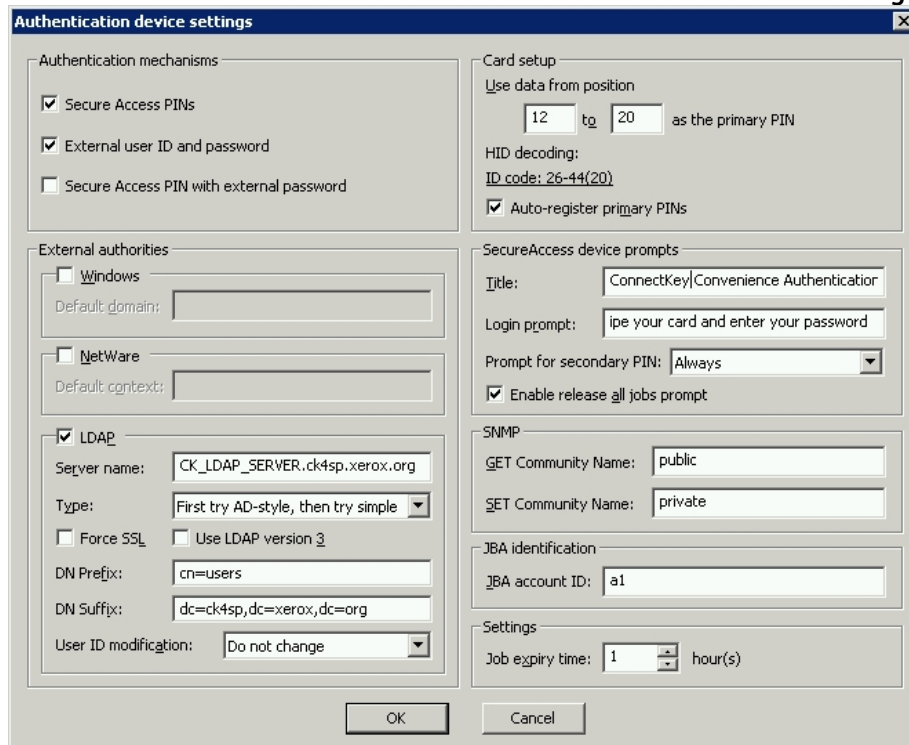
On the **active directory synchronization** screen, add the Active Directory server, in the example below this is ck4sp.xerox.org.



Return to the main screen and click on the **Domain qualification** link, the “**Qualify all user IDs with NT domain information**” should not be checked.



Return to the main screen and click on the **Authentication device settings** link.



In order for authentication to work with ConnectKey for SharePoint the Xerox Secure Access server needs to be configured to use External authorities and LDAP. To do this select “**External user ID and password**”. In order for swipe cards to work you need to have “**Secure Access PINs**” selected.

Two Factor Authentication

To enable the ability to browse folders when Xerox Convenience Authentication is enabled, you must also enable the option to export password. Enabling both Convenience Authentication and the option to Export Password is also referred to as Two Factor Authentication.

See your device’s System Administrator Guide for “Extensible Interface Platform” for instruction on how to enable “Export password”. If you do not enable export password, ConnectKey will prompt you for your username and password when you access the application at the MFP.

To configure Xerox Secure Access to use two factor authentication, follow the instructions for normal authentication with Xerox Secure Access. Instead of select “**External user ID and password**” select “**Secure Access PIN with external password**” and set the “**Prompt for secondary PIN**” to always.

The screenshot shows the 'Authentication device settings' window. It is divided into several sections: 'Authentication mechanisms' with checkboxes for 'Secure Access PINs', 'External user ID and password', and 'Secure Access PIN with external password'; 'External authorities' with checkboxes for 'Windows', 'NetWare', and 'LDAP' (selected), each with a 'Default' field; 'Card setup' with 'Use data from position' (12 to 20), 'HID decoding' (ID code: 26-44(20)), and 'Auto-register primary PINs'; 'SecureAccess device prompts' with 'Title', 'Login prompt', 'Prompt for secondary PIN' (Always), and 'Enable release all jobs prompt'; 'SNMP' with 'GET Community Name' (public) and 'SET Community Name' (private); 'JBA identification' with 'JBA account ID' (a1); and 'Settings' with 'Job expiry time' (1 hour(s)). 'OK' and 'Cancel' buttons are at the bottom.

Configuring Native MFP Authentication

Native Mode authentication is authentication done on the MFP using LDAP, Kerberos, SMB, or the device’s internal database. When correctly configured a user will be prompted to log into the MFP when they walk up to the MFP at a blocking screen, or when they click on the ConnectKey for SharePoint button by the native mode login.

When incorrectly configured, a user will be prompted not only by the native mode login, but they will also be prompted by the ConnectKey for SharePoint application.

Configuring the MFP with Native Mode Authentication using LDAP, Kerberos, or SMB authentication

In order to best use native mode authentication on the MFP using Remote Authentication sources you need to configure the sources to match the usernames and passwords of your SharePoint or Windows Network folders.

See your device's System Administrator Guide for "Setting up Network Authentication" and look for the subsections for your particular protocol such as "Configuring Authentication Server Settings for LDAP", "Configuring Authentication Server Settings for SMB", or "Configuring Authentication Server Settings for Kerberos".

See your device's System Administrator Guide for "Extensible Interface Platform" for instruction on how to enable "Export password". If you do not enable export password, or the credentials do not match your Active Directory domain, ConnectKey will prompt you for your username and password when you access the application at the MFP.

Configuring the MFP with Native Mode Authentication using the Device's Internal Database

In order to best use native mode authentication on the MFP using Local Authentication you need to configure the MFP's internal database with users that match the usernames and passwords of your SharePoint or Windows Network folders. If the usernames and passwords do not match, ConnectKey will prompt you for your username and password when you access the application at the MFP.

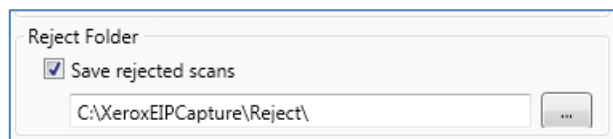
See your device's System Administrator Guide for configuring "Local Authentication" and for "Adding User Information to the Local Database".

See your device's System Administrator Guide for "Extensible Interface Platform" for instruction on how to enable "Export password". If you do not enable export password, or the credentials do not match your Active Directory domain, ConnectKey will prompt you for your username and password when you access the application at the MFP.

Reject Folder Settings

If desired, the "Reject Folder" setting can be enabled and defines the location for storing jobs, which fail during document processing. It is the system administrator's responsibility to review rejected items to take the appropriate corrective actions on these jobs. Refer to the log files to determine any error messages regarding the failure to take the appropriate corrective action such as a change to the configuration file (CFG), to identify potential external issues such as no network connectivity to a route destination, or changes to user credentials being used by the service. The "Reject Folder" location is typically used in conjunction with the configured notification options on processing failures. Using notification options will proactively send an email alert when a document fails to route properly to either folders or SharePoint.

Example configuration of the reject folder:



Name	Description
Save rejected scans	Check this box to store the rejected scanned images when the document scan fails.
Folder path for the storage of the rejected jobs	<p>Enter a directory to maintain a copy of all that failed to route to the target destination (folder or SharePoint).</p> <p>Note</p> <p>The service account for ConnectKey for SharePoint must have write permissions to Reject Folder directory. (See the “ConnectKey Service Manager” section for details).</p>

General Failure Notification Options Settings

The “General Failure Notification Options” setting is configured for sending email notifications for jobs, which fail during scanning. This option requires a SMTP mail relay and the use of a domain user account. An administrative email recipient(s) or distribution list is typically configured to receive the email notification. If LDAP Settings have been configured (see “Home Directory and Email (LDAP) Settings”), the scan user can also receive the notification. Notification Options can also be configured to attach the scanned image to the automated notification.

The following fields are required for the configuration of notification options for jobs that fail to reach their intended target destination:

General Failure Notification Options

SMTP server: 10.16.16.16

SMTP port: 25

User name: ConnectKey

Password: ••••••••

From: ConnectKey@mycorp.com

Recipients: admin@mycorp.com

Subject: Scan failed


Message: Your scan document failed

☒ Attach Documents

☐ Notify Authenticated User

Test SMTP

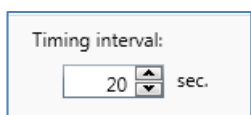
Name	Description
SMTP server	Identifies the IP address of the SMTP email relay in the deployment environment. The ConnectKey for SharePoint server must be able to communicate across the network to the identified SMTP server, contact the network administrator if you cannot communicate with the LDAP server.
SMTP port	Identifies the network port number for effective communication to the SMTP email relay in the deployment environment.
User name	Enter the SMTP relay user, which the ConnectKey service will use to authenticate for email routing. Note This user name will not be used as the From address in the automated notifications unless you enter the same credentials in the From field below.
Password	Enter the password for the SMTP user account, which the ConnectKey service will use to authenticate for email routing.
From	Enter the email address the email notification will be sent from.
Recipients	Enter the email addresses or distribution list to receive the failure notification emails. Addresses should be semicolon separated.
Subject	Enter the subject text to appear in the failure notification emails.

Message	Enter the message text to appear in the failure notification emails.
Attach Documents	Select this option to attach the scanned image to the automated failure email notification.
Notify Authenticated User	<p>Select this option to additionally send the automated failure email notification to the authenticated user who scanned the document.</p> <p>Note</p> <p>This option will be grayed out if the LDAP Settings have not been configured (see Home Directory and Email (LDAP) Settings).</p>
Test SMTP button 	<p>Clicking this button validates the configuration.</p> <p>Test results will be presented, validating the SMTP relay settings.</p>

Timing Interval Settings

The “Timing interval” setting is configured in seconds. This determines how frequently ConnectKey for SharePoint will process the scanned documents. It will not impact the frequency or speed of scanning.

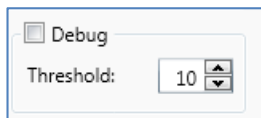
The following field is edited to define the timing interval for the service:



Timing interval:
 sec.

Debug Setting

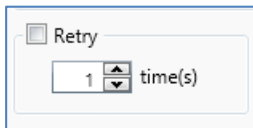
The “Debug” setting is a toggle setting that can be enabled and can have a granularity level associated with it. The debug setting controls how much information is displayed in the ConnectKey Status Monitor and written to the connectkey.log file. This information is used for troubleshooting purposes and contains a variety of information such as date/time of a scan, network address of the MFP, user info, and other data, as well as the success or failure of a scan workflow. Increasing the level from 1 to 10 will increase the amount of information and level of detail for the status information displayed/written. If the debug setting is disabled, some information will still be written/displayed, but at the minimum level allowable by ConnectKey for SharePoint.



☐ Debug
 Threshold:

Retry Setting

The “Retry” setting is a toggle setting that controls how many times ConnectKey for SharePoint should attempt to route a scanned document to its destination if there is a problem. If this setting is enabled, ConnectKey for SharePoint will attempt to complete the workflow as many times as specified by the setting before considering the workflow a failure. If all retry attempts have been exhausted and the document has still not routed, then ConnectKey for SharePoint will enforce the exception handling specified by the Reject Folder and General Failure Notification Options Settings.



MFD Advanced Settings

ConnectKey for SharePoint communicates with Xerox EIP MFPs using both FTP and HTTP communication. In the MFD Advanced Settings section, it is possible to change the default ports used for communication, to enable SSL for more secure communication, to create a certificate for use with SSL, and to change the FTP mode from active to passive.

Web Server Port

Enter the port on which the web application will be running

To Use SSL

Check “**Use SSL**” to secure the connection from the device to the web application.

- From the Choose Certificate option list, select to browse for an existing certificate or to create a new self signed one.
- In Certificate Password, enter the password for the certificate. If you created a self-signed certificate, this value will be automatically entered into the field based on the information you provided when creating the certificate.

FTP Port

In the **FTP Port** box, enter the port on which the FTP service will be running.

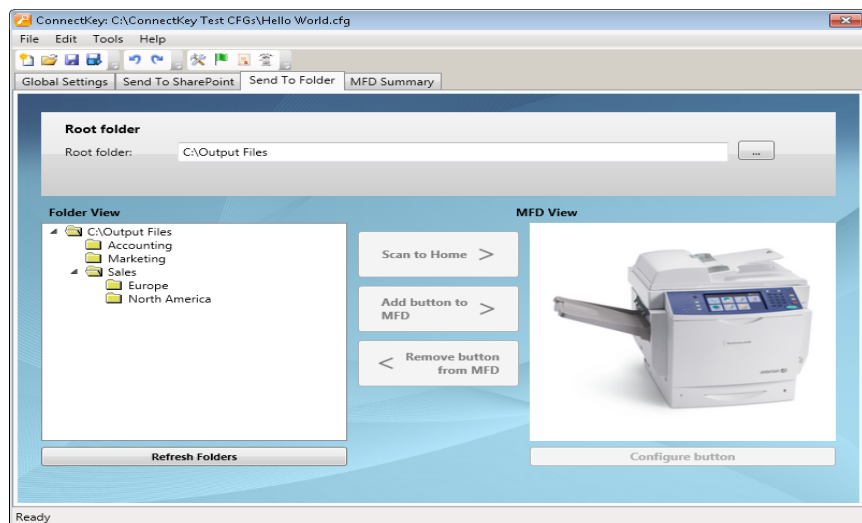
- In the **FTP Data Port Range** box, enter the port range that will be used when receiving passive ftp connections from a device. The default is ports 35000 through 49000.

Note

If you want a device to connect using passive FTP mode then this must be configured on the device. By default devices are configured to use active FTP.

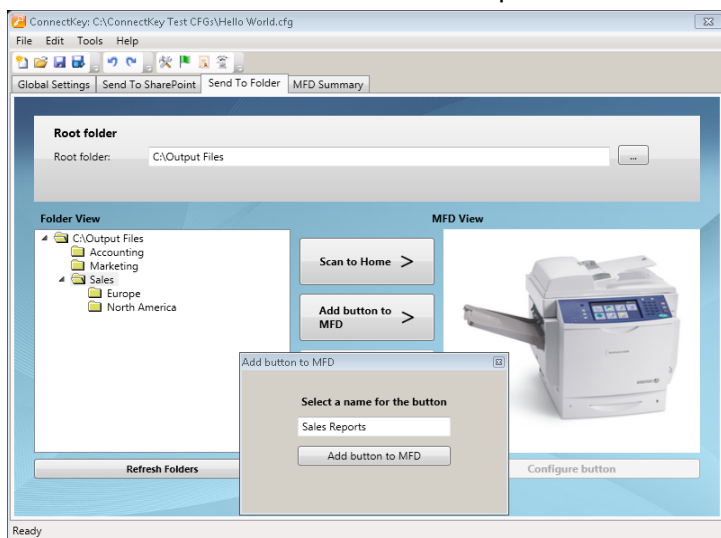
Adding a Scan to Folder Workflow Button

ConnectKey for SharePoint can be configured to scan documents to Windows Folders. Target folders are presented in an easy to use tree view manner and can be added and managed through the MFD View. If LDAP Settings have been configured (see “Home Directory and Email (LDAP) Settings”), a “Scan to Home” button can also be configured.



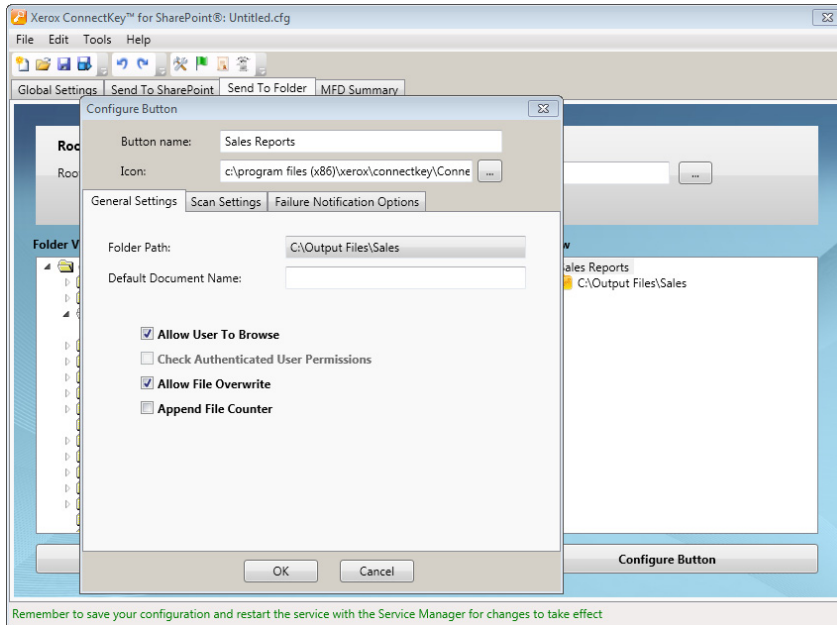
Creating a Scan to Folder Button on the MFP

1. From the ConnectKey Process Designer, select the “Send to Folder” tab.
2. Select a root folder.
3. Click on “Refresh Folders”.
4. Navigate the tree view list of folders in the Folder View and select the target folder.
5. Click the “Add button to MFD” and provide a user friendly name for the button.



6. Click “Assign Button to MFD” to add the button to the MFD View.

- Once added, options for the workflow button can be configured by selecting the button in the MFD View and clicking “Configure Button.”



The workflow button options include the following:

General Settings

- **Allow User to Browse** – At scan time this option allows the scan user to navigate downward from the target folder associated with the workflow button on the MFP Panel. Any sub-folder inside the target folder can be selected as the new destination folder.
- **Check Authenticated User Permissions** – At scan time this option will enforce Windows Folder Permissions to ensure that the scan user has write access to the target location.

Note

This option is only enabled if some form of authentication is enabled. (See Authentication Settings). It is possible for a scan user to browse a folder but not have write permissions. Please consult a Windows Network Administrator for assistance with folder permissions.

- **Allow File Overwrite** – At scan time this option will replace any existing file in the target folder with the same name. This can be useful if only the latest version of a file is desired.

Note

Mutually exclusive with “Append File Counter” option.

- **Append File Counter** – At scan time this option will always append a numeric counter to any file being placed in the target folder. Additional files with the same name will have an incremented counter appended to the name to ensure uniqueness.

Note

Mutually exclusive with “Allow File Overwrite”.

- **Default document name** – Enter a default file name, which can be accepted or overridden by the user at scan time.

- **Icon** – Browse to select a custom icon for the workflow button. By default, a folder icon is provided automatically but can be replaced with any 44x44 PNG image file. For convenience, a library of icons is provided in the installation folder for ConnectKey under the subfolder \Icons\Xerox EIP Connect.

Scan Settings

- These settings control aspects of the document size, quality, etc. Please see “Scan Settings” for details.

Failure Notification Options

- These settings control who receives email notification of scan failures for the workflow button. Please see “Notification Options Settings” for details.

Creating a Scan to Home Button on the printer

- The Scan to Home Button is enabled if Authentication and LDAP Settings have been configured (see “Home Directory and Email (LDAP) Settings”). If the scan user has a home directory attribute in Active Directory, ConnectKey for SharePoint will use this location as the target folder. See “Creating a Scan to Folder Button on the MFD” above.

Note

When using “Scan to Home”, you cannot enable “Allow User to Browse” from the General Settings tab of the “Configure Button”.

8. Repeat these steps until all Send to Folder buttons have been created. After configuring all the required Buttons, you must save your configuration. Please see the “Saving your Work” section below for more details.

Adding a SharePoint Workflow Button

ConnectKey for SharePoint can be configured to scan documents to Microsoft SharePoint (SPS). Target locations within SPS are presented in an easy to use tree view manner and can be added and managed through the MFD View. Valid locations can be libraries or folders within SPS. If desired, the administrator can enforce user permissions at scan time to ensure that the scan user can only navigate SPS Locations to which he or she has permissions.

SharePoint Routing Options

The options for routing to SharePoint are as follows:

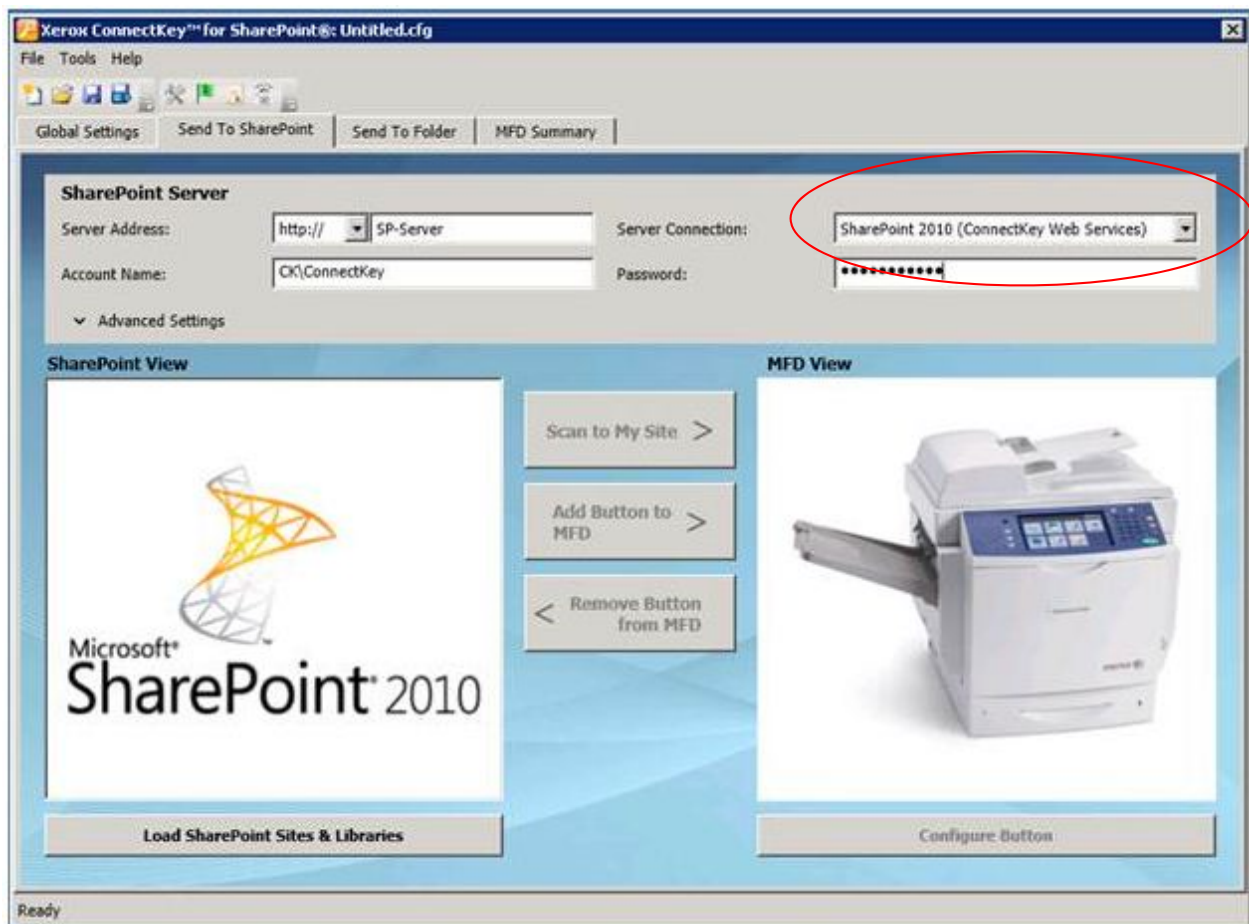
- **SharePoint 2007 (ConnectKey Web services)**
 - This method connects to a SharePoint 2007 server using the add-on web services provided with ConnectKey for SharePoint. This is the only method for connecting to SharePoint 2007
- **SharePoint 2010 (ConnectKey Web services)**
 - This method connects to a SharePoint 2010 server using the add-on web services provided with ConnectKey for SharePoint. This method does not incur the constraints listed for SharePoint 2010 (Microsoft Web Service). It provides the largest features set.

- **SharePoint 2010 (Microsoft Web Services)**

- This method allows routing to a SharePoint 2010 Server that does not have the ConnectKey add-on web services installed. This method is applicable in deployments where the customer is either unwilling or unable to use the add-on services. The following limitations apply:
 - File sizes are limited to 200 MB in size
 - Impersonation is not supported – documents will be routed using the account credentials used to connect to SharePoint in the button configuration screen
 - Support for managed metadata fields is not possible

- **SharePoint 2013 (Microsoft Web Services)**

- This method allows routing to a SharePoint 2013 Server that does not have the ConnectKey add-on web services installed. This is the only method for connecting to SharePoint 2013. The following limitations apply:
 - File sizes are limited to 200 MB in size
 - Impersonation is not supported – documents are routed using the account credentials used to connect to SharePoint in the button configuration screen
 - Support for managed metadata fields is not possible



Create a Scan to SharePoint Button on the MFP

1. From the ConnectKey Process Designer, select the “Send To SharePoint” tab.
2. Select the correct pull-down configuration for your SharePoint server; i.e., http for non-secure, and https for a secure SharePoint server.
3. Enter the IP address or host name of your SharePoint server.
4. From the pull-down menu, select the correct SharePoint Server Connection.
5. Enter a valid Account name and password.

Note

For SharePoint 2007, 2010, and 2013, domain accounts require the following format:
Domain\username.

6. Select the “Load SharePoint sites & libraries” button.
7. Navigate the tree view list of libraries and folders in the SharePoint View and select the target location.
8. Click “Add button to MFD” and provide a user-friendly name for the button.
9. Click “Add button to MFD” to add the button to the MFD View.
10. Once added, options for the workflow button can be configured by selecting the button in the MFD View and clicking “Configure button”.

Workflow button options include the following:

General Settings

- Allow user to change Document Library
 - At scan time this option allows the scan user to navigate to other libraries or downward from the target location associated with the workflow button on the MFP Panel. Any location inside the target can be selected as the new destination
- Allow User to change Folder
 - At scan time this option allows the scan user to navigate downward from the target location associated with the workflow button on the MFP Panel. Any location inside the target can be selected as the new destination.

Constraints:

- This option is only enabled with the following authentication methods:
 - Active Directory
 - Native MFP Authentication
 - Convenience Authentication with two factor authentication
- In addition to authentication constraints, this feature is only enabled when using one of the following connectivity methods:
 - SharePoint 2010 (ConnectKey Web Services)
 - SharePoint 2007 (ConnectKey Web Services)
- Impersonate Authenticated User – When selected, at scan time this option will enforce SharePoint Permissions to ensure that the scan user has access to the target location.

Constraints:

- This option is only enabled if some form of authentication is enabled. (See “Authentication Settings.”) and when using SharePoint 2010 (ConnectKey Web Services) or SharePoint 2007 (ConnectKey Web Services).
- Icon – Browse to select a custom icon for the workflow button. By default, a SharePoint icon is provided automatically but can be replaced with any 44x44 PNG image file. For convenience, a library of icons is provided in the installation folder for ConnectKey under the subfolder \Icons\Xerox EIP Connect

Scan Settings

- These settings control aspects of the document size, quality, etc. Please see “Scan Settings” for details.

Notification Options

- These settings control who receives email notification of scan failures for the workflow button. Please see “Notification Options Settings” for details.

11. Repeat these steps until all send to SharePoint buttons have been created. After configuring all the required Buttons, you must save your configuration. Please see “Saving your Work,” later in this section, for more details.

Note

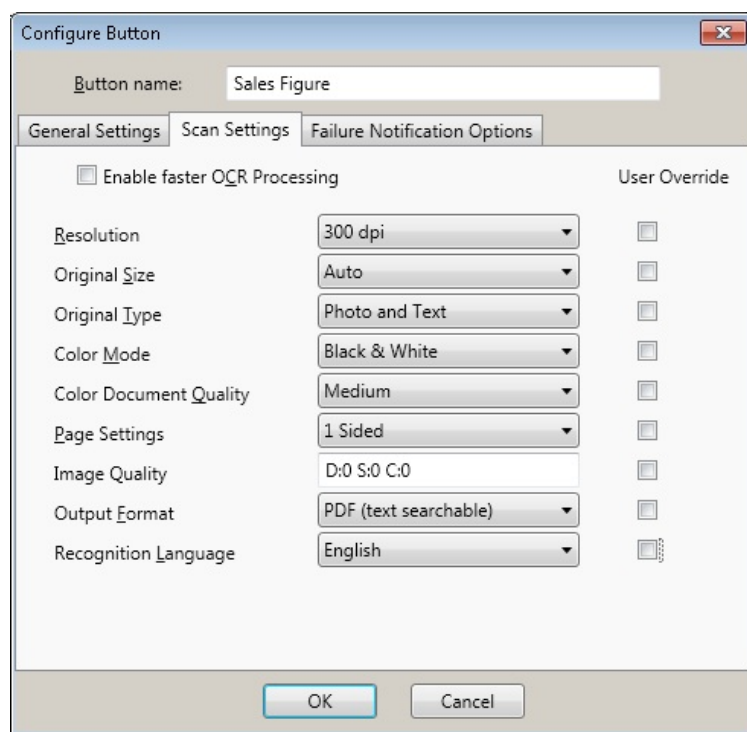
SharePoint workflows can be configured to toggle between Server 2007 and Server 2010.

Scan Settings

Each workflow button on the MFP has its own scan settings and notification options. This allows the administrator to set default parameter settings for the workflow. In addition, the administrator can allow the scan user to override some of the default settings at scan time. Common settings defined here are related to image quality and file format (see screen shot below for details).

The setting for “Enable faster OCR Processing” will decrease the amount of time necessary for performing OCR and conversion to PDF, PDF/A, XLS or DOCX Format. If this setting is enabled but the accuracy of the OCR is deemed unsatisfactory, disable it.

The setting for output formats TIFF, JPG, and PDF (Image Only) is not compatible with “user override” option and therefore are not selectable by the scan user. These options must be configured by the ConnectKey for SharePoint administrator.



Configure the default settings for the scanned document. The available settings are:

- **File Format:** The following file types are supported **PDF**, **Single Page Tiff**, **Multipage Tiff**, and **JPEG** (for color devices).
- **Resolution:** 100, 200, 300, 400, or 600 dpi

- **Original Size:** Auto, Mixed, 8.5" x 11" LEF, 8.5" x 11 SEF, 8.5" x 14" SEF, 11" x 17" SEF, 5.5" x 8.5" LEF, 5.5" x 8.5" SEF, 8.5" x 13" SEF, A4 LEF, A4 SEF, A3 SEF, A5 LEF, A5 SEF, B5 LEF or B5 SEF.

Note

LEF refers to Long Edge Feed and SEF refers to Short Edge Feed. These terms describe the manner in which the documents are feed into the MFP.

- **Original Type:** Photo and Text, Photo or Text
- **Color Mode:** Auto, Full Color, Black and White or Grayscale

Note

If the Auto option is selected, the device will detect color pages in which case the document will be scanned using the Full Color option. If no color pages are detected, the document will be scanned using the Black and White option.

For the following MFPs, the Auto option is supported only when PDF is selected for File Format. If the Auto option and another File Format option are selected, File Format will automatically change to PDF:

- WorkCentre™ 5222/5225/5230
- WorkCentre™ 5325/5330/5335
- WorkCentre™ 7120/7125
- WorkCentre™ 7232/7242
- WorkCentre™ 7328/7335/7345/7346
- WorkCentre™ 7425/7428/7435
- Xerox 4112/4127 C/P
- Xerox™ Color 550/560, Xerox Integrated Color Server
- **Color Document Quality:** High, Medium or Low
- **Page Settings:** Select the default number of sides to be scanned. The Two Sides setting indicates duplex scanning.
- **Image Quality**
 - Auto Background Suppression - This option automatically reduces or eliminates the dark background resulting from colored paper or newspaper originals. (Note: This option is disabled if the Original Type is Photo.)
 - Contrast - This option controls the differences between the image densities within the image. Select a lower setting to improve the copy quality of pictures. Select a higher setting to produce more vivid blacks and whites for sharper text and lines.
 - Lighten/Darkness - This option controls how the scan service processes the images of the scanned input document so the output document appears either lighter, darker, or the same as the original input document.
 - Sharpness - This option controls the balance between sharp text and moiré (patterns within the image). Adjust the sharpness values from sharper to softer, based on the quality of the input images.

Notification Options Settings

Each workflow button on the MFP has its own notification options settings. An administrator can define the following: whether an email notification is dispatched or not, when a scan job fails, the recipient(s), and the message content. By default, these settings are determined by the General Failure Notification Options (see General Settings), but can be overridden for each workflow button.

The screenshot shows the 'Configure Button' dialog box with the 'Failure Notification Options' tab selected. The 'Button name' is 'Sales Figures'. The 'On' radio button is selected. The 'From' field is 'ConnectKey@mycorp.com', 'Recipients' is 'admin@mycorp.com', 'Subject' is 'Scan failed', and 'Message' is 'Your scan document failed'. Both 'Attach Documents' and 'Notify Authenticated User' checkboxes are checked. 'OK' and 'Cancel' buttons are at the bottom.

Field	Value
Button name	Sales Figures
Notification Status	On
From	ConnectKey@mycorp.com
Recipients	admin@mycorp.com
Subject	Scan failed
Message	Your scan document failed
Attach Documents	<input checked="" type="checkbox"/>
Notify Authenticated User	<input checked="" type="checkbox"/>

Scan to My Site

ConnectKey for SharePoint can create workflow buttons that route to Microsoft My Sites. The **Scan to My Site** button is only enabled if authentication is configured. When this button is clicked, a workflow will be created that scans to a user's My Site location in SharePoint. The URL for this location is based on the path specified under the advanced settings option in the SharePoint Tab. This path combined with the scan user's name is used to determine the My Site Location in SharePoint. If the default path is incorrect for your environment, it can be changed.

Note: Please consult with your SharePoint Administrator for more information on how to configure My Sites in SharePoint.



Scan to My Site Constraints

The following constraints apply to My Site workflows:

- Authentication must be enabled
- My Site is only supported with:
 - SharePoint 2007
 - SharePoint 2010
 - SharePoint 2013
- The route is based on the default “my site” path specified in the SharePoint advanced settings and the server connection information with user ID appended
- Target location for SharePoint 2007 and 2010 is root folder of “Personal Documents” library; Target location for SharePoint 2013 is the root folder of “Documents” library.
- MFP panel-level browsing is not supported – Workflow buttons must be created as static route destinations
- The workflow button provides a default Document Name field, which can be set by the Xerox ConnectKey for SharePoint Administrator but can be changed at scan time
- My Site provides support for Impersonation on SharePoint 2007 and SharePoint 2010
- The workflow button only provides filename for indexing. It does not provide additional metadata fields

Saving your Work

ConnectKey for SharePoint allows you to make changes to your configuration without affecting your users. This means you can create new workflow buttons and when you are ready you can deploy these changes to your MFPs. This is a two-step process, as follows:

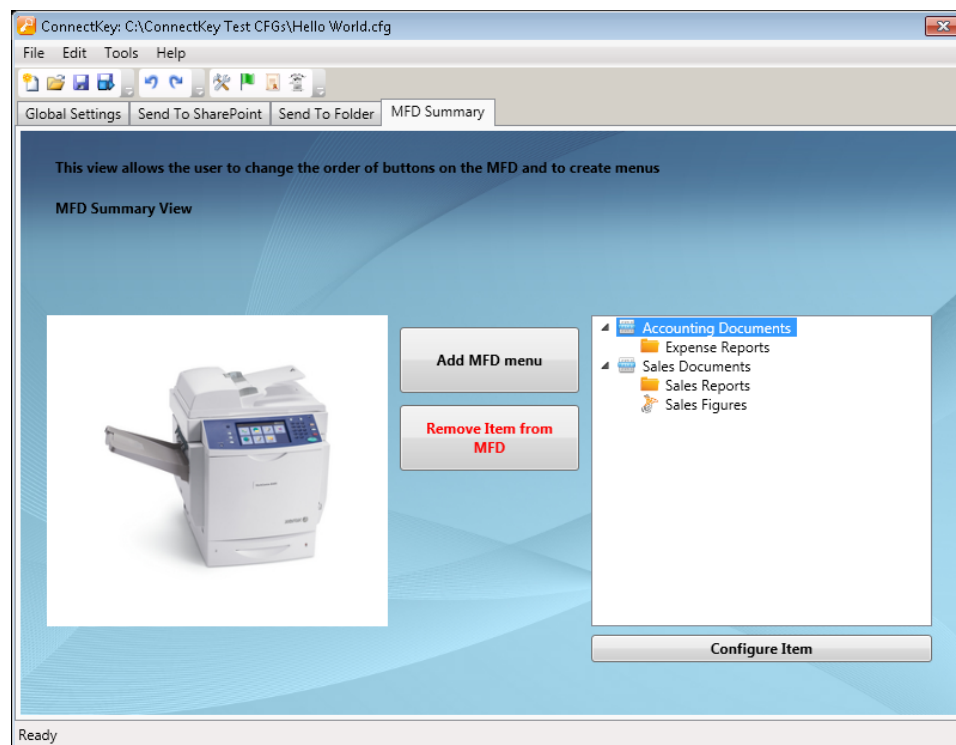
1. After making all the necessary changes to your configuration, you must save your configuration. From the File Menu, select Save
2. Next, use the Service Manager to load the configuration file and start the service. If the service is already running you must first stop the service to proceed.




The steps above are essential to ensure that your configuration is deployed to the MFPs.

For full details, see ConnectKey Service Manager.

MFD Summary View

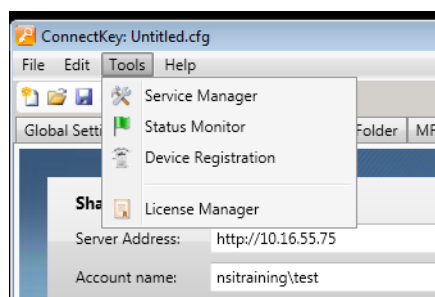
The MFD Summary tab displays the layout of buttons on the printer and allows the administrator to define a hierarchy of menus for the buttons. Using drag and drop, buttons can be organized within the menus. Button and menus can also be deleted from this view. The summary view is also a shortcut to the button configuration options. By selecting a button and clicking “configure item”, the administrator can change settings (see “Adding a Scan to Folder Workflow Button” or “Adding a SharePoint Workflow Button”). Additionally, by selecting a menu item the administrator can change the text and icon for the item.



Name	Description
Add MFD menu button 	Adds a menu item to the printer
Remove Item from MFD button 	Removes a menu or button from the printer
Configure Item button 	Shortcut to workflow button options

ConnectKey for SharePoint Toolbar Options

There are several tools that can be launched from the toolbar shortcuts or from the Tools Menu Option. This section of the document describes these tools.



ConnectKey Service Manager

3

The Service Manager is a tool for system administrators to manage the run-time engine for ConnectKey for SharePoint. The administrator has the ability to select the desired configuration file (CFG) and to stop and start the service. Furthermore, it allows the administrator to define auto-start settings, the log file location, and the Windows Service Account that ConnectKey for SharePoint will run under.

Starting the service is required for any of your workflows to be available on the MFP.

Note

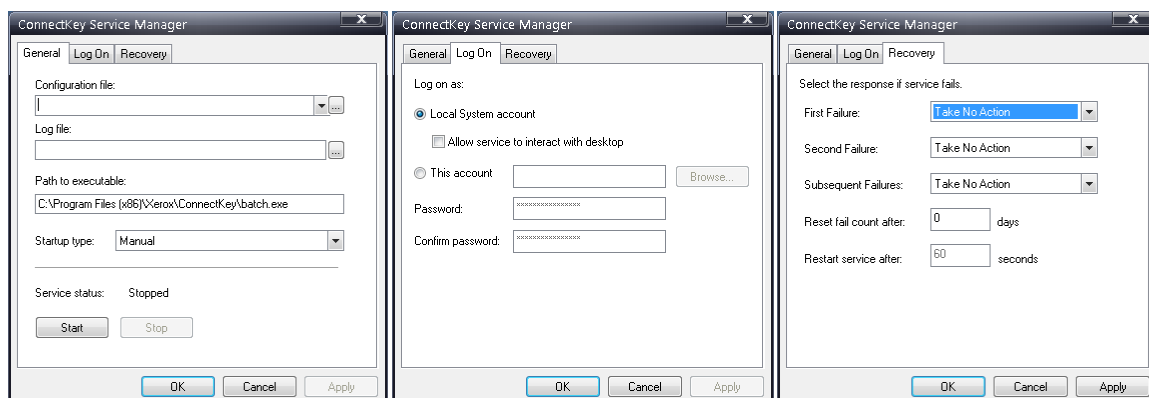
The log file path must be set before the service can be started.

⚠ WARNING

It is best practice to perform these changes during non-production hours to avoid disruption to users who may be scanning.

Overview

Select Tools > Service Manager from the ConnectKey for SharePoint administration interface menu bar.



Sample views of the Service Manager Interface tabs

The following sections provide the detailed description of the Service Manager fields and operations:

General Tab

Name	Description
Service Status	This field displays the current service status (started, stopped, etc.)
Configuration File	<p>This field contains the configuration file (CFG) name.</p> <p>The ConnectKey for SharePoint administration tool generates this file when you save your server parameters. The file has a .cfg file extension. Click the ellipses button to select a configuration file in the Windows Explorer view.</p>
Log File	This field contains the log file name. The service creates a log file for the process activities. This file must reside on the local machine.
Startup type	<p>Using this field, you can select the startup type for the service.</p> <p>Automatic restarts the service automatically if the server is restarted.</p> <p>Manual requires the service to be restarted manually every time the server is restarted.</p> <p>Disabled marks the service as disabled so that it cannot be started.</p>
Start	Click this button to start the service.
Stop	Click this button to start the service.

Log On Tab

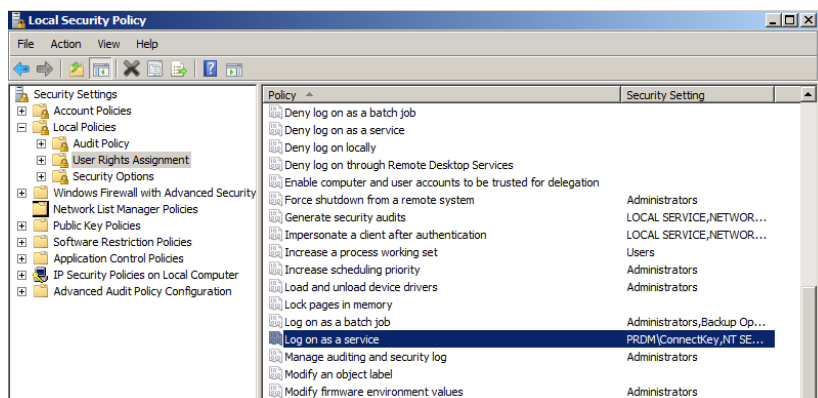
Name	Description
Log On As This Account Refer to the “Service Accounts” section below	ConnectKey for SharePoint must run under a Windows Domain Account that has read/write permissions to the folder locations that users will be scanning into. See “Service Accounts” below for additional permissions requirements. Click the Browse button to search for the desired Windows Domain Account.
Password	Enter the user password.
Confirm password	Enter the user password again to confirm.
Local System Account Refer to the “Service Accounts” section below	The Local System account is a predefined local account used by the service control manager. It has extensive privileges on the local computer.
Allow Service to interact with Desktop	When local system account is used, you may enable the Allow service to interact with desktop check box. If you select this check the box, then a service runs as though it were an interactive user and can do things like click the 'OK' button on a pop-up message. This may be useful in situations when the components used in a process are interacting with some applications that generate dialogs or pop-up messages. The service will interact with these dialogs and prevent the applications from hanging.

Service Accounts

When accessing networked resources such as SharePoint, Active Directory, LDAP, email (for failure notification options), and network folders, ConnectKey for SharePoint must use service accounts. For convenience, it is possible to use one service account for all resources as long as it has sufficient permissions to all the network resources it will be accessing.

Here are some things to note about service accounts and ConnectKey for SharePoint:

- The ConnectKey for SharePoint service must access multiple resources and is controlled by the ConnectKey Service Manager. The account used to run this service must have the following permissions:
 - Must be a local administrator (it must be added to the local administrator group)
 - Must have permissions to log on as a service. This setting is controlled via Windows Local Security Policy (see screen below example)



- The account used to run the ConnectKey for SharePoint service must have read permissions to Active Directory and LDAP in order to perform lookups for user home directory and email.
- The account used to run the ConnectKey for SharePoint service must have write permissions to the folder designated in the “save rejected scans” attribute in global settings.
- The user account used to access SharePoint should have at least the Contribute permission level for the specified folder, list, or document library.
- To use impersonation, the user used to access SharePoint should be a site collection administrator.
- ConnectKey supports only the integrated Windows authentication methods, which rely on IIS authentication for SharePoint 2010 Web applications. These methods are NTLM or Kerberos (IIS Windows Authentication). IIS settings should be checked after the Web application is created: the Windows Authentication method should be enabled and other authentication methods should be disabled.

The account used to run the SharePoint service controls both the browsing permissions and the routing permissions for Send to Folder workflows. This means that the account must have read/write permission to any network directories that will be used with ConnectKey for SharePoint.

Note

This account must have very high level permissions so that it can route documents into users' home folders on their behalf. Based on these permissions, it may be possible for a user to browse to a location that he would otherwise not have access to. However, any documents attempted to be scanned to such locations will fail if “check authenticated user permissions” has been enabled. For security purposes, it is important to note that browsing does not expose any documents in any folders to the user at the MFP.

- The account used to send email failure notifications must have permissions to send mail on the SMTP email server.

The account used to access ConnectKey for SharePoint servers must have read/write permissions to any locations within SharePoint that will be used with ConnectKey for SharePoint. Unlike Scan to Folder, it is possible to limit the browsing of the authenticated scanning user if the “impersonate authenticated user” option is enabled. This has the added benefit of submitting the documents using the scanning user's account and populating the SharePoint column for this value accordingly

Recovery Tab

The recovery tab provides options for when to attempt a service restart, if the ConnectKey Service were to stop for some reason (such as a server reboot). Restart options for a first, second and subsequent failures can be set as well as parameters for resetting the restart counter and timing interval can also be set.

ConnectKey Status Monitor

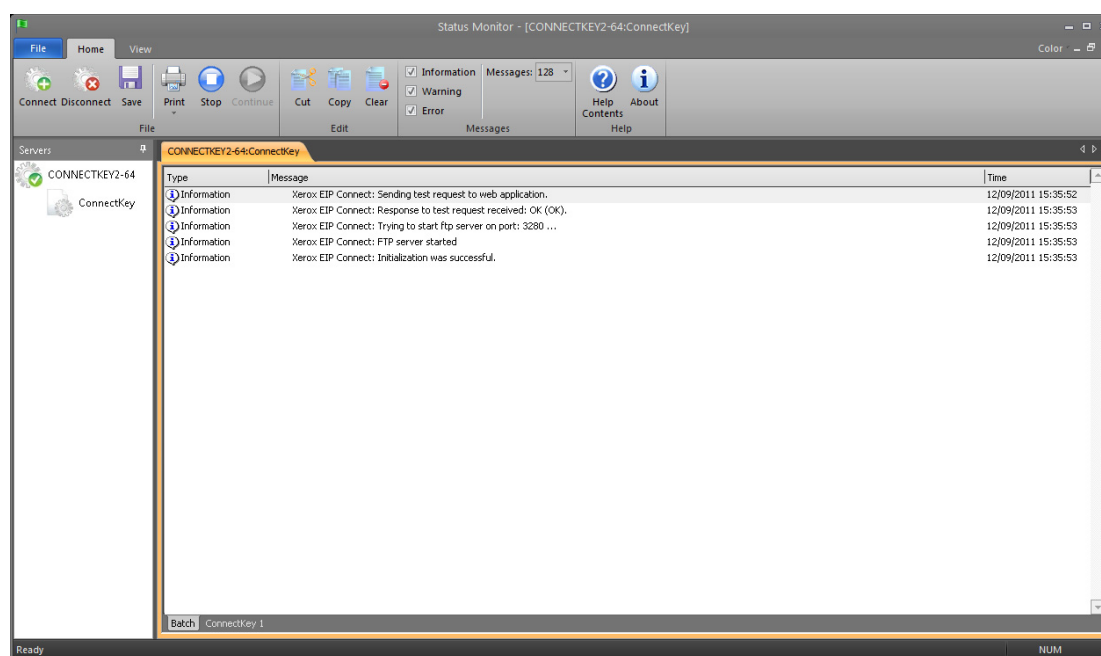
4

The ConnectKey Status Monitor is a tool for system administrators to view system activity in real time, and it can be thought of as viewing a “live” logfile. All information displayed in the monitor is also written to the ConnectKey log file (see ConnectKey Service Manager). For troubleshooting purposes an administrator should monitor live scanning with this tool to look for any error messages.

From the ConnectKey for SharePoint administration interface menu bar, select Tools > Status Monitor.

Note

The Status Monitor is not available in Canada.



Sample view of the Status Monitor interface

The Status Monitor enables the viewing of real-time status messages associated with all scanning activity for ConnectKey for SharePoint. Monitoring status messages can help troubleshoot if there are problems with scanning. The Status Monitor also helps to predict and identify the sources of any potential system problems.

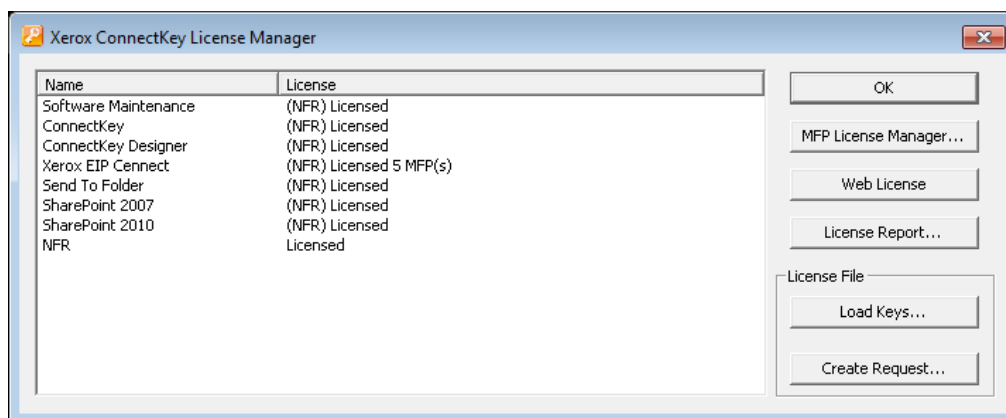
Refer to the online help for more information on how to configure the Status Monitor.

ConnectKey License Manager

5

The ConnectKey License Manager is a tool for system administrators to generate license request files and apply for software licenses from the Xerox ConnectKey Web License Portal. It can also be used to load a license key, validate the current license status, and generate a license report. (See Installation Guide for instructions on licensing the ConnectKey for SharePoint software)

Select Tools > License Manager from the ConnectKey for SharePoint administration interface menu bar.



Name	Description
OK	Closes the License Manager Window
MFP License Manager	This opens a modal window that is used for blocking and unblocking MFP licenses. Blocking an MFP is a way to temporarily make the license available for another MFP. Unblocking a license reverses this behavior. Blocking and unblocking is a way to manage licenses, when the license availability is less than the number of devices. This is a way to release a license from an MFP that has been replaced with a newer model.
Web License	This launches the Xerox Connect Key Web License Portal for licensing Xerox ConnectKey for SharePoint and for adding additional licenses for MFPs.
License Report	This option will generate an html report of ConnectKey for SharePoint licenses. Typically this would be used for a Support Call when requested.
Load Keys...	This option is used to load the license key file obtained from the Xerox Connect Key Web License Portal.
Create Request...	This option is used to generate a license request file, which will be used at the Xerox Connect Key Web License Portal to generate a License Key file.

Note

External network connectivity is required in order to complete the licensing process

ConnectKey MFP Registration Tool

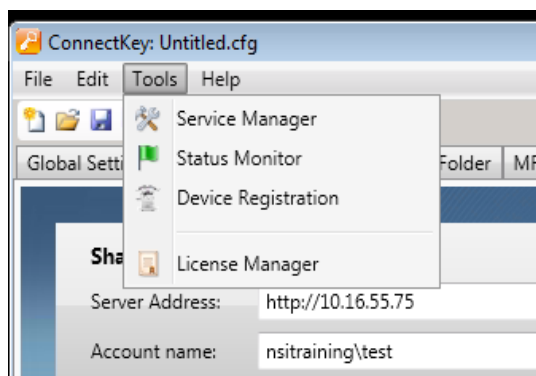
6

The ConnectKey for SharePoint Xerox EIP Device Registration Tool is designed to register supported Xerox EIP MFPs with the ConnectKey for SharePoint application. In the event that EIP is not properly configured on your device, the registration Tool will invoke the EIP Wizard to enable EIP on your device. If the wizard is unable to enable EIP on your device, it will provide you with instructions on how to manually configure EIP.

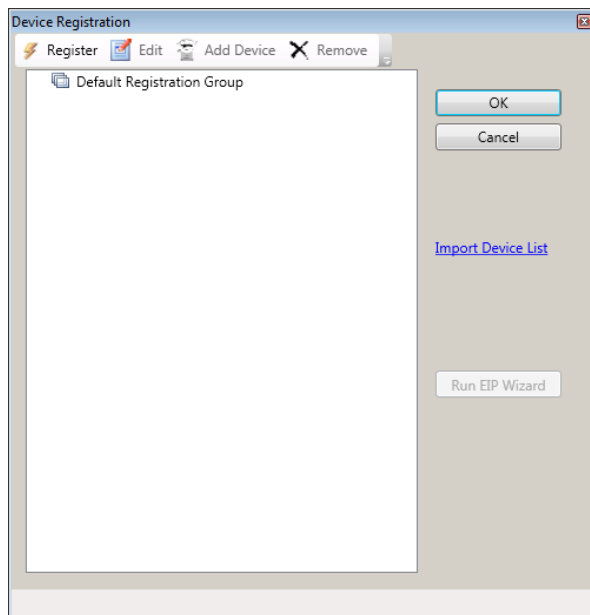
All devices must be registered in order for your workflows to be deployed to your MFPs.

Registration of MFPs with the ConnectKey for SharePoint Application

Select Tools > Device Registration from the ConnectKey for SharePoint administration interface menu bar.



The Device Registration Tool will be presented to add and configure devices:

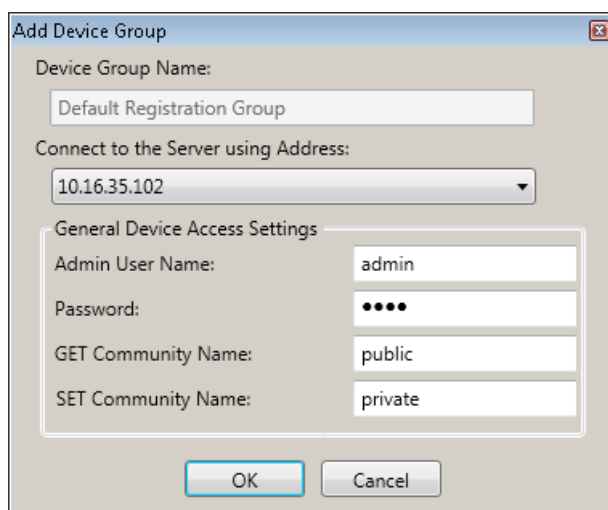


Device Registration administrator interface

Overview of Device Registration

Setting the Parameters for the Default Registration Group

All devices must be added to the default registration group. The parameters for this group will apply to all devices, but can be overridden when necessary for individual devices. See “adding a device” for details.

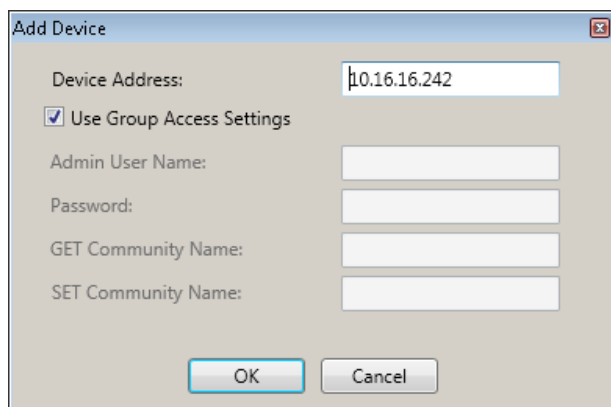


Name	Description
Connect to the server using address:	This selection box allows the registration of the ConnectKey for SharePoint Server to be performed using IP Address, Server Name or Fully Qualified Server Name. It is recommended that IP Address be used.
Admin User name	Enter the Admin User name for the device, if the group registration settings are not used.
Password	Enter the administrator Password for the device, if the group registration settings are not used.
GET Community Name	<p>Enter either public or private. The default value is public.</p> <p>Note</p> <p>This value must match the GET Community Name SNMP configuration value specified on the device (i.e. if Get Community Name is set to private on the device, then within registration manager GET Community Name must also be set to private.</p>
SET Community Name	<p>Enter either public or private. The default value is private.</p> <p>Note</p> <p>This value must match the SET Community Name SNMP configuration value specified on the device (i.e. if Set Community Name is set to private on the device, then within registration manager SET Community Name must also be set to private.</p>

Adding a Device to the Registration Group

To add a device the following procedure is required.

1. Select the “Default Registration Group”.
2. Click the “Add Device” button from the menu items.
3. The “Add Device” dialog displays:



The following parameters must be set in order to register the device:

Name	Description
Device Address	Enter either the name or IP address of the device, which will be added to the Registration Group.
Group Access Settings	Uncheck this box, if you wish to override the group settings
Admin User name	Enter the Admin User name for the device, if the group registration settings are not used. Note This option will be grayed out if the “Group Access Settings” checkbox is selected.
Password	Enter the administrator Password for the device, if the group registration settings are not used. Note This option will be grayed out if the Group Access Settings checkbox is selected.

GET Community Name	<p>Enter either public or private.</p> <p>The default value is public.</p> <p>Note</p> <p>This value must match the GET Community Name SNMP configuration value specified on the device (i.e. if Get Community Name is set to private on the device, then within registration manager GET Community Name must also be set to private.</p> <p>Note</p> <p>This option will be grayed out if the Group Access Settings checkbox is selected.</p>
SET Community Name	<p>Enter either public or private.</p> <p>The default value is private.</p> <p>Note</p> <p>This value must match the SET Community Name SNMP configuration value specified on the device (i.e. if Set Community Name is set to private on the device, then within registration manager SET Community Name must also be set to private.</p> <p>Note</p> <p>This option will be grayed out if the Group Access Settings checkbox is selected.</p>

- Once the settings have been applied, click the “OK” button to save your new device, or click “Cancel” to return to the Device Registration Tool without saving your settings.
- Continue adding devices in this manner. When all devices have been added, proceed to “Registering a Device” to begin the registration process.

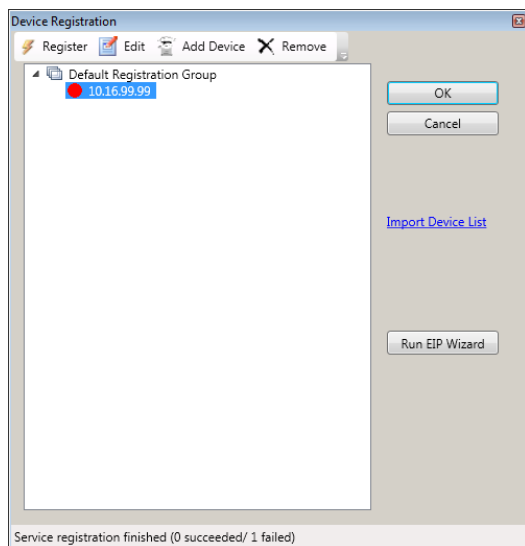
Registering Devices

To register all devices within a registration group, highlight the “Registration Group”, and select “Register” from the menu options. To register a single device, select the device and click on “Register”. The user will be presented a status bar at the bottom of the window. Once the registration process is complete, the status of device registration will be indicated as follows:

- Green – Device has been registered for use with ConnectKey
- Blue – Device Registration Status is unknown
- Yellow – Device has been successfully EIP Enabled (but has not yet been registered for user with ConnectKey for SharePoint)
- Red – Device has not been successfully registered.

Note

If you register a device without properly configuring your firewall security settings, registration will be green. You will see a “???” icon on the MFP user interface. Refer to the “Port Requirements” section in the *Xerox ConnectKey for SharePoint Installation Guide* for more details on which ports require security configuration to allow for communication.



If a Device has not Been Successfully Registered (Indicated by a Red Icon)

- The device may not be an online or a network issue may be preventing communication with the device.
- The device is online and reachable but EIP has not been enabled. See EIP Wizard below

EIP Wizard

Not all Xerox devices have EIP enabled by default or EIP may have been previously disabled. If EIP is not enabled on the device then the device will fail registration. To assist with enablement of EIP on a device, the EIP Wizard may be used to enable the various settings required for EIP. To configure EIP Services and Settings on an MFP, select the device and click the “Run EIP Wizard” button.

The EIP Wizard will walk you through several steps that will enable EIP Settings. It will attempt to automatically enable EIP. If it cannot automatically enable EIP it will present you with instructions to follow to enable EIP for your device. Please follow the instructions in the EIP Wizard carefully before contacting support.

Note

The EIP Wizard enablement process may reboot your device automatically. Please wait until the device is fully back online before continuing the wizard when a restart is needed.

Once the wizard has finished running, your device should be EIP enabled. ConnectKey will attempt to register the device again. If for any reason, the device cannot be registered after following the instructions, please refer to the ConnectKey for SharePoint Knowledge base.

<http://www.xerox.com/connectkeysharepointsupport>

Otherwise, contact Xerox Support.

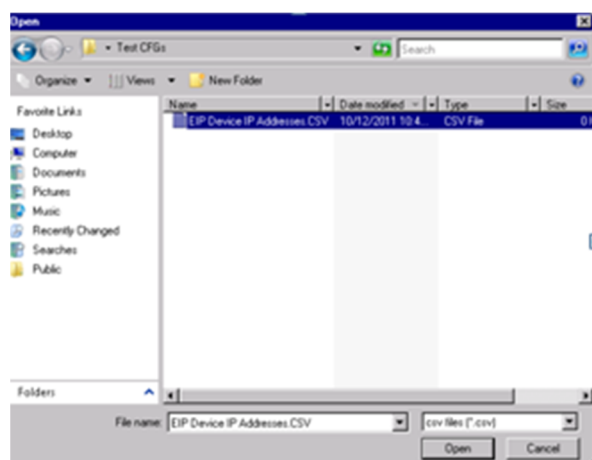
To obtain contact information, go to <http://www.xerox.com/connectkeysharepointsupport> and select support.

Adding Multiple Devices through CSV Import to the Registration Group

Multiple devices can be added at one time. This feature is helpful if you have a large number of Xerox EIP devices to be added to the solution.

To add multiple devices the following procedure is required:

1. From the Device Registration Tool, click the “Import Device List” option, to bring up the “Open” file browse interface.
2. The following windows “Open” dialog displays:



- a. Browse to the formatted CSV file for import of multiple Xerox EIP devices.
- b. Click the “Open” button to import the devices, or select the “Cancel” button to return to the previous screen.

The format of the text file must be:

[Device IP Address],[Device Admin User],[Device Admin Password],[Device SNMP Get String],[Device SNMP Set String]

Note

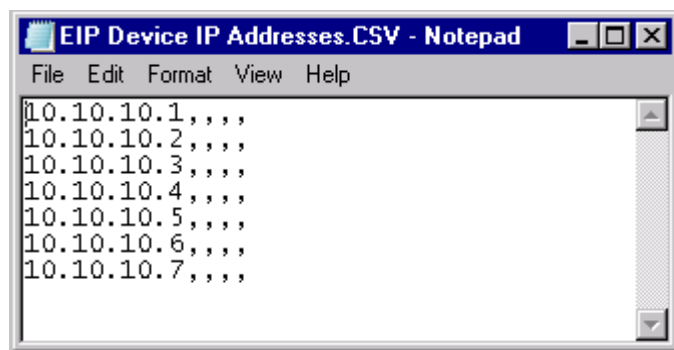
There are no spaces between each value. Given that all values except Device IP are optional, some entries may be left blank. If leaving blank entries, use the following format:

- Example #1 = [Device IP],[Device Admin Password],[Device SNMP Set String]

Or

- Example #2 = [Device IP],,,

In Example #2, the entry is an example where only Device IP's are being imported. There are no spaces in between commas. Use this format when the intent is to skip all optional registration information for the device.



Sample Device Import CSV file with 7 devices identified for import

Additional details regarding the CSV file formatting

- For Device IP, enter the IP address of the device. If this parameter is empty then the rest of the line is ignored.
- For Device Admin User, which is optional, enter the administrative user for the device. If this parameter is empty then the value configured for the group is used.
- For Admin Password, which is optional, enter the password for the administrator user of the device. This is optional, if the Device Admin User parameter is empty then this value is ignored.
- For SNMP GET String, which is optional, enter the SNMP community GET string as configured for the device. If this parameter is empty then the value configured for the group is used.
- For SNMP SET String, which is optional, enter the SNMP community SET string as configured for the device. If this parameter is empty then the value configured for the group is used.

Details regarding optional parameters

While the Device IP is required, optional parameters that are not used are treated as follows:

- If only Device IP is provided, then the values assigned for the group will always be used. In this instance, the Using same settings as group option is enabled.
- If Device IP and at least one other parameter are provided, then the corresponding group value for the missing parameter is used. This value is statically taken from values assigned to the group. If group settings are changed in the future, those new values will not be used with this device registration. In this instance, the Using same settings as group option is not enabled.

Note

If a device already in the list is found, the user will receive a warning and an option to either override the device with the new information or to keep the current device configuration.

Editing or Removing a Device in the Registration Group

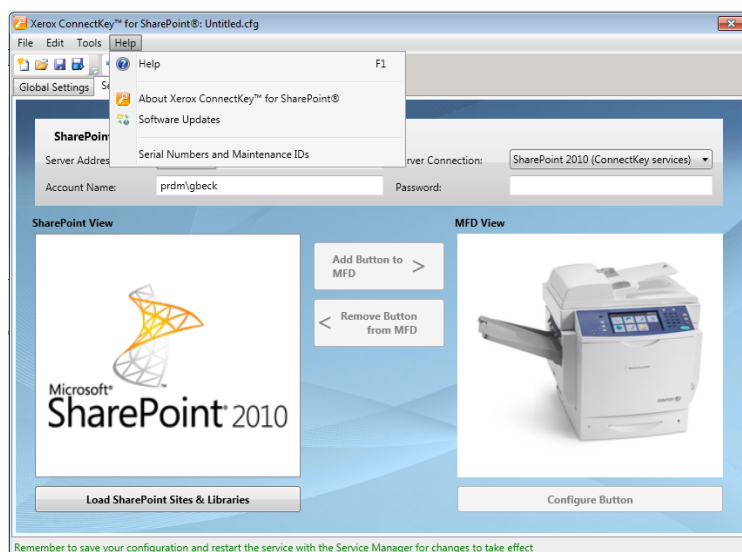
Devices can be removed or edited by selecting them from the registration group and selecting the appropriate action from the toolbar. When editing, the parameter window for “adding a device” will be presented. See “adding a device to the registration group” for details.

Serial Numbers & Maintenance Contract IDs

ConnectKey for SharePoint allows you to store the Xerox Serial Number and Maintenance contract ID you received with your ConnectKey for SharePoint purchase.

Upon first launch of ConnectKey for SharePoint, no serial numbers will be present and the application will prompt you to enter one or more Xerox Serial Numbers. If you decline to enter any numbers, the prompt will remind you on each subsequent launch of ConnectKey for SharePoint until one or more serial numbers have been entered.

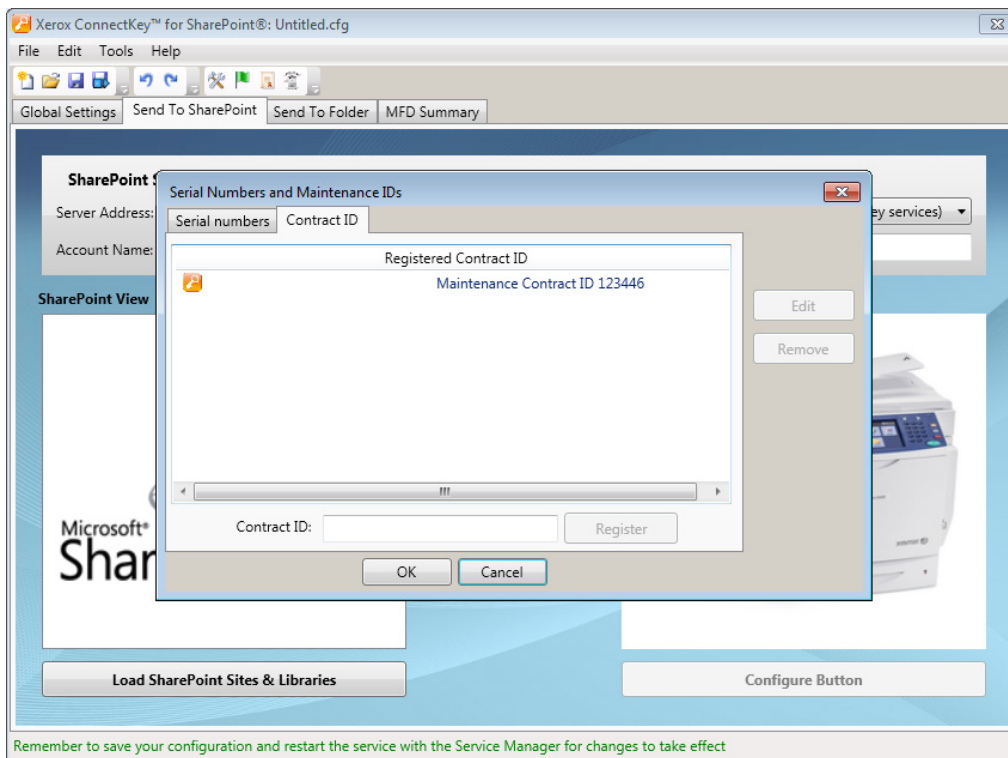
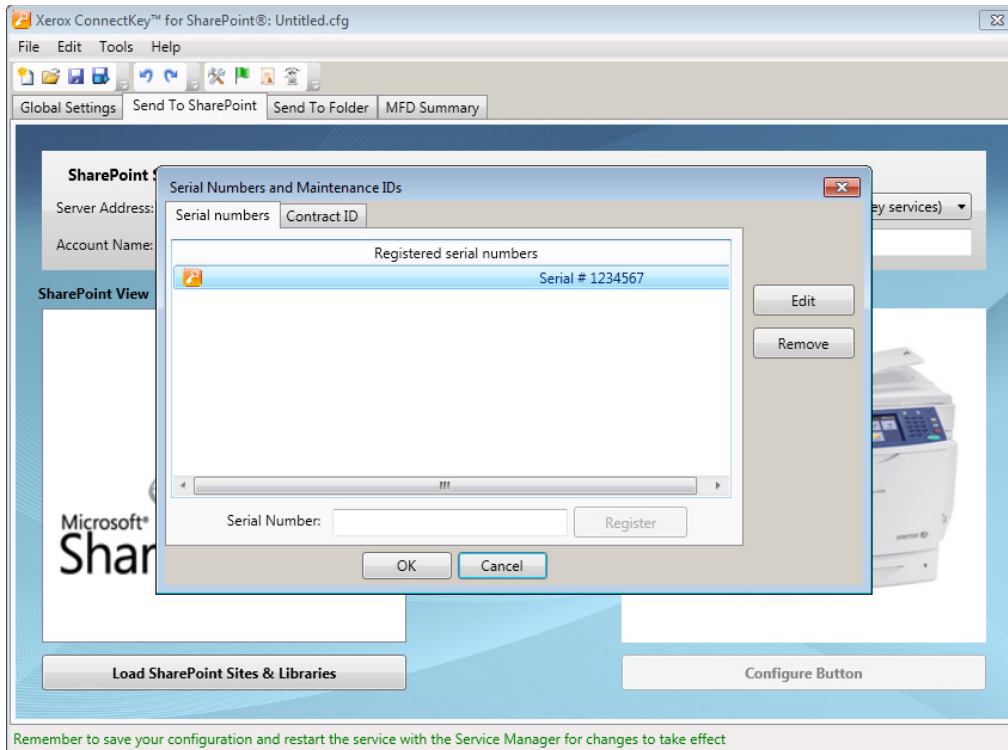
You can view your serial numbers and maintenance contract IDs or add additional ones by selecting the option from the Help Menu.



Serial numbers and maintenance contract IDs are not validated when entered and are stored with ConnectKey for SharePoint for convenience when contacting Xerox Support, transferring licenses to other servers, etc. Serial numbers may be used when ordering additional licenses for ConnectKey for SharePoint to enable more MFPs.

Serial Number and Maintenance Contract ID should be stored when converting from a trial license to a permanent license.

Serial Numbers



Software Updates

8

The software update process is different depending upon your geographical location.

For Canadian customers, software updates may be downloaded directly from <http://www.xerox.com/connectkeysharepointlicense>. This is the webpage from where you initially downloaded the Xerox ConnectKey for SharePoint software. Once you log in, expand the list under the Select Product heading. Software updates display in the resulting list. Documentation regarding the installation of the updates is available in the Product Documents just below the software download menu.

For all other locations, if Xerox releases any updates to the ConnectKey for SharePoint software, they will be made available through the Software Update Service. You can access this utility from the Help Menu. The Software Update Service will display a list of any available updates for ConnectKey for SharePoint. Download and run these individually outside of normal production hours, as the ConnectKey for SharePoint server is temporarily unavailable for scanning during this process.

The software updates are always available and downloadable regardless of maintenance status. Customers who are not current on maintenance will be able to download any updates made available for ConnectKey for SharePoint. During installation of the update, a check for maintenance status occurs. If maintenance is expired, you are provided instructions and prompted to enter a valid maintenance contract ID.

If no valid maintenance contract ID is entered, you will be forced to cancel the software updates.

General Administration Items

9

ConnectKey for SharePoint Logs

Log File Location Details

By default, log files will be located in the installation directory. The path for log files is a configurable setting, as identified by the ConnectKey Service Manager. Log files contain all system information divided into categories (task or batch). These files are intended for troubleshooting and are overwritten after seven days.

If you wish to maintain log files longer than the system default it is the vendor recommendation to create a backup routine to migrate these files to a safe storage location.

WARNING



Please note that log files may contain information used for file naming and SharePoint Indexing. If any of this information is known to be sensitive user information, it is recommended that access to these files should be restricted. Further, depending on the sensitivity of the data, admin users, such as Administrator, should have the proper data security clearance/certification (for example: HIPPA, DOD, HR). Appropriate measures should be taken for any personnel with access to this data.

Best practice is to change the default log path to a folder, which has restricted access and can only be written/read by the ConnectKey for SharePoint service account and authorized users.

Basic Troubleshooting

Troubleshooting Tips

The following are some general troubleshooting tips that should be checked before contacting Xerox Support.

ConnectKey for SharePoint Application Button is not on the MFP or does not execute

1. Ensure the ConnectKey for SharePoint service is running.
2. Validate the device is in the list of registered devices.
 - a. If the device is not in the registered device list, ensure you have adequate licenses for the device, and add the device to the Registered Devices list (see License Manager).
 - b. If the device is in the list of registered devices, Register device again. Verify registration is successful (i.e., green).
3. Validate network connectivity between the Xerox EIP MFP and the ConnectKey for SharePoint Server via a ping test.
4. Check for firewall or antivirus interference at both the ConnectKey for SharePoint Server and the network level.

Document did not Reach Its Expected Destination

Documents may fail to reach the expected destination for many reasons. When this happens, the document will be routed to the general reject folder (see Global Settings). An administrator should check this folder on a regular basis. Additionally, it is recommended that email notification options (see Global Settings) be enabled so that a more proactive approach can be taken. If there is a scan failure, consulting the ConnectKey.log file (located in the ConnectKey for SharePoint installation folder) is the best way to determine the cause of the failure. Based on this information, the scan may be tried again after the underlying issue has first been resolved. Some common causes for a failure are:

- The target system is unavailable.
- The network is experiencing issues.
- The ConnectKey for SharePoint server license has not been licensed or may have expired (see License Manager).
- The scan never completed at the MFP. This will be indicated by a “scan transfer failed” message on the MFP and indicates that the document was never sent to the ConnectKey for SharePoint server for final routing.

- No email notification has been sent when a scan document fails to reach its expected destination.

No Email Notification has been Sent When a Scan Document Fails to Reach Its Expected Destination

- Validate that the expected recipient(s) is on the recipient list (see Notification Options).
- Check for firewall or antivirus interference at both the ConnectKey for SharePoint server and the network level.
- Check spam filter for email recipient.

ConnectKey for SharePoint Service will not Start (or Stops Immediately)

- Check that the service account being used to run ConnectKey for SharePoint (see Service Manager) has not been disabled and that the password is accurate.

Document did not Convert to the Desired Output Format (PDF, PDF/A, XLS, DOCX) with Satisfactory Results

The quality of the document conversion is related in part to one or more of the following factors:

- Poor quality original document (documents that have already been photocopied or faxed, etc)
- Hand written documents (these cannot be properly OCR'd)
- Poorly formatted documents (pertains mostly to XLS formats that require good table structure)
- Faster OCR Processing has been enabled (see Scan Settings)
- Image Quality Scan Settings need to be adjusted (see Scan Settings)

Document Processing Time is Unsatisfactory

ConnectKey for SharePoint uses a state of the art OCR Engine for high quality document conversion. Document processing speed is related in part to one or more of the following factors:

- Document size: The higher the number of pages in a document, the longer the processing time.
- Document complexity: Pages with large amounts of text and images require more processing time.
- Other documents in the queue: ConnectKey for SharePoint is a server based application and all documents scanned from any MFP will be processed in a first-come, first-out (FIFO) manner. As such, if a large document or many documents are in the queue, subsequent documents will be processed afterwards.
- The toggle setting for Faster OCR Processing (see Scan Settings).
- Color Documents scanned in color require more processing time.

ConnectKey for SharePoint does not connect to the SPS Server to display a list of libraries and folders

- Ensure that the ConnectKey Web Service Extension has been installed on the SPS Server (see Installation Guide).
- Ensure that the SPS Server is online.
- Check that the account used to access the SPS Server has correct permissions.
- For SPS residing in a domain, ensure the Account name is entered in the correct format, i.e., Domain\username.
- Check that the version of SPS is correct (Toggle setting for SPS 2013, SPS 2010, or SPS 2007).
- General network issues.

Color Document Output was selected but the output file was black and white

If the MFP is not color capable, the output will default to B&W regardless of scan setting chosen.

