MFP

TT-032916_4R

TECHNICAL TIP

Models: **MX-3070N / 3570N / 4070N**
MX-3050N / 3550N / 4050N
MX-5050N / 6050N
MX-5070N / 6070N

Priority Medium

Date: June 2017

Subject: **Active Directory® Integration**

Active Directory® Integration for the MX-3070N/3570N/4070N, MX-3050N/3550N/4050N, MX-5050N/6050N, MX-5070N/6070N

Updated June 16, 2017

Introduction to Active Directory Integration

The new color Advanced and Essential series have a couple of new advanced security features. One of these features includes Active Directory integration. This is designed to help IT administrators implement stronger, controlled security on these MFPs. An Active Directory registered MFP is a trusted resource which allows secure communication and transaction within the network.

Benefits of Active Directory Integration include:

- Secure and trusted user authentication and network communication
- Single-Sign-On to network resources via secure token
- Seamless user access to
  - Scan to network folders
  - Scan to home directory
  - Scan to email
- Active Directory user authentication for printing
- Enhanced printer management using Active Directory

In this document, you will find the following Active Directory related settings and instructions:

1) Active Directory Registration
2) Active Directory Authentication
3) ID Card Settings for Active Directory Authentication
4) Single-Sign-On to Active Directory Resources
5) Printing in the Active Directory Integrated Environment
6) FAQ
   - 6-1. Which models are supported?
   - 6-2. What is the structure of the AD/LDAP Directory Information Tree for Active Directory?
   - 6-3. What is the available MFP information in AD?
   - 6-4. Why can't I register the MFP to AD?
   - 6-5. How can I map MFP authority group/user control?

1. Active Directory Registration

In order to take advantage of the Active Directory integrated environment, the target MFP needs to be registered with the Active Directory. All attributes required for the MFP to join the domain need to be set at the device's Web page. With the firmware (released in May 2017 and later), these MFPs can be registered as a computer and visible in the AD console.

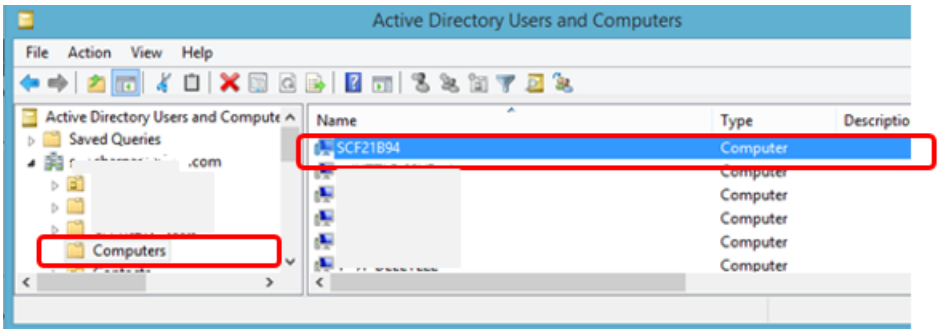


Figure 1: Active Directory Console. MFP registered as a computer

Basic settings to connect Active Directory:

- System Settings >Network Settings >Active Directory Settings >Domain Name
- System Settings >Network Settings >Active Directory Settings >Search Attribute

Device registration with Active Directory:

- System Settings >Network Settings >Active Directory Settings >Device Registration Account: User Name*
- System Settings >Network Settings >Active Directory Settings > Device Registration Account: Password*

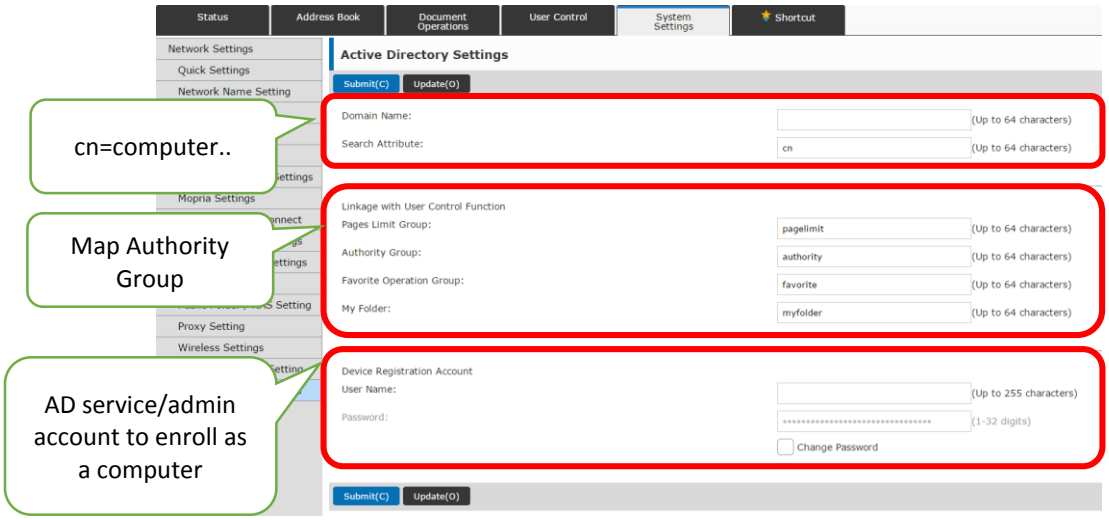


Figure 2: MFP Device Web Page Active Direction Settings

*The Active Directory user account which can write to CN=computers is required to register MFP to AD.

2. Active Directory Authentication

Since the MFP joins the domain, a stronger user authentication becomes available. "Active Directory Authentication" is added as one of the options for user authentication. The authentication can be enabled on the device's Web page:

- User Control >Default Settings >User Authentication: Enable
- User Control >Default Settings >Authentication Server Settings: Active Directory

Options for user authentication:

- **Login Locally**
  Authentication performed using a user list created and stored locally on the MFP
- **LDAP Authentication**
  Authentication performed against the LDAP server
- **Active Directory Authentication**
  Authentication performed against the Active Directory server, which allows Kerberos token-based authentication with stronger security

<MFP Device Operation Panel Authentication Screen>

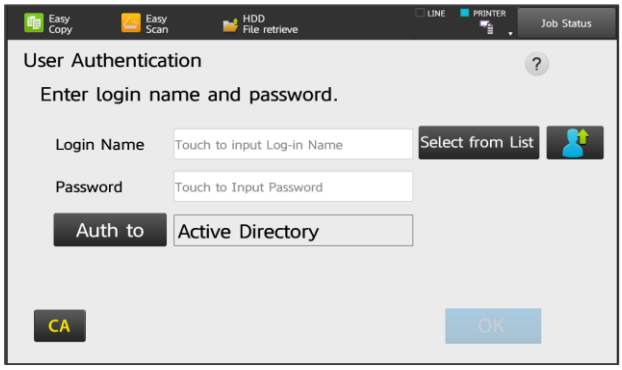


Figure 3: MFP Operation Panel User Login Screen

3. ID Card Settings for Active Directory Authentication

For a simplified user experience, ID card authentication can be used. Please follow the settings below to enable ID card authentication in the Active Directory integrated environment. ID card registration supports up to 1,000 users per device.

3.1 Common Settings to Enable ID Card Authentication

After registering the MFP with Active Directory, the following "User Control" settings on the MFP need to be configured:

- User Control >Default Settings >User Authentication: Enable
- User Control >Default Settings >Authentication Server Settings: Active Directory
- User Control >Default Settings >Use IC Card for Authentication: Tick the box to enable

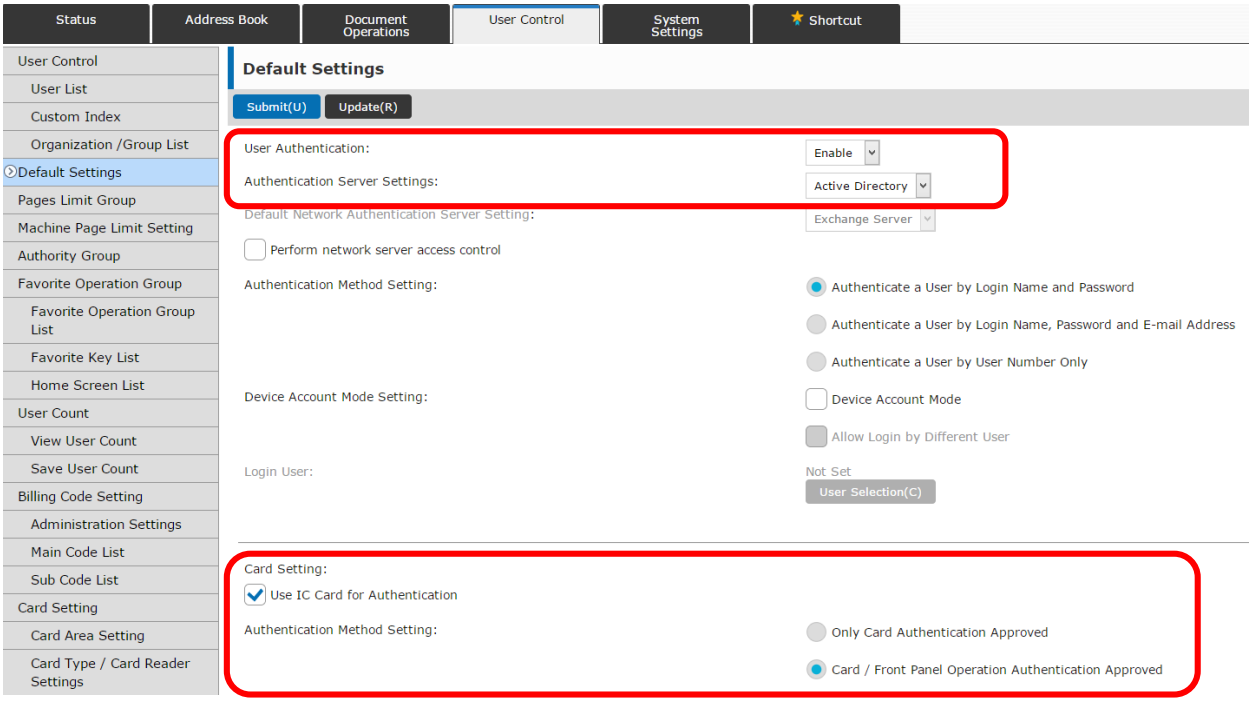


Figure 4: MFP Device Web Page User Authentication Settings

3.2 ID Card User Self Registration

ID card self-registration is available by eliminating a burden of the IT administrators to register and manage ID cards. Each user can simply walk up to the MFP and register his/her ID card.

<Device Operation Panel ID Card Authentication Screen>

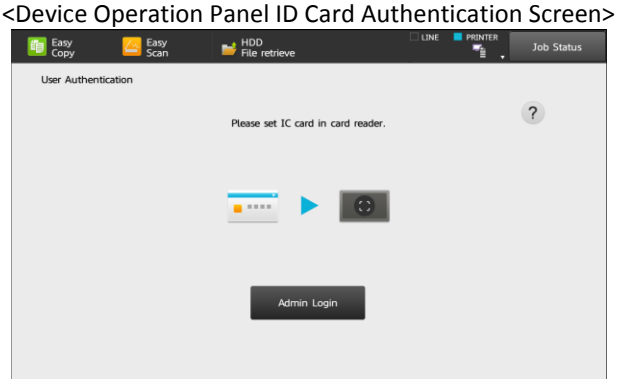
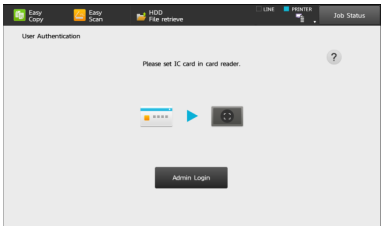


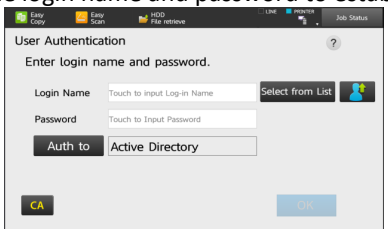
Figure 5: MFP Operation Panel ID Card Login Screen

ID Card User Self-Registration Workflow

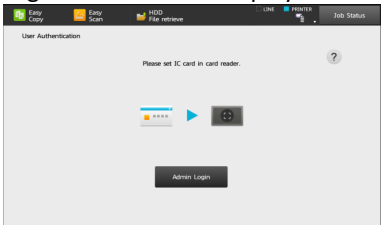
1) Swipe a card to log on to the MFP



2) For the first time user, enter the login name and password to establish a successful login.



3) The ID card is registered with the user. Simply swipe the ID card to logon to the MFP next time. When the password is changed, a manual login screen will be displayed to enter the updated password.



3.3 ID Card Setting Options

There are two modes available for the ID card to meet an organization's security and operation requirements. Please select the mode and follow the settings.

Convenience Mode

The convenience mode provides a service for the organization when productivity and convenience are of primary importance. The MFP stores user name and password on the MFP device at user's first time log in. The next time, the user can simply use his/her ID card to log on to the MFP, eliminating manual typing of credentials, while securing the access to the device as well as for activity logging, and more.

Settings:

- User Control >Default Settings >Cache User Information: Tick the box to enable
- User Control >Default Settings >User IC Card for Authentication: Tick the box to enable
  - Only Card Authentication Approved (Login Option)
  - Card/Front Panel Operation Authentication Approved (Login Option)

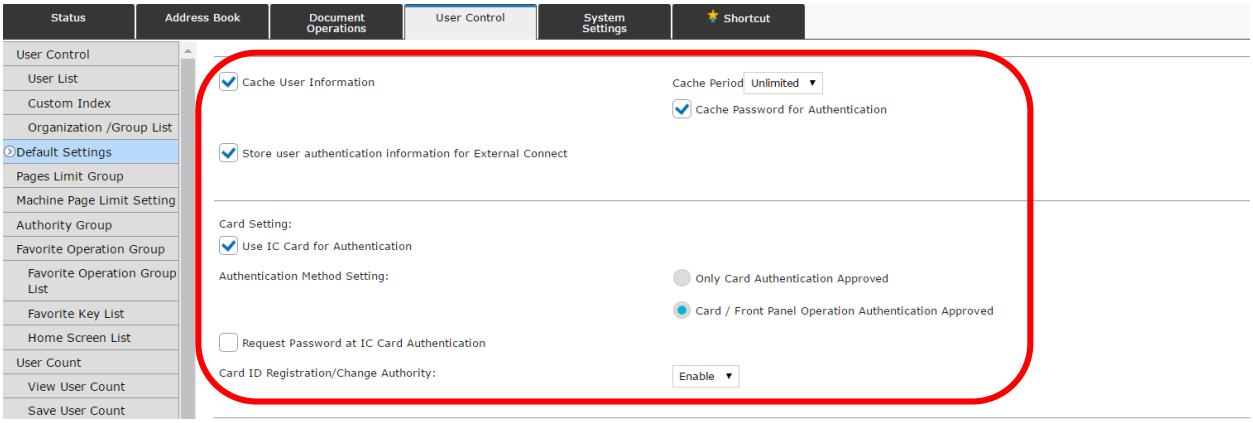


Figure 6: MFP Device Web Page ID Card Configuration Screen

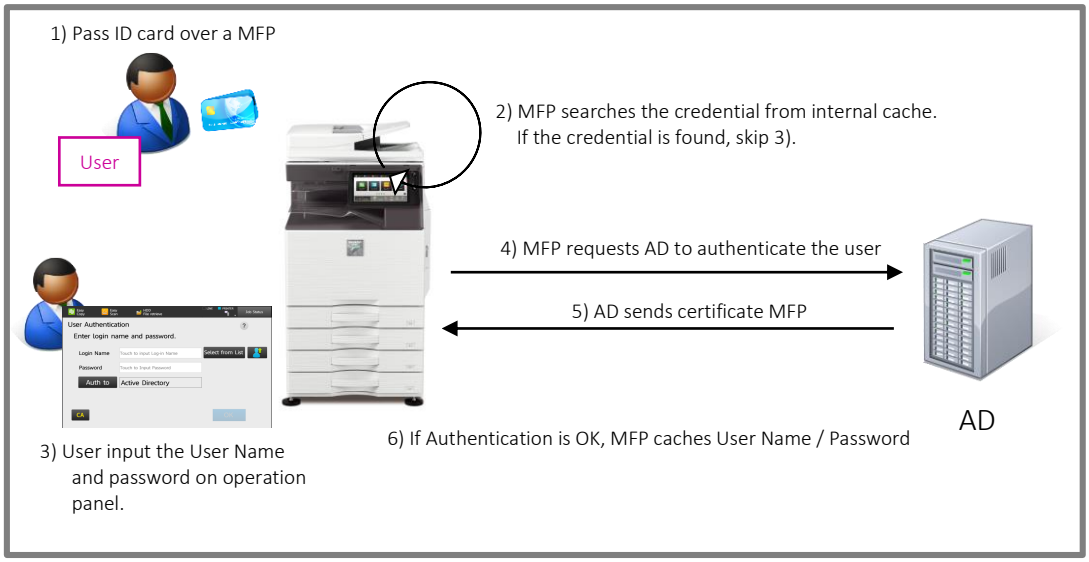


Figure 7: Convenience Mode

Secure Mode

The secure mode is designed for more security conscious organizations. It is more secure as passwords are not stored on the MFP. Only the user name and ID card information are stored at user's first time login. When the user logs on to the MFP with the ID card, the user simply types in his/her password.

Settings:

- User Control >Default Settings >Cache User Information: Disable

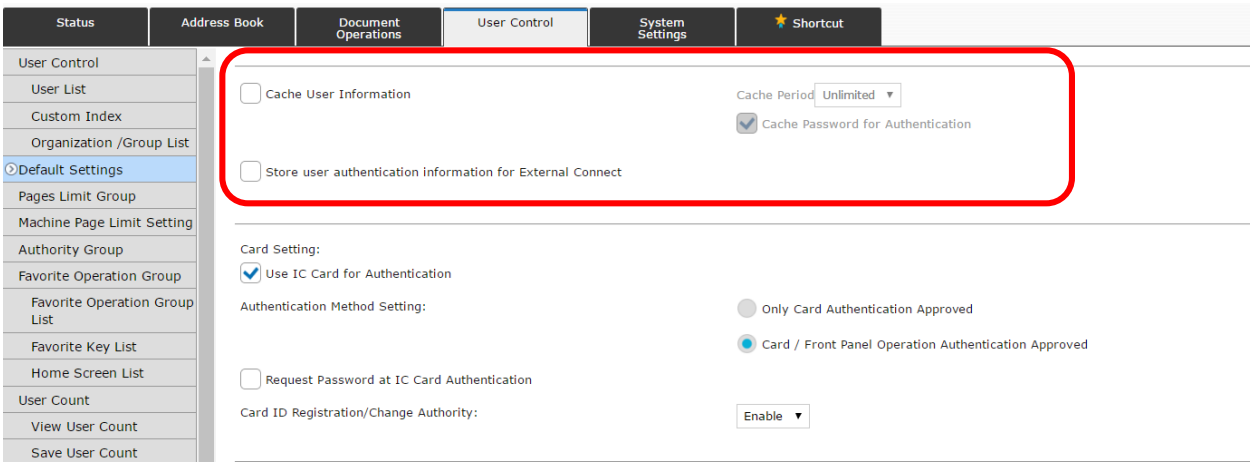


Figure 7: MFP Device Web Page ID Card Configuration Screen

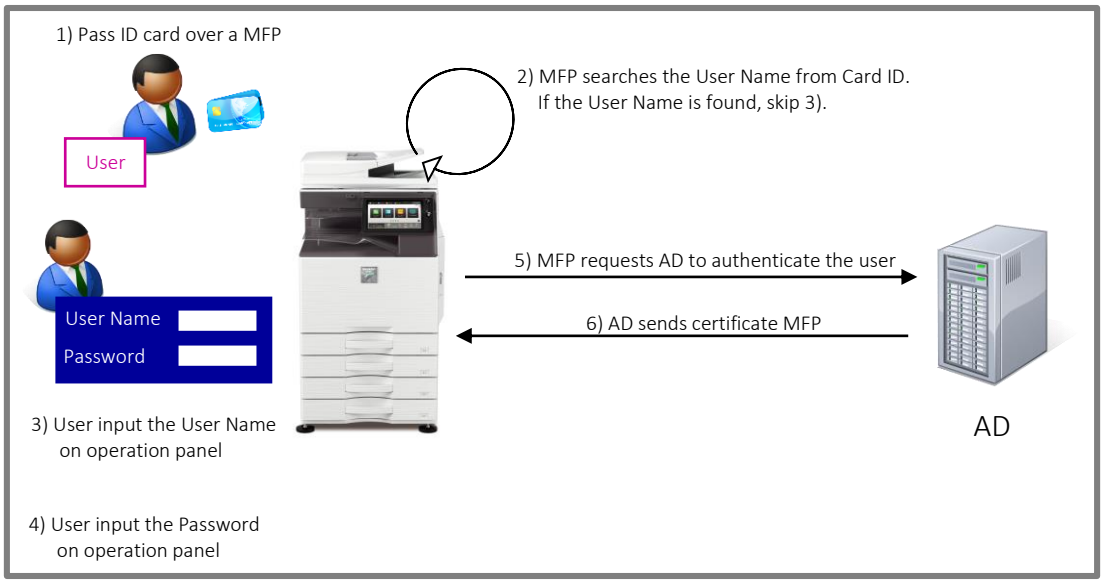


Figure 8: Secure Mode

4. Single-Sign-on (SSO) to Active Directory Resources

Once the MFP is registered with Active Directory, the MFP can establish Single-Sign-On and securely access to network resources.

Improvements of “Scan to folder” and “Scan to email” include:

- **Scan to Folder**
  Scan to folder is more secure and seamless in the AD integrated environment. Once authenticated, users do not have to enter their user name and password to access the folder from the MFP. They can browse folders and subfolders to locate scan destinations.

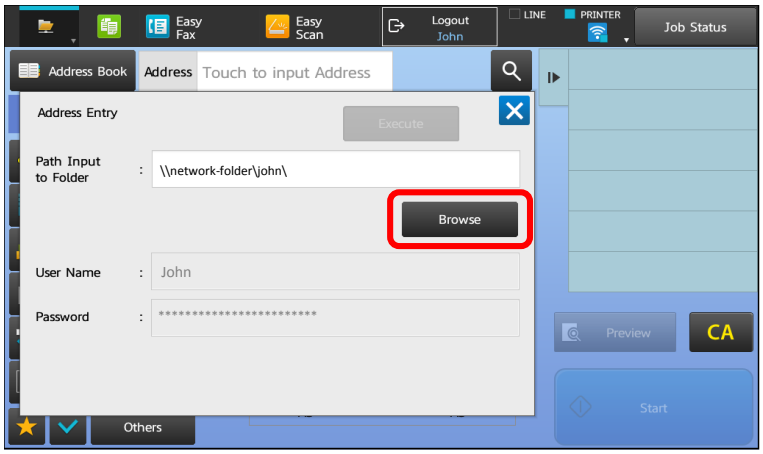


Figure 9: MFP Operation Panel Scan to Folder User Interface

The default value of “Path Input to Folder” is Home Directory. Home Directory is displayed as a default destination in the Path field. When the Path field is blank, select “Browse.” Home Directory path will be displayed when available. If not, the screen to browse the network will be displayed.

Selecting destinations from address book
When the credentials (user name and password) are set for the registered folder in the address book, the registered credentials are used to access the folder. When the credentials are not set in the address book, logged in user credentials are used to access the folder.

- **Scan to Home Directory**

  Using Kerberos token, scan to home directory is both seamless and secure. IT administrators can maintain and manage information security with control while providing convenience to end customers. The logged in user's home directory can be set as a default destination. The home directory will be auto-populated in the address field on the MFP operation panel.

  Device Web page settings:

  - System Settings >Image Send Settings >Scan Settings >Default Address >Default Address Settings: Enable
  - System Settings >Image Send Settings >Scan Settings >Default Address >Add Selected: Apply Home Directory of the user for login

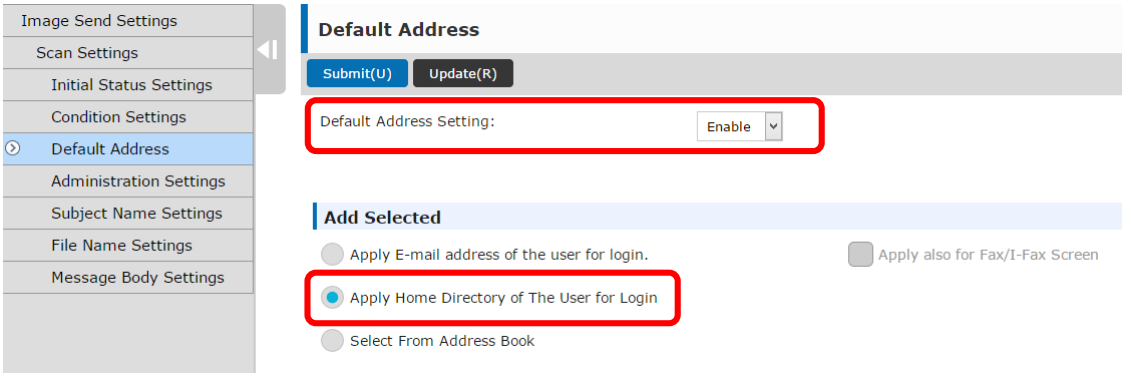


Figure 10: MFP Device Web Page Default Address Settings

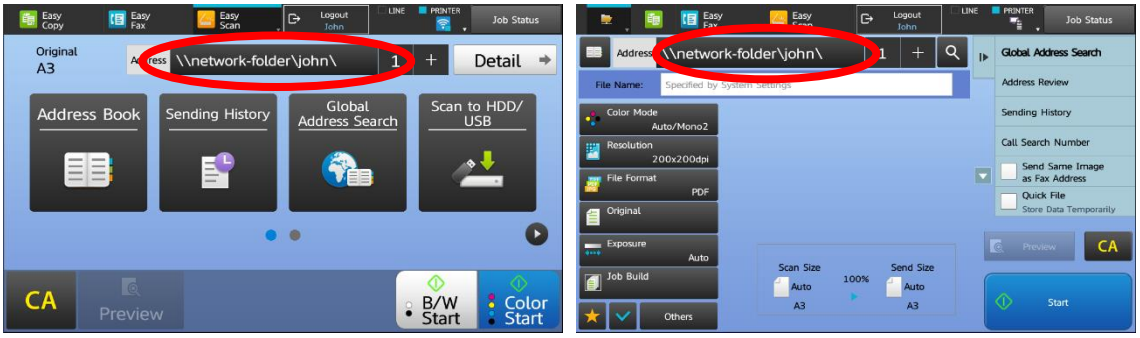


Figure 11: MFP Operation Panel Easy Scan and Scan to Folder User Interface

- **Scan to email**

  Scan to logged-in user (Scan to me) is easier and more secure. The MFP obtains the logged in user's email address from Active Directory and seamlessly establishes scan to me workflow. The logged in user's e-mail address can be set as a default destination, The email address will be auto-populated in the address field on the MFP operation panel.

  Device Web page settings:

  - System Settings >Image Send Settings >Scan Settings >Default Address >Default Address Settings: Enable
  - System Settings >Image Send Settings >Scan Settings >Default Address >Add Selected: Apply E-mail address of the user for login

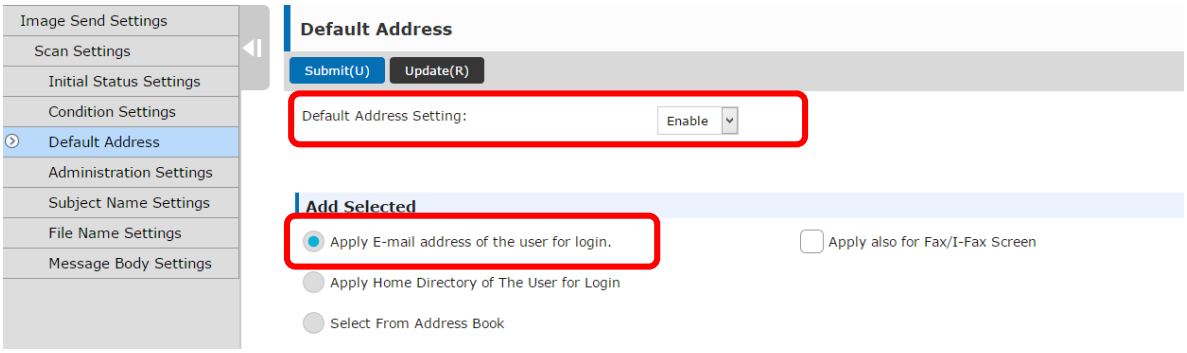


Figure 12: MFP Device Web Page Default Address Settings

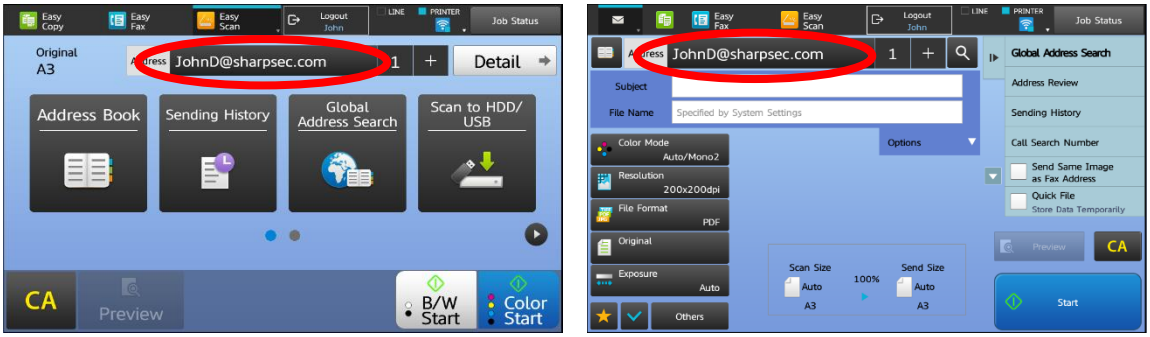


Figure 13: MFP Operation Panel Easy Scan and Scan to Email User Interface

- **Scan with Exchange Connect Feature**
  Color Advanced and Essentials series offer seamless integration with Exchange server. With the combination of AD integration and Exchange connector, the access to exchange server is secured with the Kerberos token. No information is stored on the MFP and it provides seamless scan to email experience for your users.

- **SSO to Cloud Services**
  The color Advanced and Essential series has an "Email/Cloud Connect" feature to print from and scan to popular cloud services including:
    - Gmail™ webmail service (OAuth)
    - Exchange Online/Office365®
    - Google Drive™ (OAuth)
    - OneDrive® for business
    - SharePoint® Online
    - Box (OAuth)

  When MFP user authentication is enabled, Single-Sign-On can be enabled to log on to these cloud services for convenience. Users will be asked to enter cloud login information at the first time they use these connect features. Either OAuth or credential is stored on the MFP used to establish SSO. The stored information is encrypted but if the security is a concern, only the user ID is stored and a password is requested when users access to such services, or completely disable single sign on to these cloud and email services.

  Device Web page settings:

  - System Settings >User Control >Default Settings >Store user authentication information for External Connect > Enable or Disable

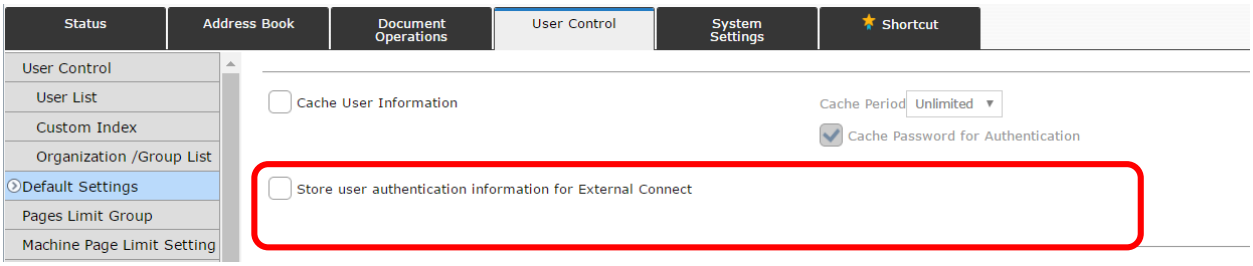


Figure 14: Cloud and Email Connect SSO enable/disable

- **Scan Restriction**
  IT administrators have a better control in users scanning actions. Restrictions such as “scan only to home directory” or “scan only to logged-in users email address” as well as domain and destination entry restrictions can easily be set on the MFP device’s Web page.

  - System Settings >Image Send Settings >Scan Settings >Default Address >Default Address Settings: Enable
  - System Settings >Image Send Settings >Scan Settings >Default Address >Add Selected: “Apply Home Directory of the user for login” or “Apply E-mail address of the user for login”
  - System Settings >Image Send Settings >Scan Settings >Default Address >Add Selected: Allow cancel of the first entered address

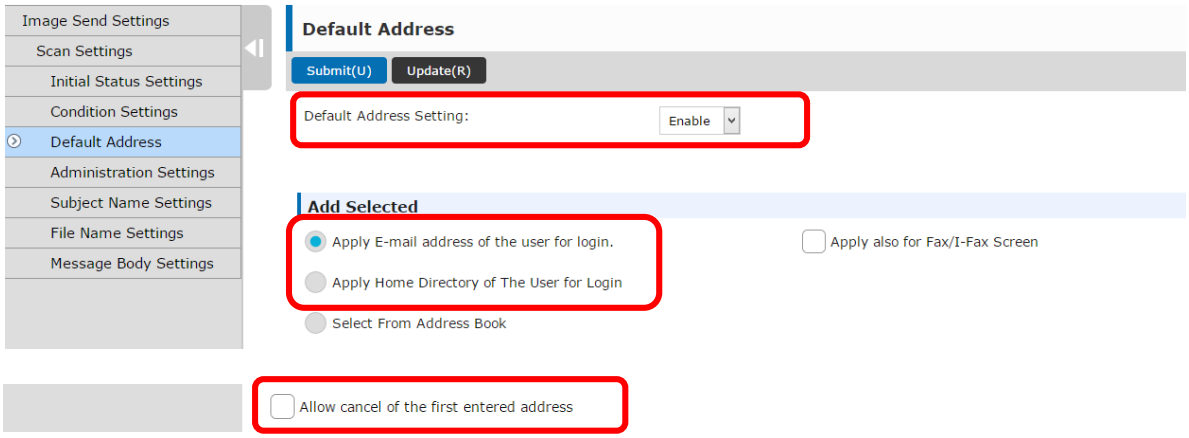


Figure 15: MFP Device Web Page Default Address and Restriction Settings

5. Printing in the Active Directory Integrated Environment

- **Printing form Sharp Print Driver**

When Active Directory authentication is selected, user authentication is requested. Sharp print driver is being enhanced to deliver an ultimate printing experience with security. When “Single-Sign-On” is selected under the “Job Handling” tab, Sharp MFPs authenticate print jobs via the Kerberos token, which was generated when each user logs on to their PC/laptop, allowing seamless and trusted printing requests.

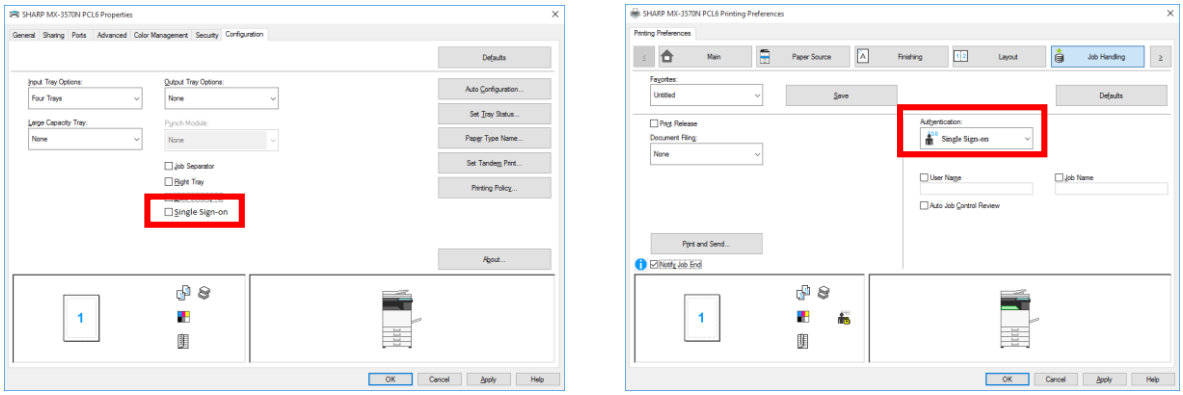


Figure 16: MX-3070N Windows Print Driver Job Handling Interface

- **Serverless Print Release**

When “Print Release” is ticked, it enables Active Directory authentication for “Serverless Print Release.” Please refer to the Print Release Settings Guide for more details.

- **Mobile Printing**

User authentication needs to be enabled when printing from on Windows®, Mac®, and select mobile printing applications including Sharpdesk® Mobile in the Active Directory integrated environment.

When Single Sign-on of the configuration tab in the print driver is enabled, the driver searches the MFP status. If the MFP is not registered to the domain, an error message will be displayed. When auto-configuration is selected, the driver searches the MFP status. If the MFP is registered to a domain, the “Single Sign-on” in the configuration tab will be turned on.

6. Frequently Asked Questions (FAQ)

6-1 Which models are supported?
6-2 What is the structure of the AD/LDAP Directory Information Tree for Active Directory?
6-3 What is the available MFP information in AD?
6-4 Why can't I register the MFP to AD?
6-5 How can I map MFP authority group/user control?

6-1. Which models are supported?

The following models support AD integration:

- MX-3070N/3570N/4070N
- MX-3050N/3550N/4050N
- MX-5050N/6050N
- MX-5070N/6070N
- MX-6580N/MX-7580N (MFP joins as a printer. Kerberos token based SSO with print driver is not available.)
- MX-M905 (MFP joins as a printer. Kerberos token based SSO with print driver is not available.)

6-2. What is the structure of the AD/LDAP Directory Information Tree for Active Directory?

In the Active Directory, OU and Container (CN) for the system need to be configured in order to register the MFP to the domain.

- [Built in] : Defined Security Group is stored
- [Computers] : Client Computer is stored
- [Domain Controllers] : Domain Controller is stored
- [System] : Setting related to domain object is stored
- [Users] : Defined User Account and Security Principal are stored

Active Directory Structure for MFP

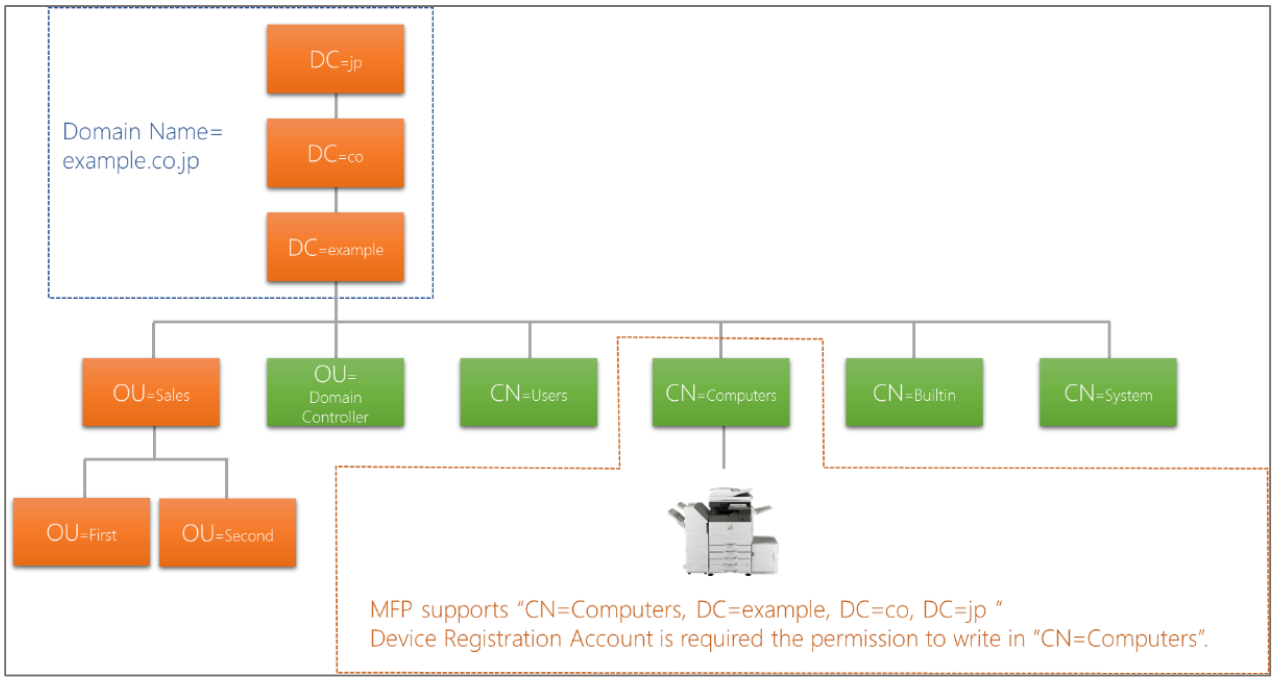


Figure 17 AD Structure

How you see the registred MFP in AD

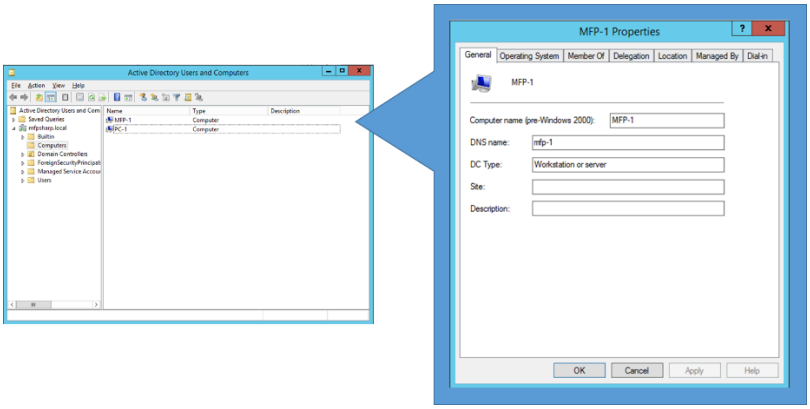


Figure 18 Registered MFP in A

6-3. What are the available MFP information in AD?

The following is the value examples and attributes for MFP.

Items	Attributes	Contents	Value Example
Server Name	serverName cn	Network Settings>Network Name Settings>Device Name	SC651EEC
Location	location	Common Settings>Machine Identification Settings>Machine Location	Nara Office 6F
Description	description	Common Settings>Machine Identification Settings>Memo	Sharp Printer

6-4. The MFP cannot connect to AD/the MFP cannot be registered.

When you encounter an issue that the target MFP cannot be registered or connected to AD, please check the following:

a. Reboot the MFP
b. DNS settings
c. Device registration account
d. Active Directory attribute settings
e. Clock adjust settings
f. Confirm Reverse Lookup Zone in DNS
   MFP require to setup Reverse Lookup Zone for DNS.

a. Reboot the MFP

When the MFP is rebooted, the MFP tries to register itself to Active Directory.

b. DNS setting

Please check DNS is properly set and configured.

c. Device registration account

Please review the proper format for the device registration account is used. Please avoid characters such as “@” or “DOMAIN\”. The device can capture the domain that is used for authentication.

Incorrect:
adminitrator@xxxxx.com
Correct:
Administrator

In addition, please ensure that the account used for device registration has a permission to write to CN=computers.

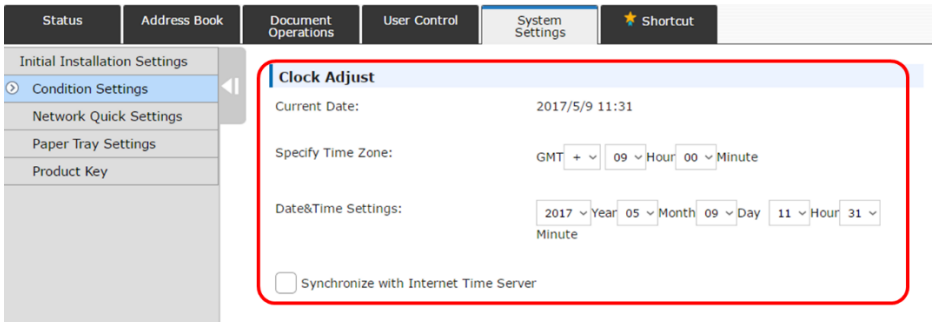
d. Active Directory attribute settings

Please check the attribute settings. it is slightly different from the typical LDAP attribute settings. “CN=computers” needs to be entered in the attribute field for MFP to register as a computer.

Please see more information on AD structure at ***6-2 What is the structure of the AD/LDAP Directory Information Tree for Active Directory?***

e. Clock adjust settings

In AD integration, It is required to set the clock adjust setting of MFP within 5 minutes compared with the time of authentication server.



7) Figure 19 MFP Clock Adjust Settings

f. Confirm reverse lookup zone in DNS

When the time zone is not set properly within the AD, please follow the steps below:

- Create New Zone

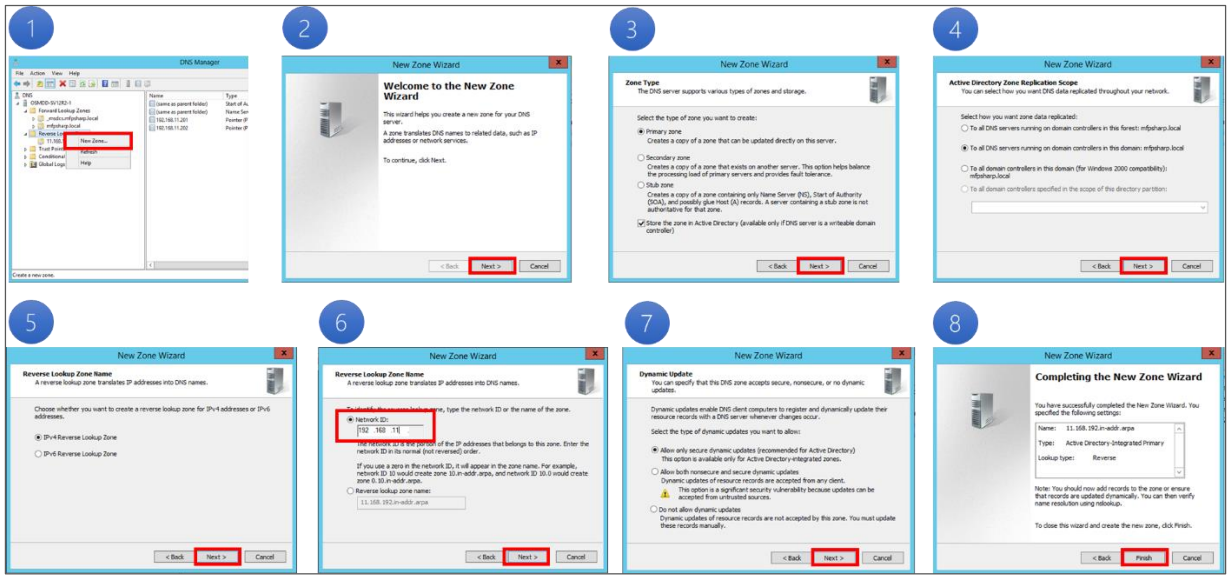


Figure 20 Reverse Lookup Time Zone AD Settings (New Time Zone)

- Create New Pointer

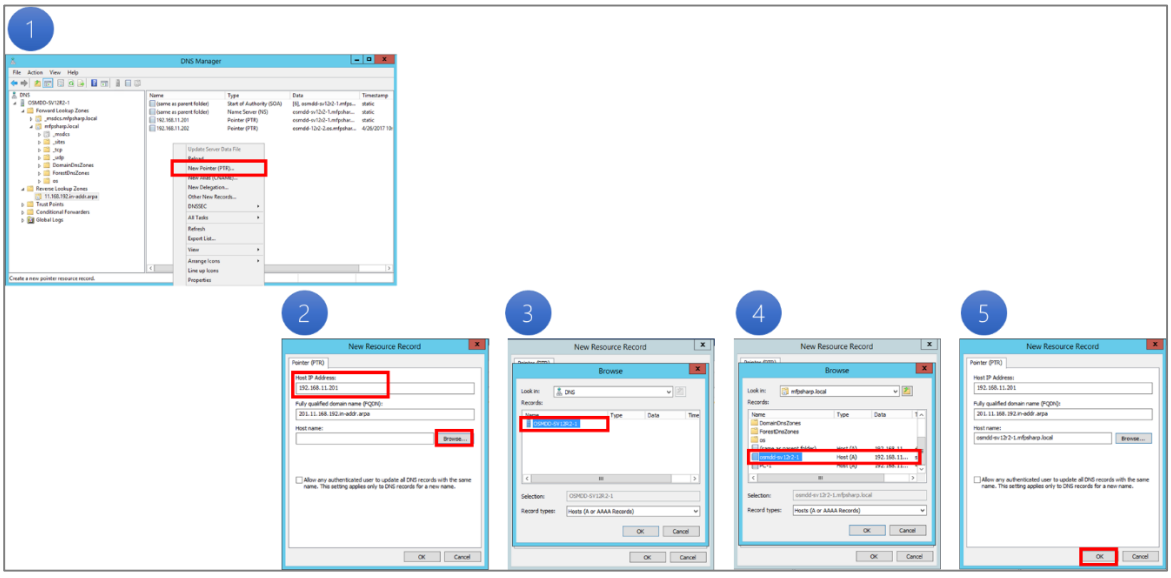


Figure 21 Reverse Lookup Time Zone (New Pointer)

6-1. How can I map MFP authority group/user control?

The MFP AD integration can be mapped to authority and favorite group to provide for IT administrator more control in MFP access including printing preferences/restrictions as well as page limit. Utilizing available attributes, you can configure and map these preferences as described in below.

Available preferences and restrictions:

- Pages Limit Group
- Authority Group
- Favorite Operation Group

The group name that is set for each group can be mapped using available AD attributes.

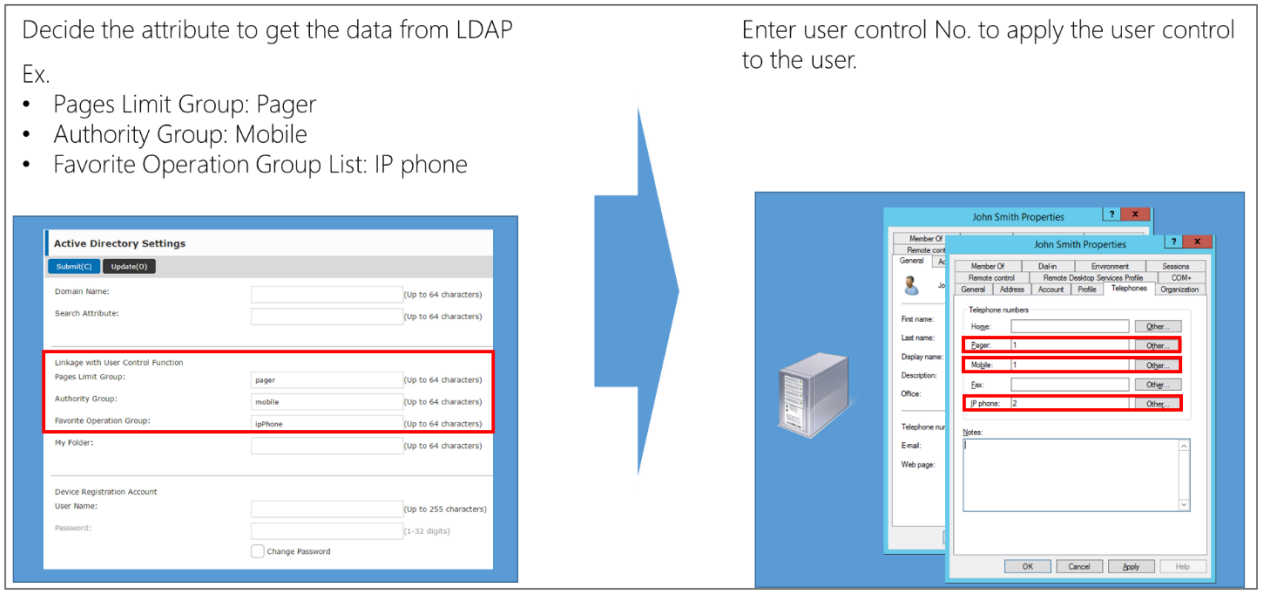


Figure 22 MFP AD attributes mapping

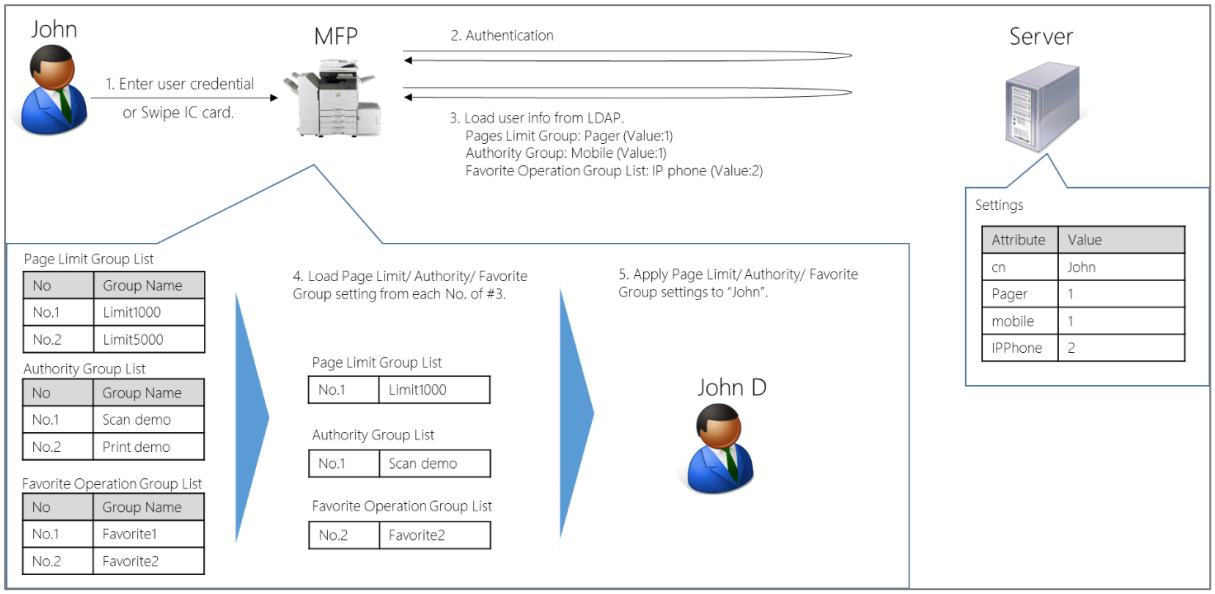


Figure 23 MFP group mapping concept

Active Directory Attribute List

Attribute	Name in AD
givenName	First Name
sn	Last Name
Initials	Middle Name / Initials
cn	Common Name
displayName	Display Name
userPrincipalName	Logon Name
description	Description
telephoneNumber	Telephone Number
mail	Email
wWWHomePage	Web Page
homeDirectory	Home Folder
homeDrive	Home Drive
homePhone	Home Phone
pager	Pager
mobile	Mobile
facsimileTelephoneNumber	Fax
ipPhone	IP Phone
info	Notes
co	Country
company	Company
department	Department
physicalDeliveryOfficeName	Office
title	Title

SHARP ELECTRONICS CORPORATION
100 Paragon Drive, Montvale, NJ 07645
1-800-BE-SHARP • www.sharpusa.com

Document Number 16051
©2017 Sharp Electronics Corporation. All rights reserved.

Design and specifications subject to change without notice. Sharp and all related trademarks are trademarks or registered trademarks of Sharp Corporation and/or its affiliated companies. Microsoft, Windows, and Active Directory are registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective holders.

The information contained within this document is for troubleshooting purposes only to help resolve the issue described. This information is not officially supported by Sharp Electronics Corporation and no warranty is provided, written or implied. Design and specifications are subject to change without notice.

Sharp, Sharp OSA, Sharpdesk, My Sharp, and all related trademarks are trademarks or registered trademarks of Sharp Corporation and/or its affiliated companies. All other trademarks are the property of their respective owners.