

## MFP

TT-20412

**TECHNICAL  
TIP**

MX-M283N/MX-M363N/MX-M453N/MX-M503N  
MX-M623N/MX-M753N

Models: MX-4100N/MX-4101N/MX-5001N  
MX-2610N/MX-3110N/MX-3610N  
MX-4110N/MX-4111N/MX-5110N/MX-5111N

**Priority:** Medium

**Date:** April 2012

**Subject:** Authentication and Access Control with Active Directory and HID Cards

**Description:** MFP users can now be authenticated and controlled using HID access cards and card readers.

**Details:** See the instructions and examples on the following pages to see how to set up the HID card and card reader with Active Directory.

## Network Login Using a USB HID Card Reader with the Aries and Virgo MFP

On the Sharp C-Jupiter II, Jupiter III, Dragon III, Aries and Virgo series MFPs, you can link authority groups, favorite operation groups and page limit groups to unused attribute fields in individual user records in active directory. By using a Custom LDAP address book with LDAP Server Access Control for authentication, network users can be controlled in the same fashion as was previously possible only with local MFP accounts.

However, the Aries and Virgo series have a new field (Card ID) added to the LDAP Server Access Control settings that extends this capability to users with HID cards. This allows them to login into the MFP using network authentication via a HID card!

Using an HID card has several advantages over the normal network authentication method using network user names and passwords:

- The user is authenticated at the MFP to the network with a single card swipe without having to type in a password.
- The user is authenticated at the MFP to the network, even if the user's network password has changed.
- Users without a HID card cannot log into the MFP, even if the user has a network user name and password.
- Users with HID cards cannot log into the MFP if the card IDs have not been entered in to the users' records in Active Directory.
- Once the users HID cards are authenticated to the network for the first time, the users can still log into the MFP with their same permissions when the LDAP server is not available.
- Printing, copying and scanning permissions are granted on login based on the entries in the users' records in Active Directory.
- This method requires no users be created or HID cards registered on the MFP.

The following pages show logon screens seen when using HID cards with different permissions in Active Directory using the Linkage with User Control Function on the Aries or Virgo MFPs.

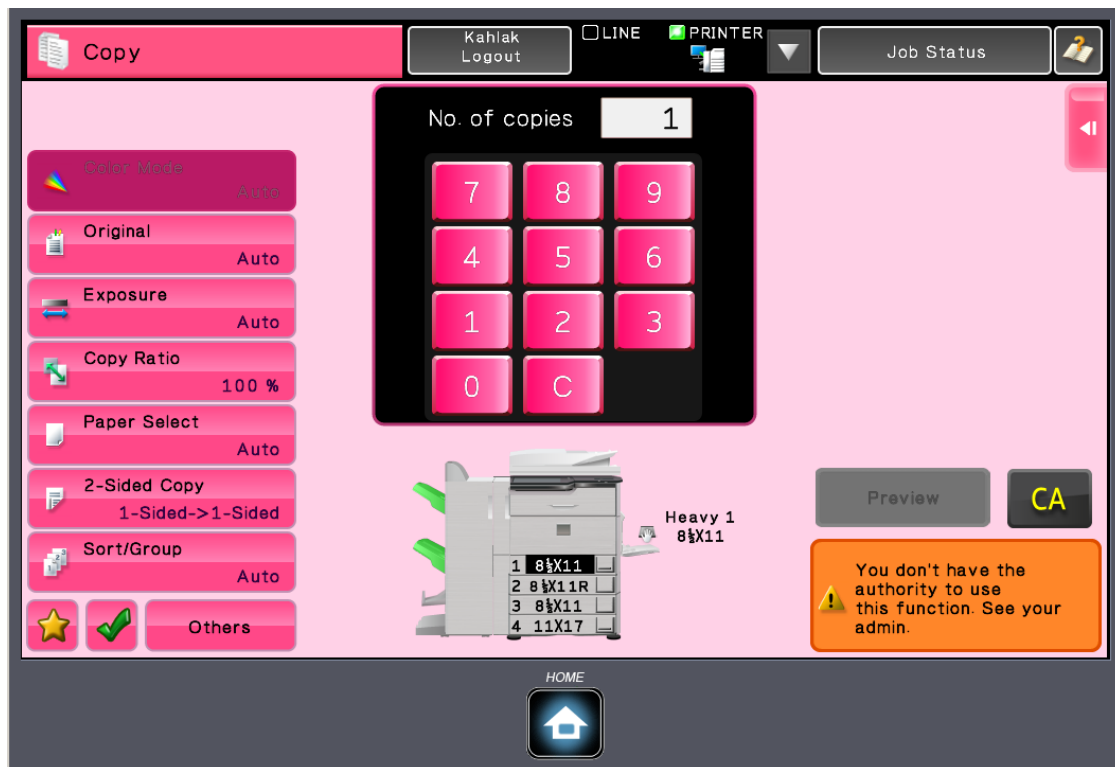
A. User granted full control for Color and Black and White mode operations.



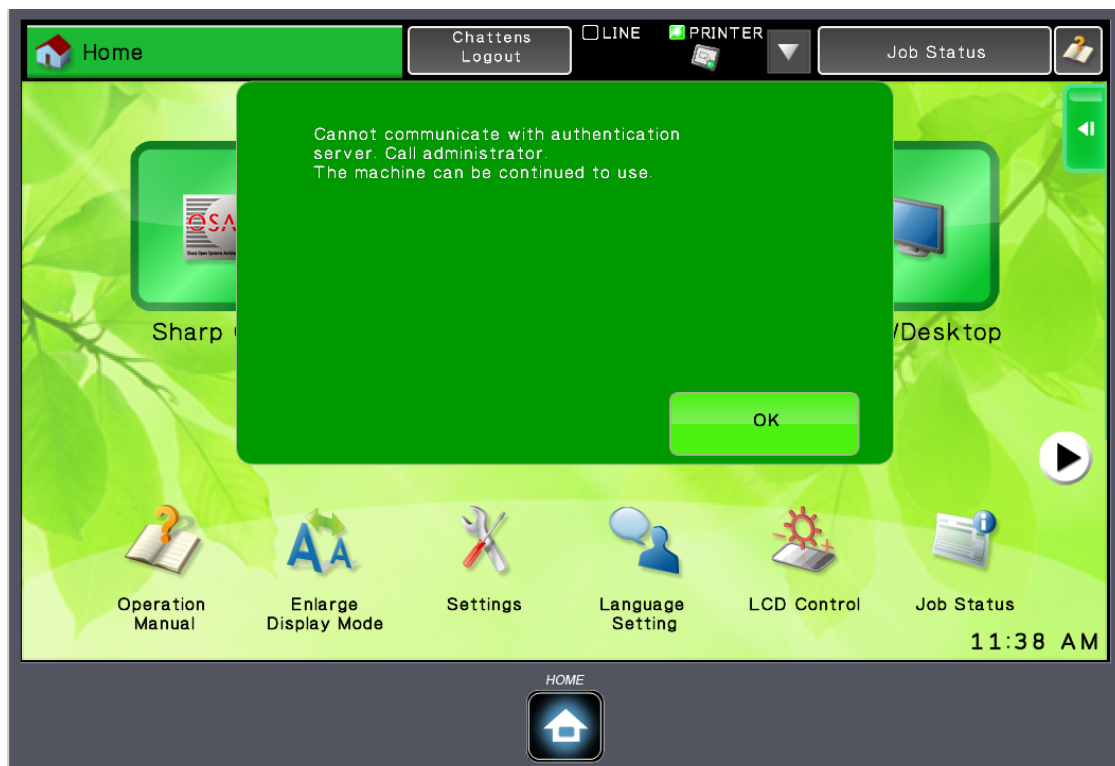
B. User granted only Black and White mode operations.



C. User prohibited from using any functions of the MFP.



D. Screen presented when the LDAP server is not available for a user granted full control. (Pressing the OK button allows access to the MFP panel.)



The following are the steps used to create the custom LDAP server with LDAP Server Access Control with a HID card for network authentication on a Sharp MX-5111N that produced the screens shown above.

NOTE: It is assumed that the MFP has been previously installed and properly configured in the network. Further, full administrative access and knowledge of Active Directory is available.

#### A. Create Authority Groups

1. Navigate to the home page of the MFP.
2. Click on the Login button and login as the Administrator.
3. Click on User Control on the left hand menu item and then click on the Authority Group List sub menu.
4. Click on the Add button and the new Authority Group Registration screen will appear.

**SHARP MX-5111N**

User Name: Administrator Logout(L)

### Authority Group List

Update(R)

Default Group List:

Group Name:	Admin
	System Administrator Authority
	User
	Guest
	Color Prohibited Authority
	Scanner Prohibited Authority

No.	Group Name
Not Set	

Select All(S) Clear Checked(Z)

Add(Y)

5. Name the Authority Group Full Control and select User as the registration model. Click on the Submit button when done.

**SHARP MX-5111N**

User Name: Administrator Logout(L)

### Authority Group Registration

Submit(U) Cancel(C)

Group Name: Full Control (Up to 32 characters)

Select the Group Name to be the Registration Model: User

Switch to Single Screen Mode

Job Settings System Settings

#### Copy

Color Mode Approval Setting:

Black & White:	Allowed
Full Color:	Allowed
2 Color:	Allowed
Single Color:	Allowed

Special Modes Usage: Allowed

Sending while copying: Allowed

Approval Setting to Use Toner Save Mode: ☒ No Toner Save ☐ Toner Save1(Toner Consumption: Much)

- Next, add another Authority Group naming it B&W Only and select Color Prohibited as the registration model. Click on the Submit button.
- Finally, add another Authority Group naming it No Access and select Guest as the registration model. Select Prohibit for all functions on this page and click on the Submit button when done. The Authority Group List should appear as below.

**SHARP MX-5111N**

User Name: Administrator Logout(L)

### Authority Group List

Update(R)

Default Group List:

Group Name:

- Admin
- System Administrator Authority
- User
- Guest
- Color Prohibited Authority
- Scanner Prohibited Authority

Group List:

No.	Group Name
<input type="checkbox"/> 1	Full Control
<input type="checkbox"/> 2	B&W Only
<input type="checkbox"/> 3	No Access

Select All(S) Clear Checked(K)

## B. Create Favorite Operation Groups

While numerous changes can be made for a Favorite Operation Group, only the screen background colors will be changed in this example.

- Click on User Control on the left hand menu item and then click on the Favorite Operation Group List sub menu.

**SHARP MX-5111N**

User Name: Administrator Logout(L)

### Favorite Operation Group List

Update(R)

Default Group List:

Group Name :

Following the System Settings

Group List:

No.	Group Name
Not Set	

Select All(S) Clear Checked(K)

Add(Y) Return to the Defaults(C)

Back to the Top on This Page ▲

Update(R)

- Click on the Add button and the new Favorite Operation Group Registration screen will appear. Name this group Green – Full Control and click on the System Settings tab.

**SHARP MX-5111N**

User Name: Administrator Logout(L)

### Favorite Operation Group Registration

Submit(U) Cancel(C)

Group Name:  (Up to 32 characters)

Select the Group Name to be the Registration Model:

Copy Image Send Document Filing **System Setting**

Switch to Single Screen Mode

☒ Enlarge Display Mode

Original Size Detector Setting:

AB-1	Document Glass: A3, A4, A4R, A5, B4, B5, B5R
	Document Feeder: A3, A4, A4R, A5, B4, B5, B5R, 11x17, 8 1/2x14, 8 1/2x11
AB-2	Document Glass: A3, A4, A4R, A5, B5, B5R, 216x330(8 1/2x13)
	Document Feeder: A3, A4, A4R, A5, B4, B5, B5R, 11x17, 8 1/2x11, 216x330(8 1/2x13)
AB-3	Document Glass: A4, A4R, A5, B4, 8K, 16K, 16KR
	Document Feeder: A3, A4, A4R, A5, B4, 11x17, 8 1/2x11, 216x330(8 1/2x13), 8K, 16K

- Scroll down the page to the MFP Display Pattern Settings and select Pattern 4 (green background) from the drop down box and click on the Submit button.

Job Log Security Settings Custom Links Operation Manual Download

Cancel Detection at Document Glass

MFP Display Language Setting:

Key Operation Setting: Time for Accepting Key Entry:  sec.

☒ Disable Auto Key Repeat

Time for Accepting Key Entry of Long Touch:  sec.

Double Tap Interval Setting:  sec.

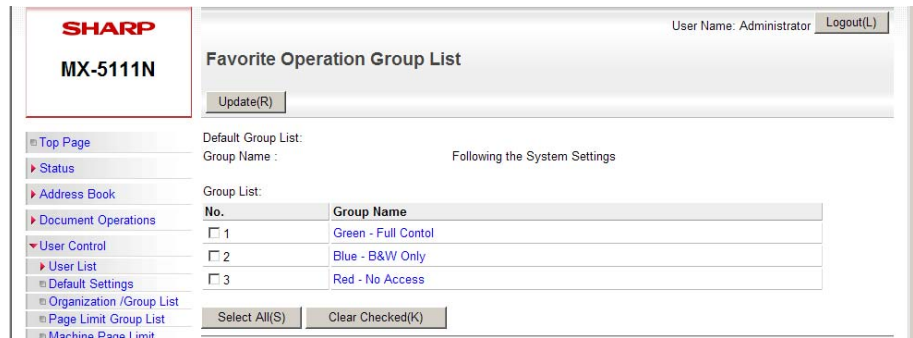
Keys Touch Sound:

☐ Key Touch Sound at Initial Point

Keyboard Select:

MFP Display Pattern Setting:

- Next, add another Favorite Operation Group, name this group Blue – B&W Only and then click on the System Settings tab. Scroll down the page to the MFP Display Pattern Settings and select Pattern 2 (blue background) from the drop down box and click on the Submit button.
- Finally, add another Favorite Operation Group, name this group Red – No Access and then click on the System Settings tab. Scroll down the page to the MFP Display Pattern Settings and select Pattern 6 (red background) from the drop down box and then click on the Submit button. The Favorite Operation Group List should now appear as shown on the next page.



SHARP MX-5111N

User Name: Administrator Logout(L)

### Favorite Operation Group List

Update(R)

Default Group List:  
Group Name : Following the System Settings

Group List:

No.	Group Name
<input type="checkbox"/> 1	Green - Full Control
<input type="checkbox"/> 2	Blue - B&W Only
<input type="checkbox"/> 3	Red - No Access

Select All(S) Clear Checked(K)

## C. Create Custom LDAP Server on the MFP

1. Click on Network Settings on the left hand menu item and then click on the LDAP Settings sub menu.
2. Click on the Add button and the new Global Address Book Settings screen will appear.
3. Enter the name to use for this address book, the LDAP search root and the IP address or DNS name of the LDAP server.  
NOTE: It is important that the Search Root field has at least the domain root path entered. If this field is left blank, authentication can be done but the Linkage with User Control Function will not be applied.
4. Change Server Type from Standard to Custom so that that the default attributes fields can be edited.  
NOTE: LDAP attributes must be capitalized and spelled exactly as shown or the Linkage with User Control Function will not be applied.
5. As this address book will be used for authentication only, change the Search Attribute field from cn to sAMAccountName. This attribute returns the user's logon name rather than his first and last name from the cn attribute.  
NOTE: This is important as the user account is auto created on the MFP when the user logs on for the first time at the MFP. When printing, the user must supply his logon name (sAMAccountName) and password. If the default cn attribute is used in the custom LDAP setup, two accounts for the same user will be created. As an example, if the user's cn attribute is Don Clark and his logon name is clarkd, two users accounts will be created on the MFP – \*Don Clark and \*clarkd.
6. It is assumed that the following user attributes were available for use with the Linkage with User Control Function:
  - a. physicalDeliveryOfficeName (Displayed as Office on user's General tab in Active Directory Users and Computers )



- b. wWWWHomePage (Displayed as Web page on user's General tab in Active Directory Users and Computers)
  - c. ipPhone (Displayed as IP phone on user's Telephone tab in Active Directory Users and Computers)
7. Under the Linkage with User Control Function, type in physicalDeliveryOfficeName in the field for Authority Group, wWWWHomePage in the field for Favorite Operation Group and ipPhone in the field for Card ID.

**SHARP MX-5111N**

User Name: Administrator Logout(L)

**Global Address Book Settings**

Submit(U) Cancel(C)

Top Page

Status

Address Book

Document Operations

User Control

System Settings

Network Settings

Quick Settings

General Settings

Protocol Settings

Services Settings

Print Port Settings

**LDAP Settings**

Public Folder / NAS Setting

Proxy Setting

HTTP Access Settings

View Login User

Application Settings

Energy Save

E-mail Alert and Status

Name: Authenticate (Up to 42 characters)

Search Root: dc=sharpshow,dc=com (Up to 512 characters)

LDAP Server: 172.29.105.72

Server Type: Custom

User Identity Attribute: uid (Up to 64 characters)

Search Attribute: sAMAccountName (Up to 64 characters)

Obtain E-mail address from: mail (Up to 64 characters)

Obtain Internet Fax address from: mail (Up to 64 characters)

Obtain Fax number from: facsimileTelephoneNumber (Up to 64 characters)

Public Key Search: userCertificate (Up to 64 characters)

Linkage with User Control Function

Pages Limit Group: pagelimit (Up to 64 characters)

Authority Group: physicalDeliveryOfficeName (Up to 64 characters)

Favorite Operation Group: wWWWHomePage (Up to 64 characters)

My Folder: myfolder (Up to 64 characters)

Card ID: ipPhone (Up to 64 characters)

Custom Attribute1: (Up to 64 characters)

8. Complete the port number with the default LDAP port of 389 or the Global Catalog port of 3268, the LDAP user name and password and authentication type as needed for the network. For Server Usage, uncheck the box for Address Book and check the box for User Authentication. Press the Execute button for Connection Test. If there are no problems, click the Submit button to save the settings.

Port Number: 3268 (0-65535)

Timeout: 5 seconds (0-60)

User Name: hazeni (Up to 255 characters)

Password: (1-32 digits)

Authentication Type: NTLM

Bind Prefix: uid (Up to 64 characters)

Server Usage: ☐ Address Book ☒ User Authentication

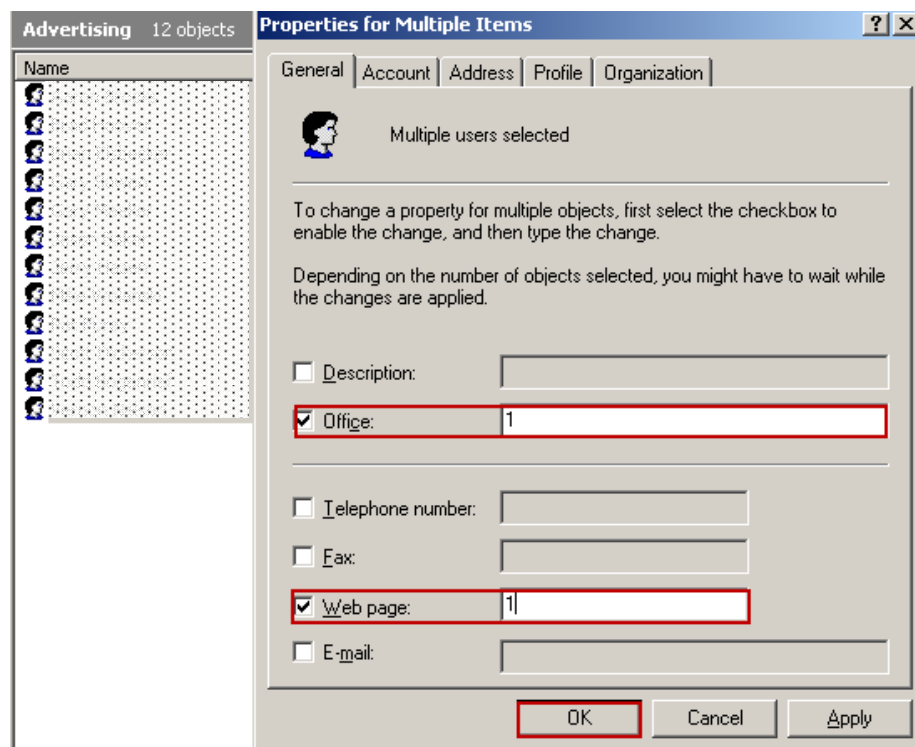
☐ Enable SSL

Connection Test: Execute(U)

#### D. Update user attributes in Active Directory

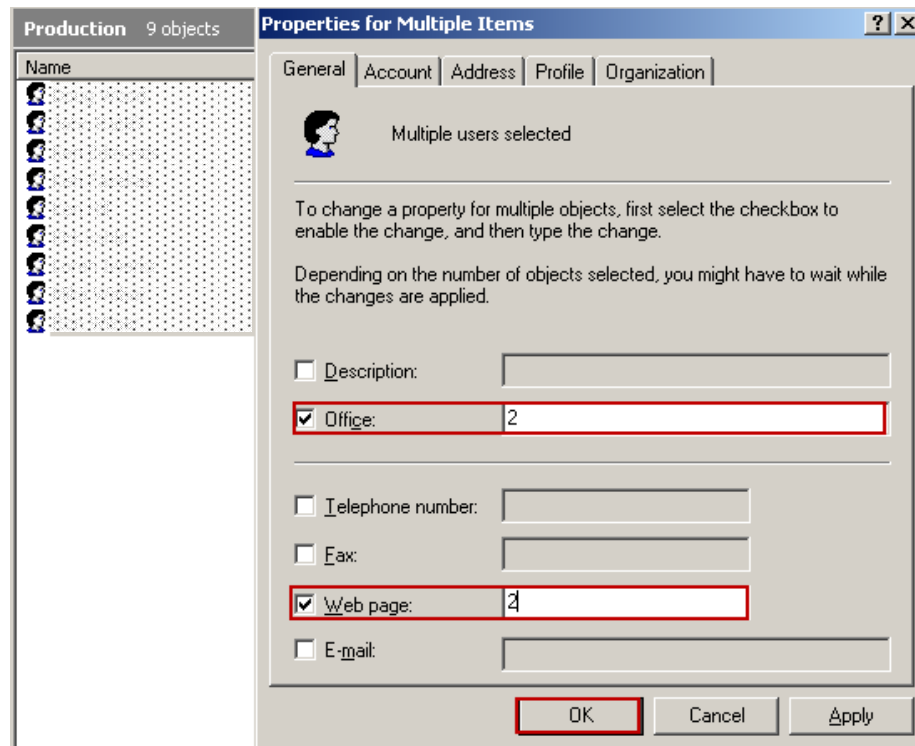
NOTE: The following steps should be performed by a qualified Network Administrator. The Active Directory structure used for this example places users in organizational units that correspond to their job functions. MFP permissions will be based on these organizational units. Users in the Advertising and Managers organizational units will have permissions to use all functions of the MFP and can print in color or black and white. Users in the Production unit can also use all functions of the MFP but can only print in black and white mode. Users in the Temporary unit will not be allowed to use any MFP function.

1. On the Domain Controller, open the Active Directory Users and Computers administrative tool.
2. Expand the Advertising ou and highlight all users. Right click, select Properties and click on General tab. Click on the check boxes next to Office and Web page. Place a 1 in the Office and Web page fields and then click on OK. All users in this unit will now belong to the Full Control authority group and the Green – Full Control favorite operations group when they log in at the MFP.



3. Repeat for the above for the users in the Managers ou as they will have the same authority and favorite operations groups assigned to them.

- Expand the Production ou and highlight all users. Right click, select Properties and click on General tab. Click on the check boxes next to Office and Web page. Place a 2 in the Office and Web page fields and then click on OK. All users in this unit will now belong to the B&W Only authority group and the Blue – B&W Only favorite operations group.



- Expand the Temporary ou and highlight all users. Right click, select Properties and click on General tab. Click on the check boxes next to Office and Web page. Place a 3 in the Office and Web page fields and then click on OK. All users in this unit will now belong to the No Access authority group and the Red - No Access favorite operations group.

- Next, users assigned with HID cards that are to be given access to the MFP must have their HID card number added to their user attributes. In the Active Directory Users and Computers tool, right click on the user name to add a card to and select Properties. Click on the Telephones tab and fill in the IP phone field with the number contained on the HID card. Click on OK when done.

The screenshot shows the 'Jerry Hazen Properties' dialog box with the 'Telephones' tab selected. The 'IP phone' field is highlighted with a red box and contains the number '24929'. The 'OK' button at the bottom is also highlighted with a red box.

Member Of	Dial-in	Environment	Sessions	Remote control	
Terminal Services Profile		COM+	Exchange General		
E-mail Addresses		Exchange Features	Exchange Advanced		
General	Address	Account	Profile	Telephones	Organization

Telephone numbers

Home:  Other...

Pager:  Other...

Mobile:  Other...

Fax:  Other...

IP phone:  Other...

Notes:

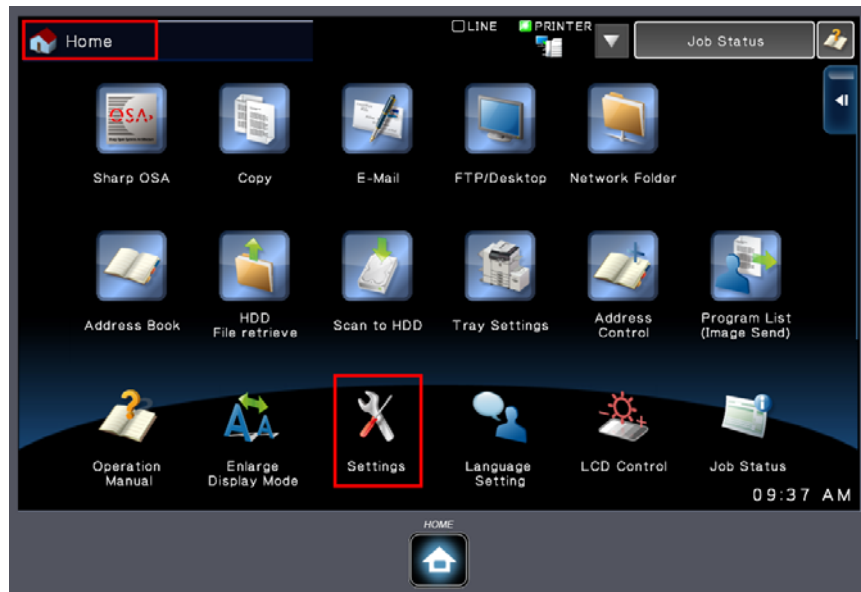
OK Cancel Apply Help

- Repeat for each user who will have access to the MFP keeping in mind that a card can only be registered to a single user.

E. Install the Card Reader to the MFP and enable User Control.

All that remains to implement this solution is to install the HID card reader on the MFP and set the authentication method to HID card only. The following

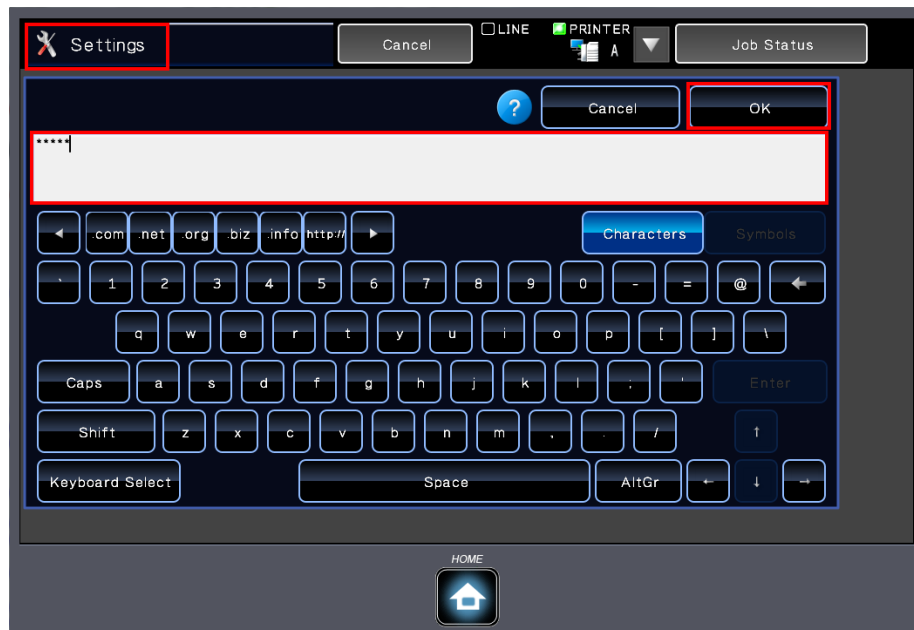
1. At the MFP, press the Settings button on the Home screen of the display.



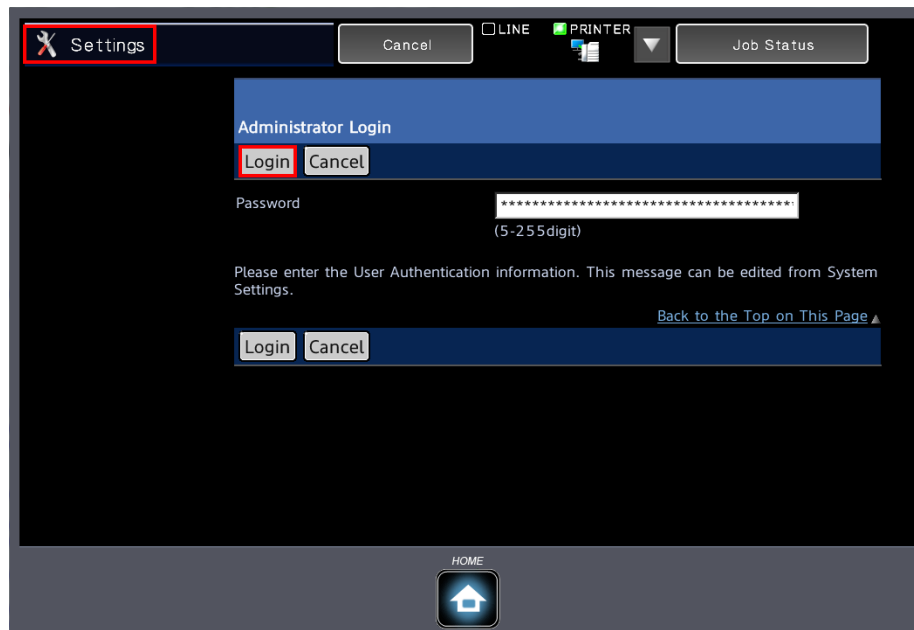
2. At the Settings screen, press the Administrative Login button.



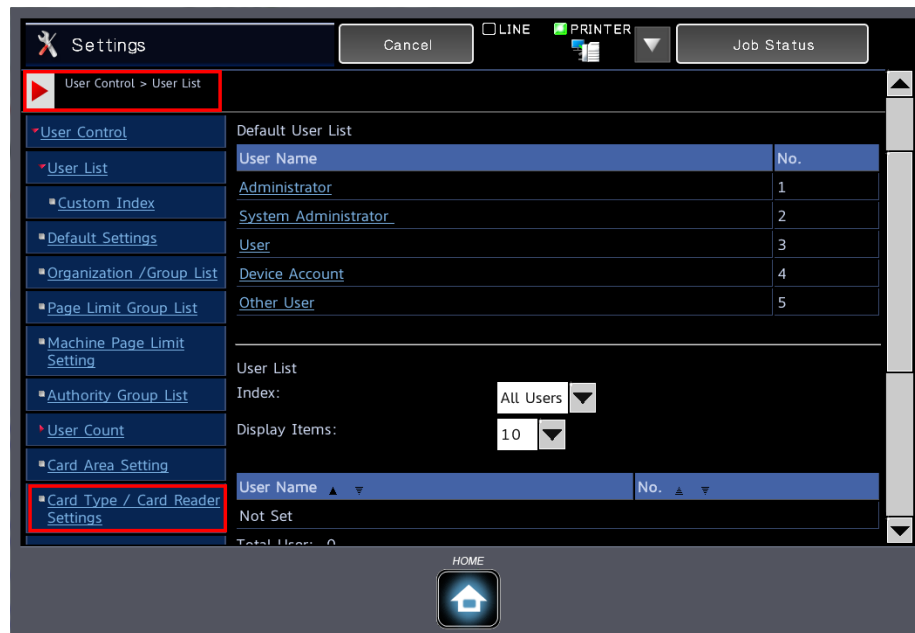
- When the following screen appears, type in the administrator password (default admin) and then press the OK button.



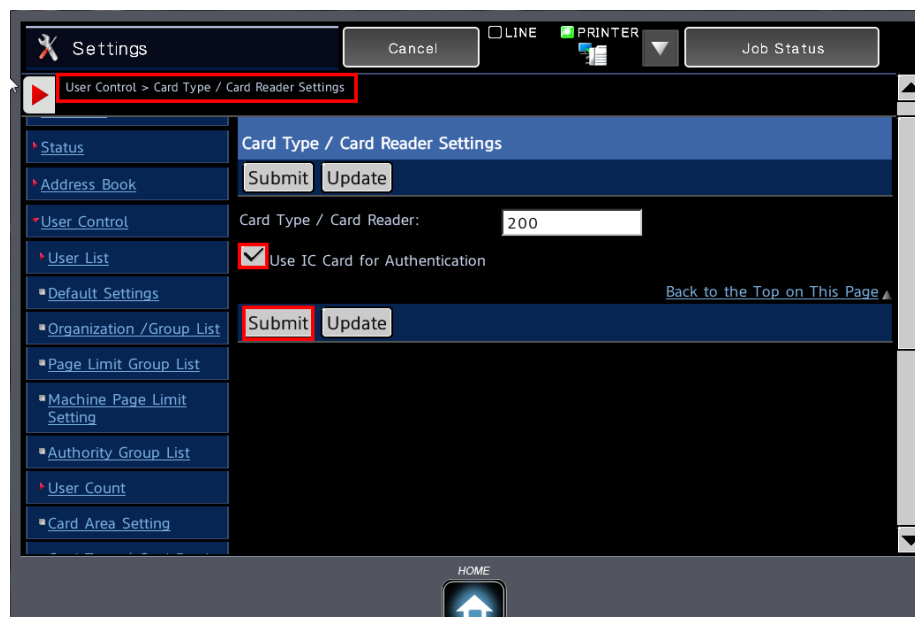
- Press the Login button.



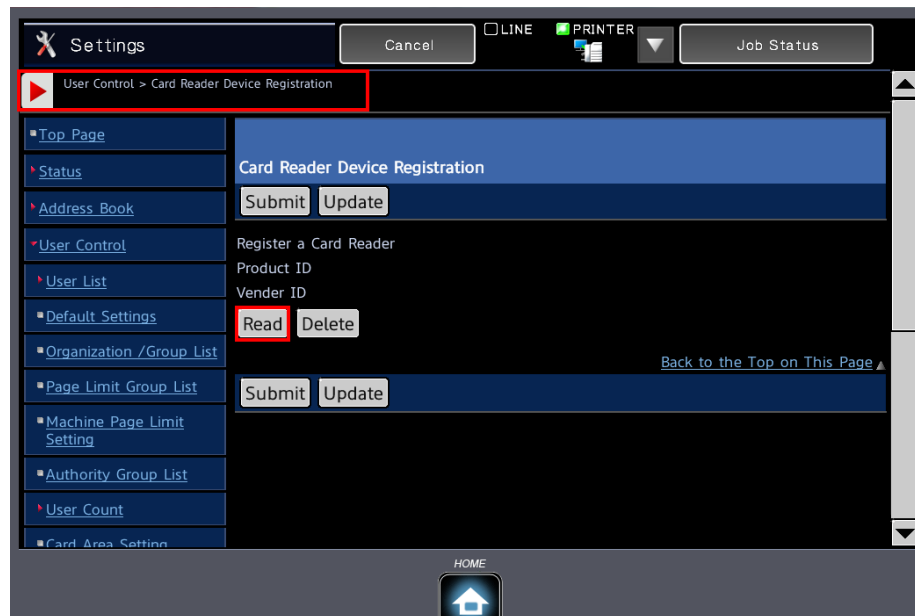
5. When the Settings screen reappears, click on the User Control menu to expand it and then click on Card Type / Card Reader Settings.



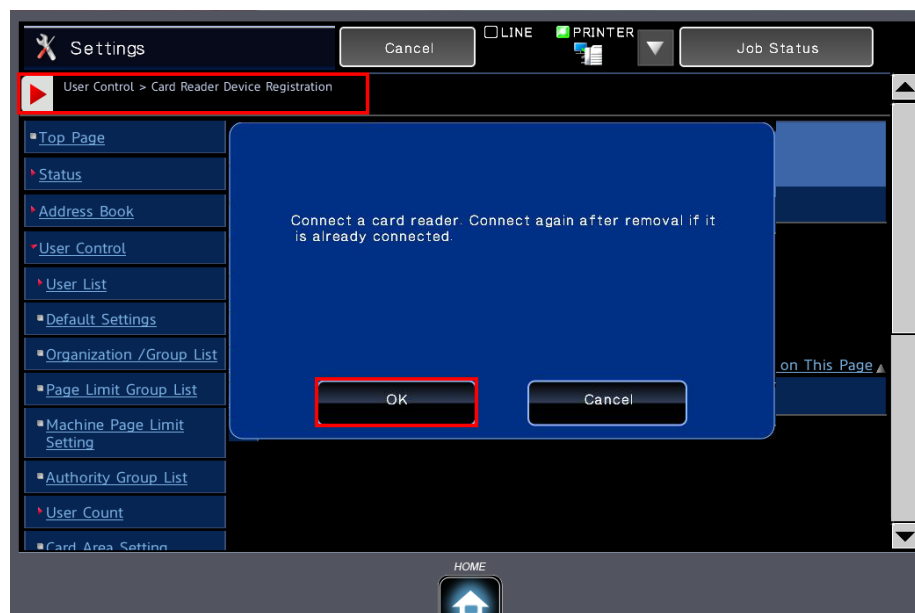
6. Click on the checkbox for Use IC Card for Authentication and then press the Submit button.



7. Scroll down under User Control, select the Card Reader Device Registration menu item and then click on the Read button.



8. When the following message appears, insert the USB cable from the HID card reader into the USB connector of the MFP and then press the OK button.





9. After a few moments, the Product ID and Vendor ID fields will be populated with the values from the card reader. Click on the Submit button after this occurs.

The screenshot shows the 'Settings' application window. The 'User Control > Card Reader Device Registration' path is highlighted in the left sidebar. The main content area is titled 'Card Reader Device Registration' and includes a 'Logout' button. Below the title, there are 'Submit' and 'Update' buttons. The 'Submit' button is highlighted with a red box. The main content area displays the following information:

Register a Card Reader	
Product ID	15354
Vendor ID	3111

Below the table, there are 'Read' and 'Delete' buttons. At the bottom of the main content area, there are 'Submit' and 'Update' buttons. A 'Back to the Top on This Page' link is also present. The bottom of the window features a 'HOME' button with a house icon.

10. Under User Control select Default Settings menu item.

The screenshot shows the 'Settings' application window. The 'User Control > User List' path is highlighted in the left sidebar. The main content area is titled 'Default User List' and includes a 'Logout' button. Below the title, there is a table with the following data:

User Name	No.
Administrator	1
System Administrator	2
User	3
Device Account	4
Other User	5

Below the table, there are 'User List' and 'Index' buttons. The 'Index' button is highlighted with a red box. The main content area displays the following information:

User Name	No.
Not Set	

At the bottom of the main content area, there are 'User List' and 'Index' buttons. The 'Index' button is highlighted with a red box. The bottom of the window features a 'HOME' button with a house icon.

11. Select Enable from the drop down list for User Authentication and leave the Authentication Method Setting at the default as shown.

Settings

Cancel LINE PRINTER Job Status

User Control > Default Settings

Default Settings

Submit Update

User Authentication: Enable

Authentication Method Setting:

- ☒ Authenticate a User by Login Name and Password
- ☐ Authenticate a User by Login Name, Password and E-mail Address
- ☐ Authenticate a User by User Number Only

Device Account Mode Setting:

- ☐ Device Account Mode
- ☐ Allow Login by Different User

Login User: Not Set User Selection

Actions when the Limit of Pages for

HOME

12. Scroll down and select the LDAP server created for use as the authentication server from the drop down list. Check the box next to Perform LDAP server access control and any other desired options on this screen.

Settings

Cancel LINE PRINTER Job Status

User Control > Default Settings

Card Reader Device Registration

System Settings

Network Settings

Application Settings

Energy Save

E-mail Alert and Status

Job Log

Security Settings

Job is Stopped when the Limit of Pages is Reached

After reaching to the page limit, cancel the job and delete the job during receiving

☐ A Warning when Login Fails

☒ Disabling of Printing by Invalid User

☐ Automatically print stored jobs after login: Login Name

Default Network Authentication Server Setting: Authenticate

☒ Perform LDAP server access control.

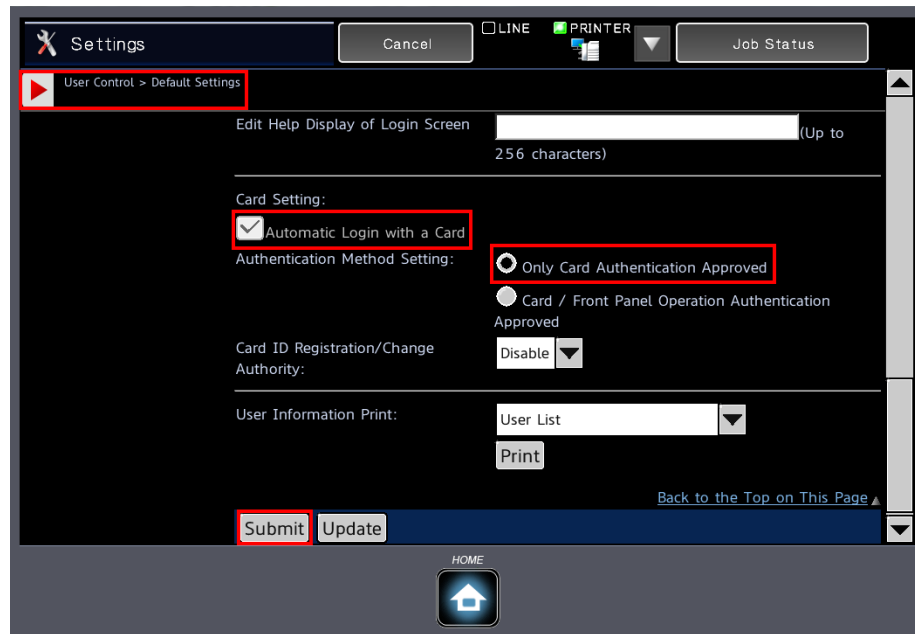
☒ Display Usage Status after Login

Login Name Display: Display login name

☐ Include Job Status in user authentication

HOME

13. Scroll down to the last screen, click on the box next to Automatic Login with a Card and click on the radio button for Only Card Authentication Approved. Click on the Submit button when done.



14. The Home screen will then be displayed as shown below and only users with their HID cards registered in Active Directory or the MFP administrator can log into the MFP. Their permissions to use the MFP functions will be restricted by the Authority Group that was assigned to them in Active Directory as shown on Pages 2 and 3 of this document.

