SET UP AND OPERATION GUIDE

Version 5.1

Novermber 2016

KYOCERA

Contents

Trademarks **4**

Introduction **4**

Access Lock **5**

Features summary *5*

What's New in Version 5.1 ..... *5*

Supported models *6*

Authentication 6

Network Authentication *6*

Public Access button *7*

MFP-Local authentication *7*

Using Access Lock with Coin Vending Machine *8*

Authorization 8

Access Control policy *8*

Permissions *8*

Accounting 9

Installation and Setup 10

Setup Outline *10*

Step 1. MFP Application Installation *11*

Step 2. Prepare Network Settings *12*

Step 3. Install settings on MFP *20*

Step 4. Setup Print Authorization *22*

Step 5. Configuring Card Authentication *24*

Appendix **25**

Setting up Cryptek Netgard for CAC/PIV authentication 25

Network Configuration *25*

Netgard Setup and Configuration *26*

Configuring Netgard for Access Lock *27*

Setting up Proximity Card Reader (USB connected) 30

Setting up Proximity card reader (Network connected) 31

Terms used in this document

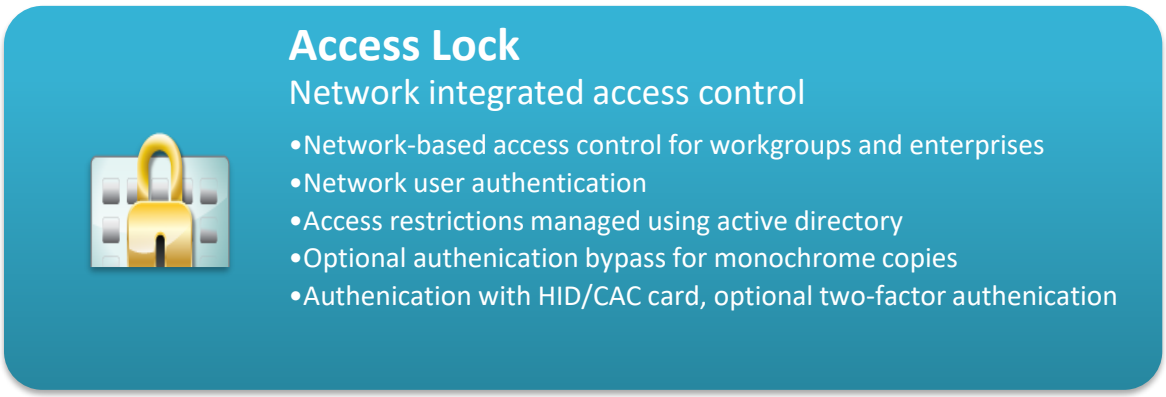
Term	Explanation
MFP	Kyocera Multi-Function Printers
HyPAS	Hybrid Platform for Advanced Solutions: software technology included in many Kyocera MFPs.
KX Driver	Kyocera extended driver for advanced printing functions

Trademarks

- Microsoft, MS-DOS and Windows are registered trademarks of Microsoft Corporation of either the United States or other countries.
- Windows XP is a trademark of Microsoft Corporation.
- Microsoft Windows Vista, Microsoft Windows 7, SharePoint and Microsoft Internet Explorer are trademarks of the Microsoft Corporation in the U.S. and other countries.
- Adobe Acrobat and Adobe Reader are trademarks of Adobe Systems, Incorporated.
- Other company names and product names in this Operation Guide may be the trademarks or registered trademarks of their respective owners. TM and ® are not mentioned in each case in this guide.

Introduction

Access Lock is a software suite used for regulating access to Kyocera MFPs for improved security and reduced wastage. This user guide covers functionality offered by the software and the tasks required to deploy the solution.



Access Lock

Access Lock provides a comprehensive authentication and authorization solution for HyPAS-enabled Kyocera MFPs. Several LDAP-based authentication options are provided. Access to MFP functions can be regulated by assigning permissions to user groups.

Features summary

- Authentication options
  - Username and password
  - Proximity card swipe
  - Proximity card swipe + numeric PIN (Two-factor)
  - CAC / PIV card support with Cryptek Netgard device
  - Anonymous authentication for limited access
  - Local MFP authentication
  - Multiple LDAP servers (domains) supported (up to 5)
  - Payment to Coin Vending Machine
- Authorization
  - MFP functions can be locked or allowed based on user's LDAP group membership
- Remote Configuration
  - Create and maintain settings using utility
  - Upload settings to multiple MFPs using utility
- Software Compatibility
  - LDAP V3 is used to communicate with directory servers such as Microsoft Active Directory.
  - SSL/TLS support is available to encrypt communication between MFP and directory server. Note: SSL/TLS must be enabled on the directory server for this feature to work properly.

What's New in Version 5.1

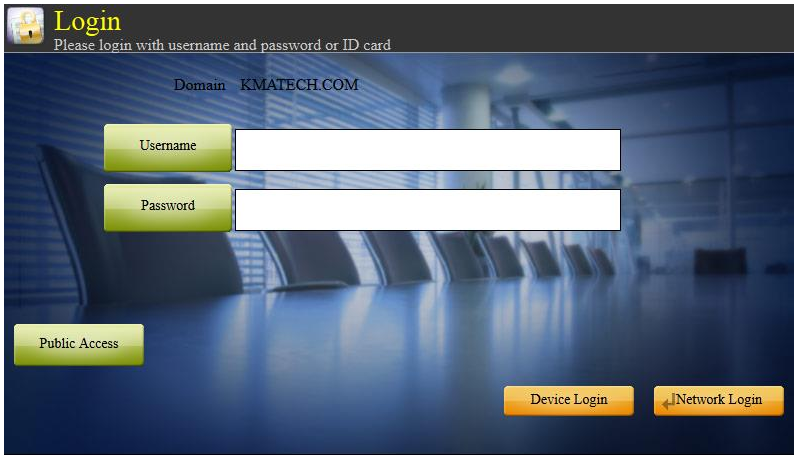
- LDAP Server Host name and IP Address fields are now separate.
- Ability to search through a list of user names for the ID Card Authentication Query Account Name instead of having to manual enter the fully distinguished name of a user account.

Supported models

For a full and updated list of supported MFP models, please refer to the AccessLock product page on KDAConnect.com.

Authentication

The purpose of authentication is to establish user's identity. At the login screen on the MFP, the user has several methods for authentication. Each of these can be enabled or disabled by the Administrator. This section describes the end-user experience with each authentication mechanism.



Network Authentication

Logging in with Username and Password

1. Press the Username button. Enter username using software keypad that appears
2. Press the Password button. Enter password using software keypad that appears.
   Note: Password will appear as * characters
3. Press the Network Login button (or press the Return button on the keypad)

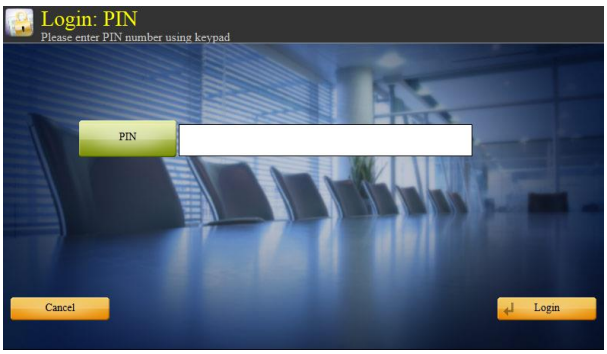
Selecting domain

1. If multiple domains are available for authentication, the login screen will display a domain selection dropdown.
2. User can change the domain before authenticating with the methods listed in this section.

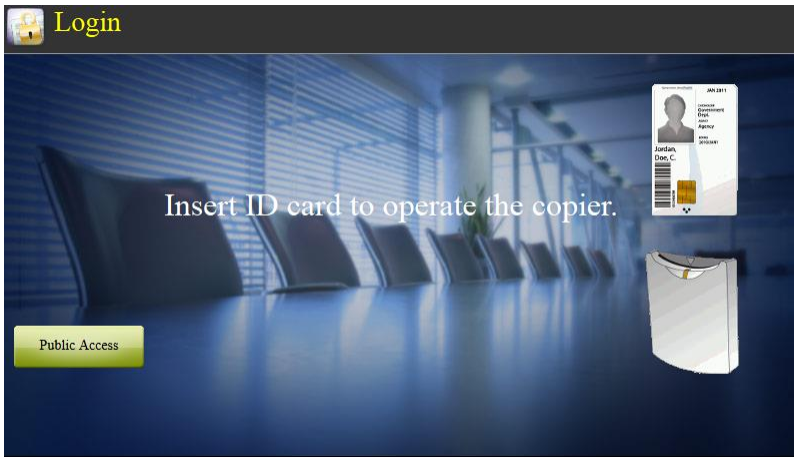
Logging in with Proximity card

1. Simply swipe ID card at the card reader to authenticate.

2. If the MFP is configured for Two-factor authentication, the MFP will prompt for a PIN number. PIN number can be entered using the numeric keys on the MFP keypad.



Logging in with CAC/PIV card using Cryptek Netgard



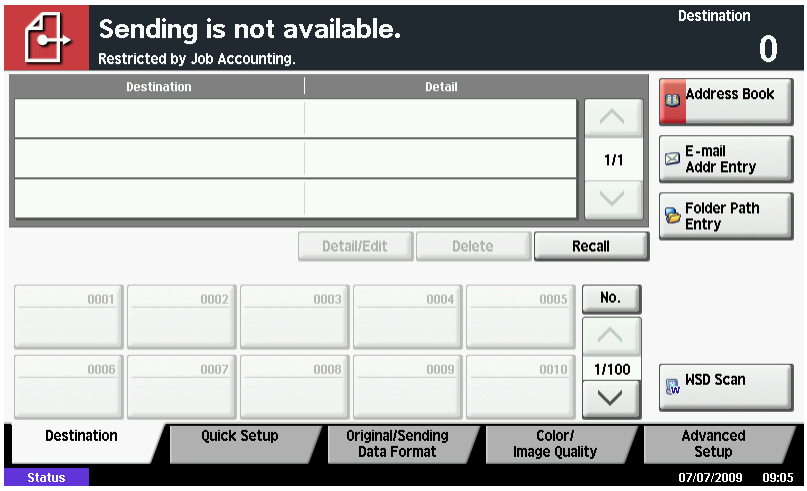
1. If the system is configured to with Cryptek Netgard, the operation panel will display an animation of the CAC card being inserted into the reader as shown to the right.
2. When CAC / PIV card is inserted into the reader, the panel will prompt for a PIN number. When the correct PIN is entered, the MFP is unlocked.

NOTE: Only a limited number of retries will be allowed before the card is locked out.

Public Access button

1. 'Public Access' button will be displayed only if configured by the Administrator.
2. Pressing the Public Access button allows the user to access certain functions of the MFP that are allowed for public use. For example, all users could be allowed to make monochrome copies without authentication.

3. If the user tries to access a function that is not allowed under Public Access, the MFP will display a message stating the function is not available as shown below.



MFP-Local authentication

Users can also login to access MFP functions using credentials programmed into the MFP. This is especially useful to perform administrative operation on the MFP using the panel. This type of authentication does not require LDAP server.

Note: Default username and password are Admin, Admin.

Using Access Lock with Coin Vending Machine

Access Lock can be used together with a Coin Vendor machine such as a JAMEX vending system.

When user inserts coins (or payment card) into the payment device, MFP will be unlocked to allow user to make copies. User will be logged in to the MFP till coins are exhausted (or payment card is removed).

Authorization

After user's identity is established through authentication, the system would allow or deny access to MFP functions. Access control policies are defined by the Network Administrator. This section describes how policies are defined and how the software works to determine functions that are allowed or denied.

Access Control policy

The following table lists where permissions are defined for each authentication method.

Login method	Access control policy
Network login	Permissions are assigned to LDAP user groups. Effective permissions are determined based on groups the user belongs to.
Public Access	Permissions set by administrator, applies to anyone using 'Public Access' button.
MFP-local	Permissions set on the MFP for the local user account.

Permissions

Following functions of the MFP can be individually restricted in access control policies.

Permission	Description
Copy	Access to copier function This includes Monochrome, Color, Auto-color and single color.
Copy color	Permission to make color copies
Send	Permission to scan documents
Print	Allow or deny printing from document box. To control printing from PC, refer to section on PC printing authorization.
Print color	Permission to print documents in color
Fax	Permission to use MFP's fax capability
Administrative access	Level of access: Administrator or User

Accounting

When used together with PaperTrail, Kyocera's job tracking software, Access Lock can report users' activity on the MFP to a central database for accounting and auditing purposes. This allows generation of detailed usage reports to:

- Study how the equipment is being utilized
- Minimize wastage by restricting color
- Maximize utilization by relocating devices

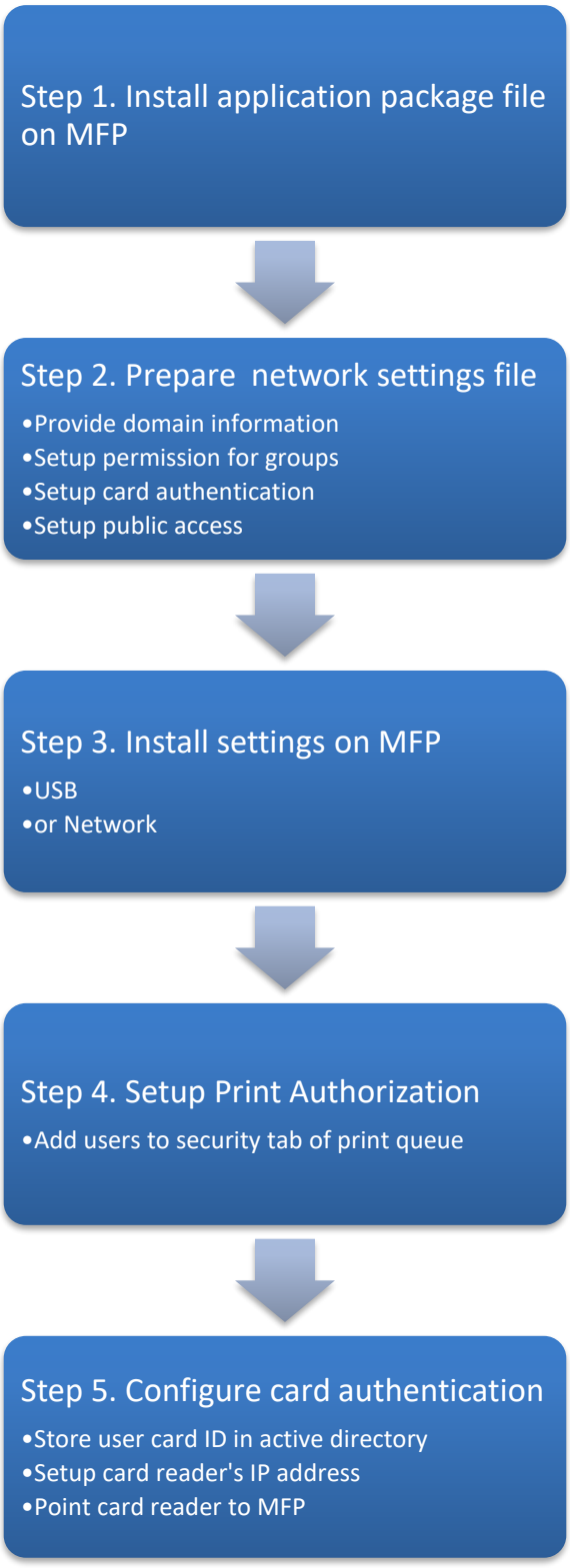
Detailed information about each job (print, copy, scan and fax) is collected and transmitted to the server in encrypted TCP messages. If the server is temporarily not available, the data is cached locally and then transmitted to the server at the next connection opportunity.

Job information includes:

- Job owner (login account including domain)
- Document name
- Scan and fax destinations
- Page details: color/monochrome, size, media type, output tray, duplex

Installation and Setup

Setup Outline



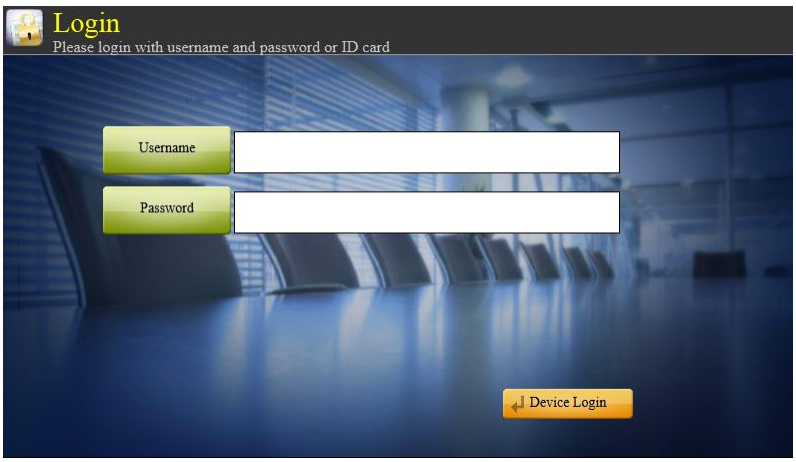
Step 1. MFP Application Installation

Required File

- AccessLock4.pkg

Installing Access Lock

1. Copy *AccessLock4.pkg* from *C:\Program Files\Kyocera\Access Lock* to the root folder of an empty USB flash drive. Do not copy both .pkg files to the flash drive. Copy only one depending on the MFP model.
2. Open *System Menu* and scroll to next page and press *Application* button. If prompted to authenticate, login with an administrator account. The application screen will list all applications currently installed on the MFP.
3. Press *Add* button to open *Application-Add* screen. Then insert the USB flash drive into USB slot at the side of the panel. Within a few seconds, the MFP will display *AccessLock* in the list of applications found on the USB flash drive.
4. Select *AccessLock* and press the *Install* button. When prompted to confirm, press *Yes*. The MFP will confirm that the application installed correctly. Then, press the *Remove Memory* button. After the MFP confirms that it is safe to remove the USB memory device, remove it from the MFP.
5. Press the *Close* button to exit back to *Application* page.
6. Select *AccessLock* and press *License On* button. When prompted to confirm licensing, press the *Yes* button.
7. Press the *Close* button to exit back to the *System Menu* screen. Wait for approximately one minute for the security application to take effect.
8. Immediately after installation, the authentication screen would allow only local (device) authentication as shown below. Default administrator username and password is 'Admin', 'Admin'.



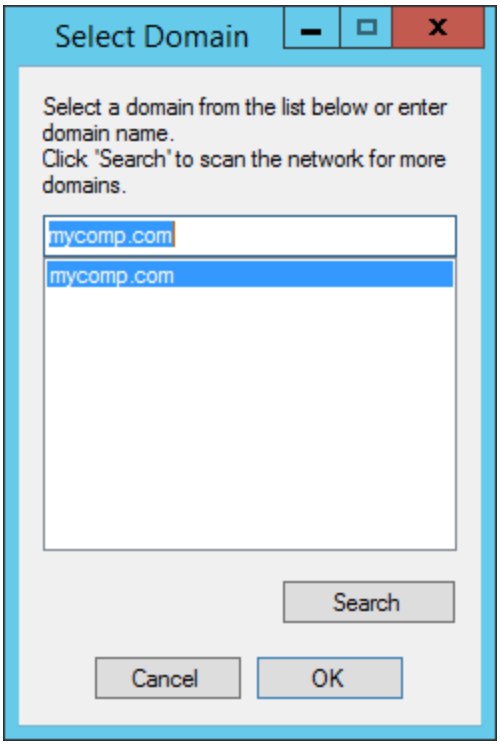
Step 2. Prepare Network Settings

Installing Configuration Utility

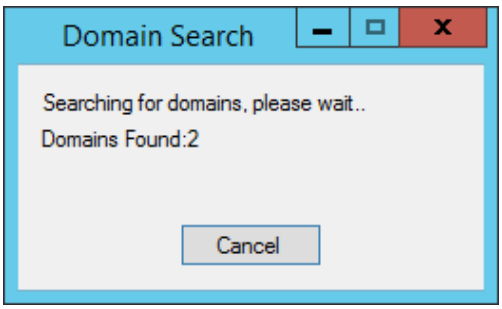
- Execute *Access Lock setup.exe* to begin installation. Follow the installation wizard screens to complete installation.
- The default installation location is *C:\Program Files\Kyocera\Access Lock*, which can be changed if required.
- The installer may download and install *Microsoft .NET 2.0 Framework*, as it is a pre-requisite.

Setting up Authentication

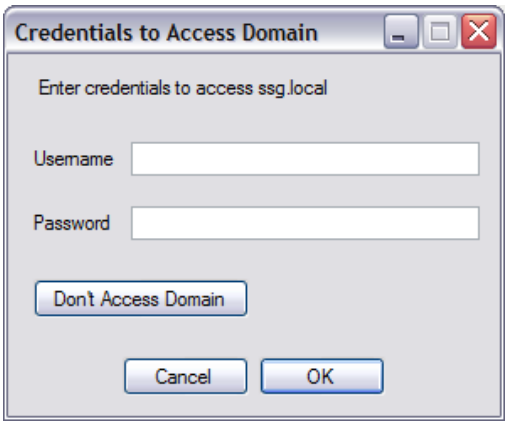
- Launch *Access Lock Settings application* by clicking on *Start > All Programs > Kyocera > Access Lock > Settings*
- Click *File > New* to create a new configuration
- Click *Edit > New Domain* to add a domain to the configuration
    - Either select a domain from the list or enter domain name manually



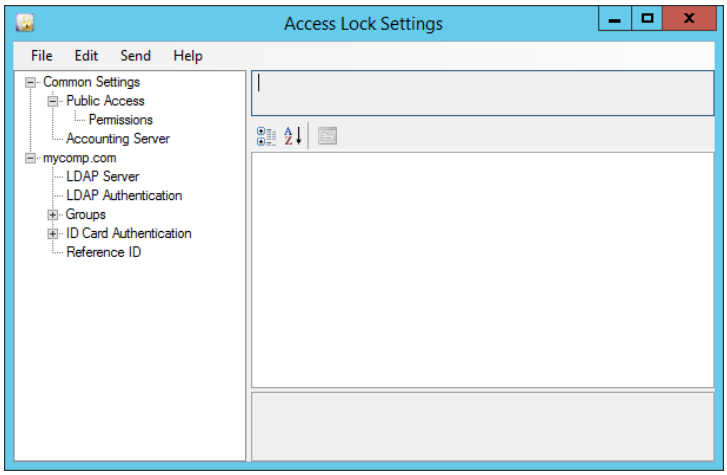
    - Click Search button to find domains using WMI. Searching with WMI may take a few minutes to complete.



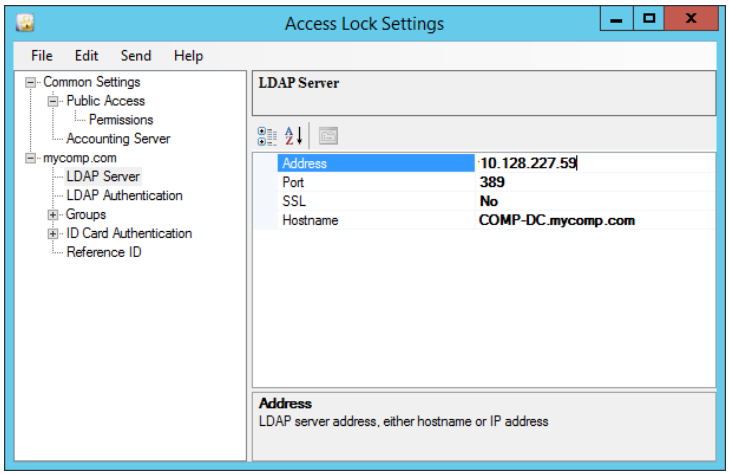
- Some domains may require user credentials to access member objects. In such case, the software may prompt for user login. If authentication information is not available (ex., when setting up off-line) or not required (ex., simple CAC authentication), click the 'Don't Access Domain' button



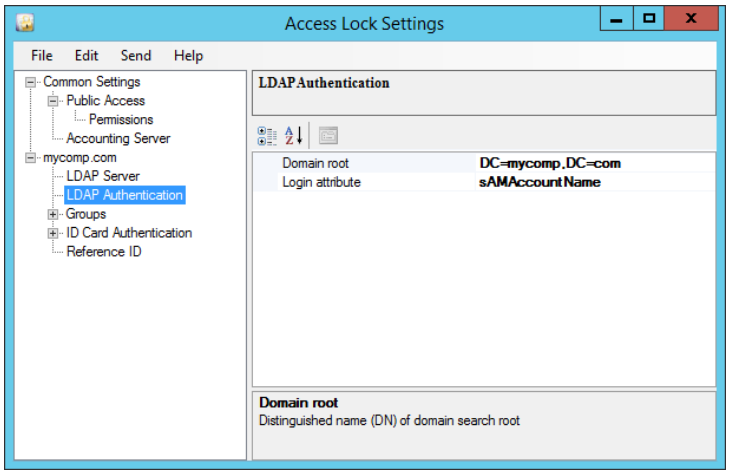
- The configuration tree should now look like:



- LDAP Server
  - **Address:** IP Address of domain controller
  - **Port:** Default value for Active Directory is 389
  - **SSL:** Enable if LDAP server is configured to allow SSL/TLS communication
  - **Hostname:** Host Name of domain controller

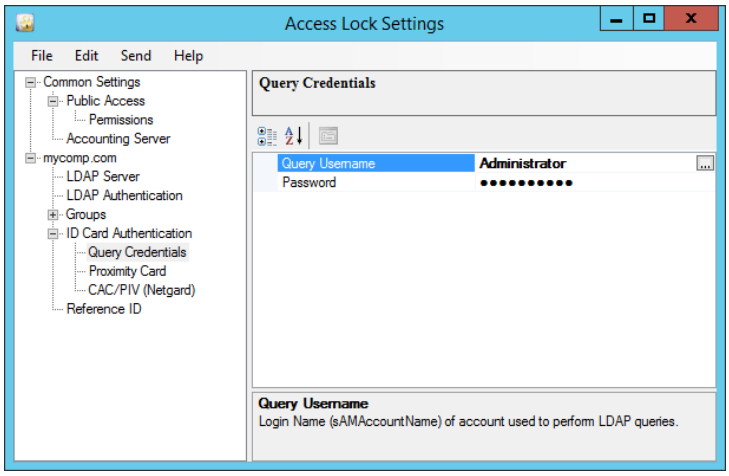


- LDAP Authentication
  - **Domain root:** Starting point for user search. Typically, it would be: CN=Users,DC=<domain>,DC=<com>
  - **Login attribute:** Typically, login name is stored in *sAMAccountName* attribute



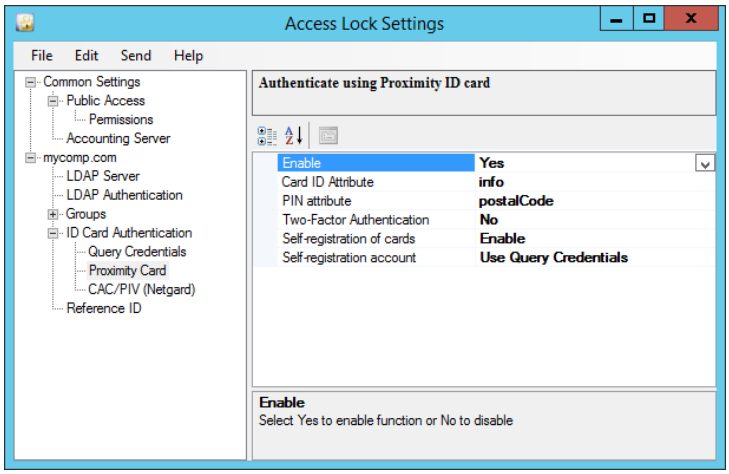
- ID Card Authentication
  - Two types of ID cards are supported
    - Proximity Cards using RFIdeas USB card readers. Several card types are supported, please refer to RFIdeas web site.
    - CAC/PIV Cards using Cryptek Netgard device.
  - Query Credentials are required when using either ID card system. Query credentials are used only to lookup user information from Active Directory.

- Query Credentials
  - **Query Username:** Enter the name of a user account that will be used for running queries on Active Directory. You can also press the ellipsis button (…) to view a list of available users
  - **Password:** Password to the query user account



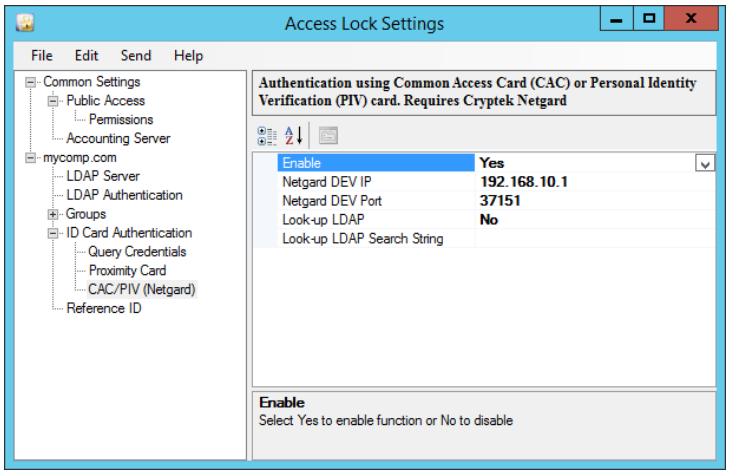
Note: Query credentials are stored in a secure, encrypted form in the configuration file.
Note: On Microsoft Exchange Server, this user account must be added to the 'Pre-Windows 2000 Compatible Access' group. Membership to this group allows executing queries on Exchange Server. Steps for this can be found at: http://support.microsoft.com/kb/325363.

- Proximity Card Authentication
  - **Enable:** Turn ON/OFF proximity card authentication
  - **Card ID Attribute:** LDAP attribute where Card ID is stored
  - **PIN Attribute:** LDAP attribute where PIN number is stored
  - **Two-Factor:** If selected, user must enter a PIN number after swiping ID card.



  - **Self-registration of cards:** Enable/Disable end-users from registering their cards at the MFP panel after authentication
  - **Self-registration account:** Indicate the account to be used for registering card in Active Directory. If "Use Logged-in User Credentials" is selected, Access Lock would use the end-user's credentials to register the card. If "Use Query Credentials" is selected, the credentials provided under the 'Query Credentials' field are used for all users. If the account has insufficient rights to update Active Directory, registration would fail.

- CAC/PIV Card Authentication (Cryptek Netgard)
  - **Enable:** Turn ON/OFF CAC/PIV card authentication
  - **Netgard DEV IP:** IP address assigned to the DEV port on Netgard. Default value is 192.168.10.1.
  - **Netgard DEV Port:** Port number used to communicate with Netgard. Default value is 37151.

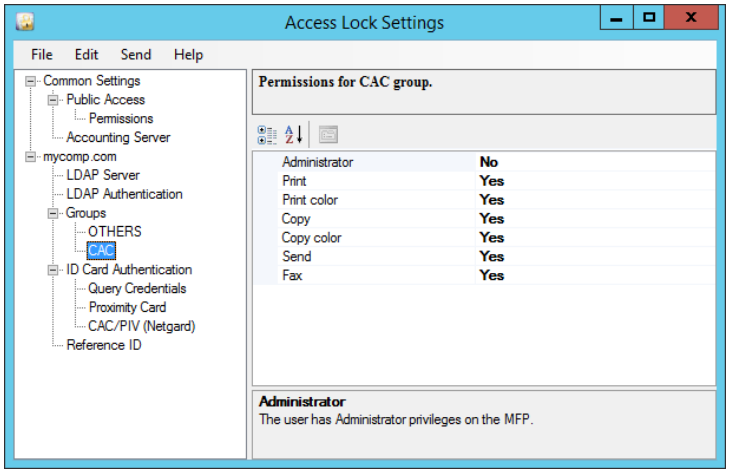


  - **Look-up LDAP:** Enable this feature to retrieve user information from Active Directory. For this feature to work correctly, LDAP authentication on Netgard must be enabled and configured correctly as described in the Appendix: Setting up Cryptek Netgard: Setting up LDAP authentication.

When Look-up is enabled, Access Lock will:

a) Query LDAP for the user's group membership;
b) Deny login if the user account does not exist;
c) Assign permissions based on membership. In addition, email address will be obtained from LDAP.

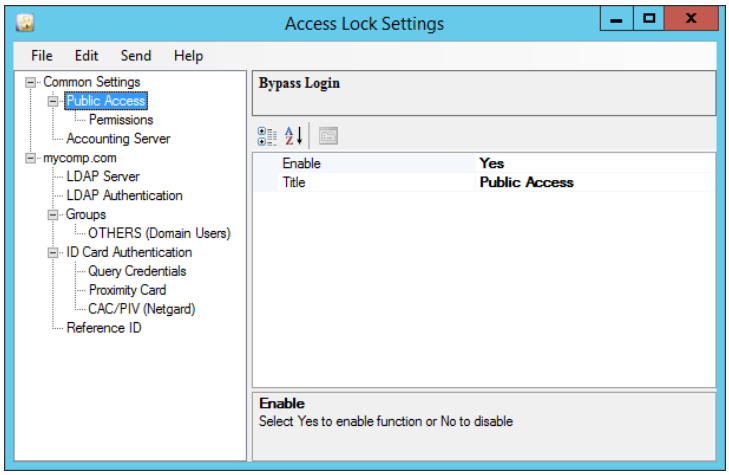
When look-up is disabled, the user will be assigned permissions programmed in 'CAC' group. CAC group is a special group in Access Lock settings that is not part of Active Directory or LDAP.



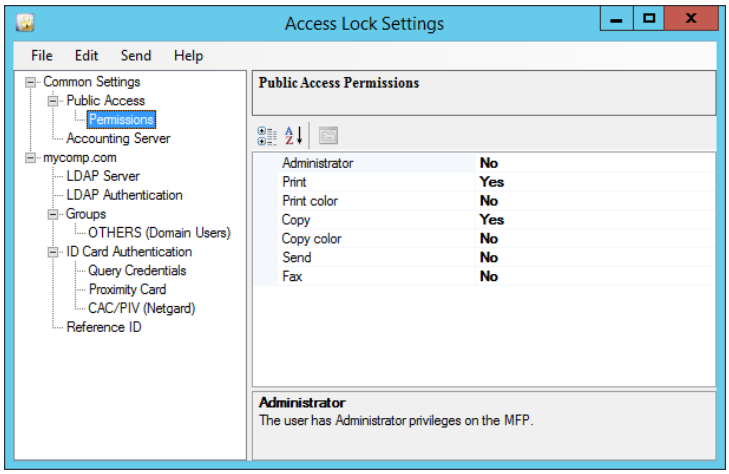
Setting up Anonymous Access

Enabling *Public Access* displays a button on the login screen that would allow users to access device functions without authenticating with username and password. Permissions for such login can be configured under *Common Settings > Public Access*.

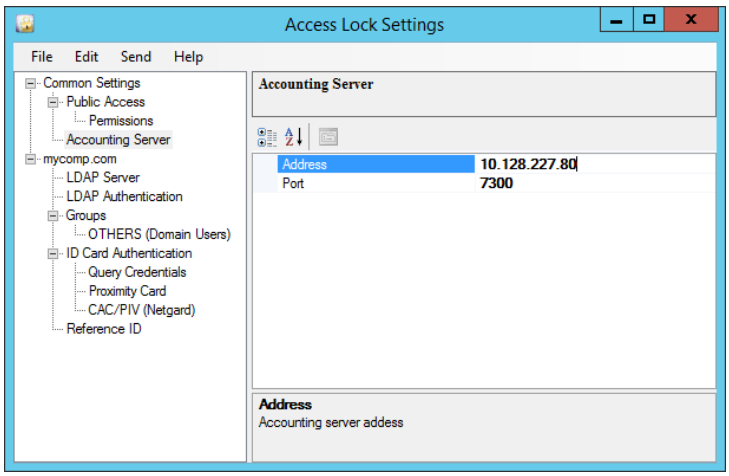
- Common Settings > Public Access
  - **Enable:** Show *Public Access* button and allow anonymous authentication
  - **Title:** Label that should appear on the button



  - **Permissions:** Privileges applied when user gains access via this button



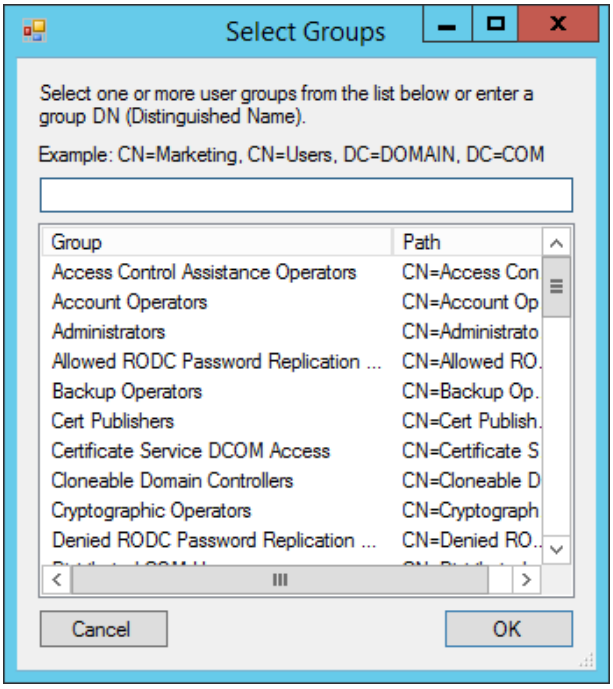
- Common Settings > Accounting Server
  - **Address:** IP address or Host-name of accounting server
  - **Port:** Port number used to transmit usage data (Default: 7300).



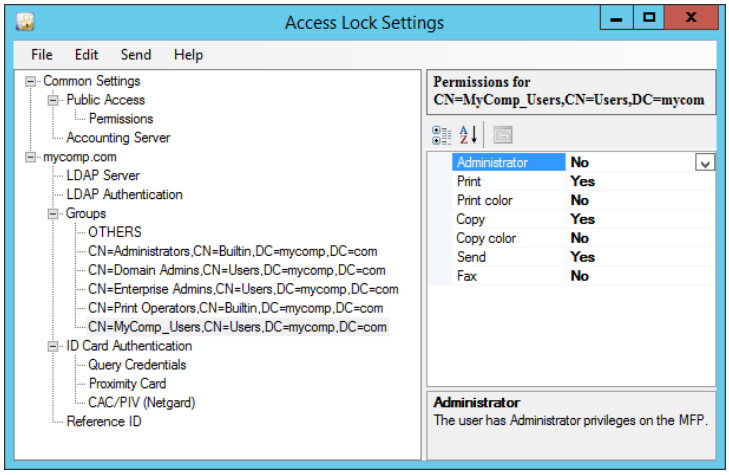
Setting up Group Permissions

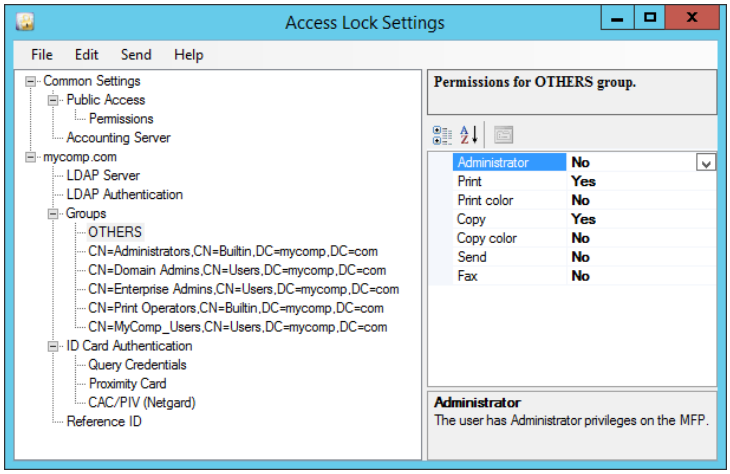
- Click *Edit* > *New Group* from the menu (or *Group* > *New* from the context menu).

- The select groups dialog appears, showing all user groups in the domain. Administrator can either select one or more groups from the list or key-in a group DN manually.



- Each group appears in the tree view as a node. Select one or more nodes to view and edit permissions. Example to the right shows color output and fax restricted.



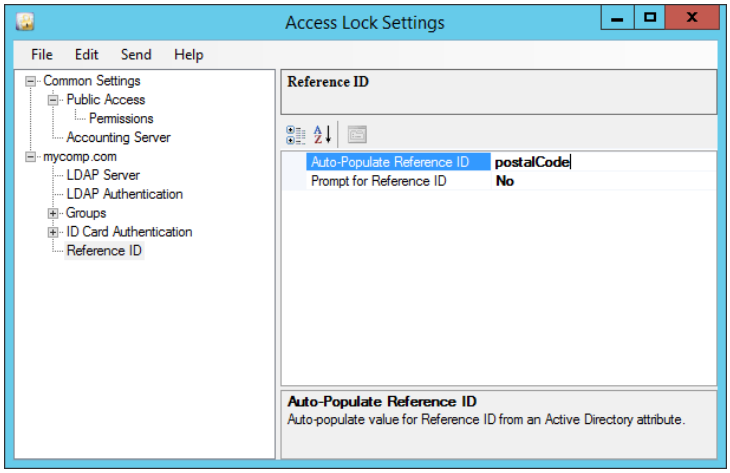


- OTHERS group serves as a 'catch-all' group. It cannot be renamed or deleted. If a user logs in and does not belong to any of the configured groups, he is assigned permissions from the OTHERS group.

- Permissions:
  - **Print:** User can print
  - **Print Color:** If print and print color is enabled, user can print color pages
  - **Copy:** User can make copies
  - **Copy Color:** If copy and copy color is enabled, user can make color copies
  - **Send:** User can scan and send images to destinations
  - **Fax:** User can send faxes
  - **Administrator:** User get administrator privileges on the MFP

Setting up Reference ID Lookup

Access Lock can be setup to automatically lookup Active Directory and retrieve a value for Reference ID. This value is then used to track activities performed at the copier.



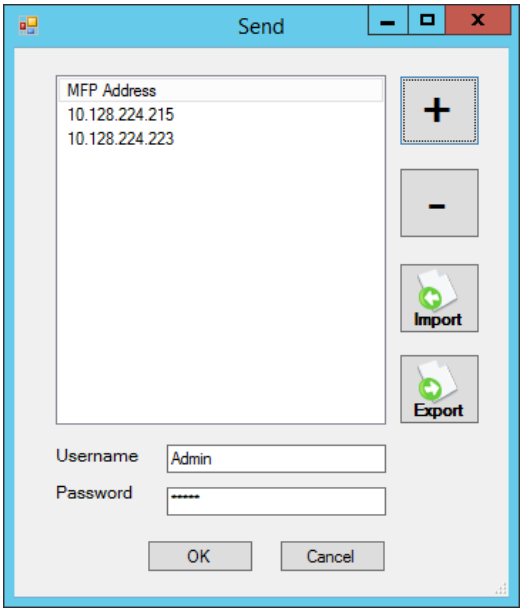
- **Reference ID > Prompt Reference ID:** Select Yes to display a text box prompting for a Reference ID value at the login screen.
- **Reference ID > Auto-Populate Reference ID:** Enter the name of an LDAP attribute name that contains the Reference ID value.

Step 3. Install settings on MFP

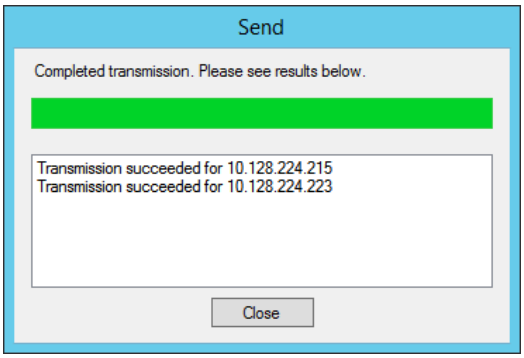
Installing settings over the network

Settings can be transmitted to multiple MFPs using the Send dialog, launched from Send menu item.

- Click *Send > Send to Device*. In the Send dialog that appears, enter or import MFP address list.
- The MFP address list can be exported and saved in a text file for quick broadcast to a MFP fleet



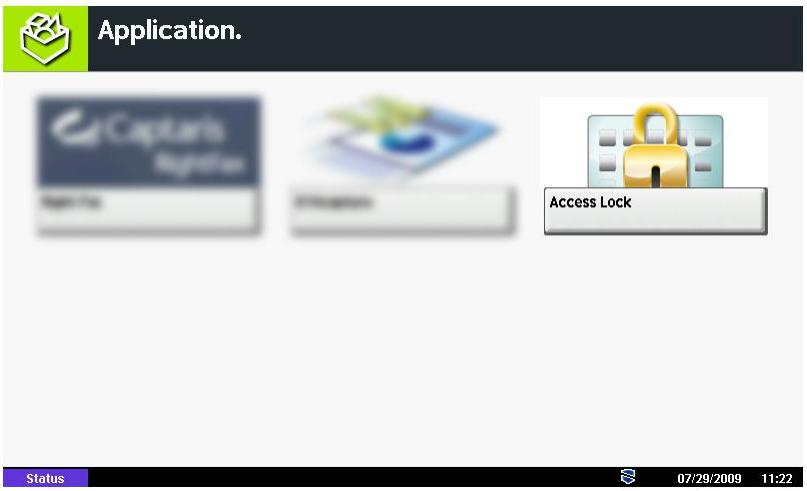
- Click OK button to begin transmission of the settings. A progress dialog will report result of transmission.
- After successful transmission, the new settings would take immediate effect.



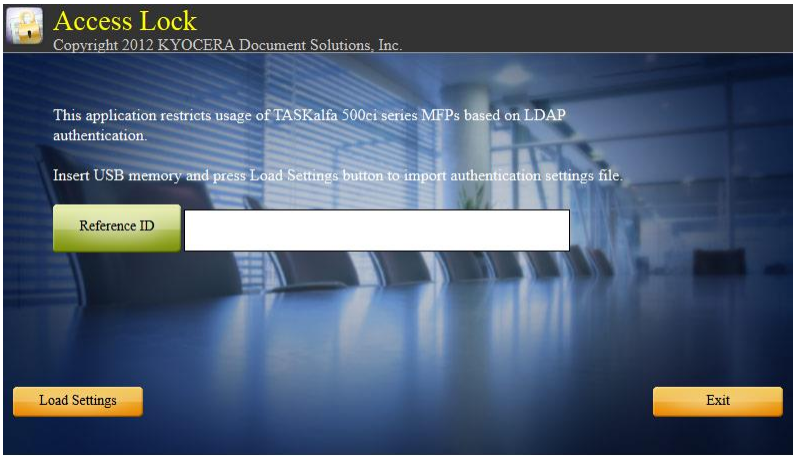
Note: MFP must have Access Lock application installed prior to configuration. Username and Password must be entered and must match local user account on MFP with administrator privileges.

Installing settings with USB flash drive

1. Save the settings to an XML file using the *File* > *Save As* menu item.
2. Copy the settings XML file to the root of a USB flash drive.
3. Login to the MFP with administrative access (default: Admin, Admin – note the capital A)
4. Switch to Application screen by pressing the *Application* button on the panel. Press *Access Lock* application button

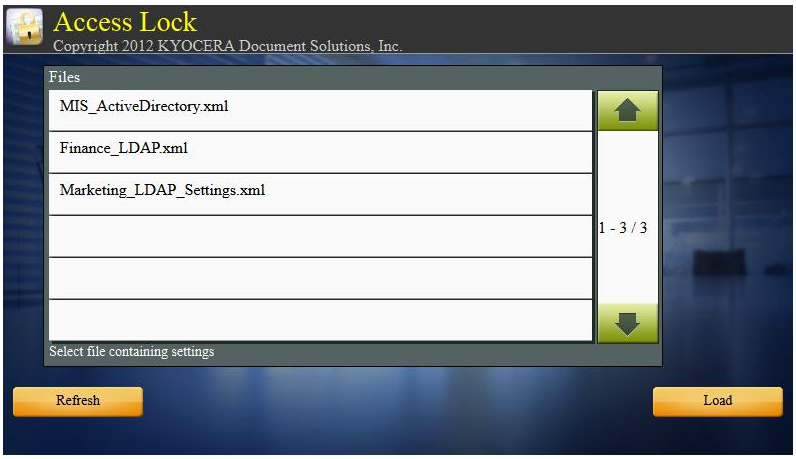


5. Press *Load Settings* button on the bottom-left corner of the screen



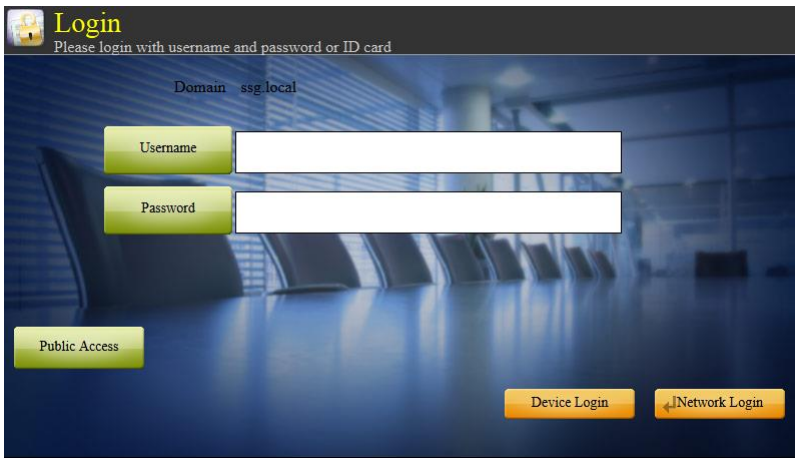
6. Insert USB flash drive and wait for a minute. If the MFP displays a dialog box with the message "Removable memory is recognized. Displaying files. Are you sure?", press No.

7. Press *Refresh* button on the bottom-left corner of the screen. Now the list of files on the drive will be displayed:



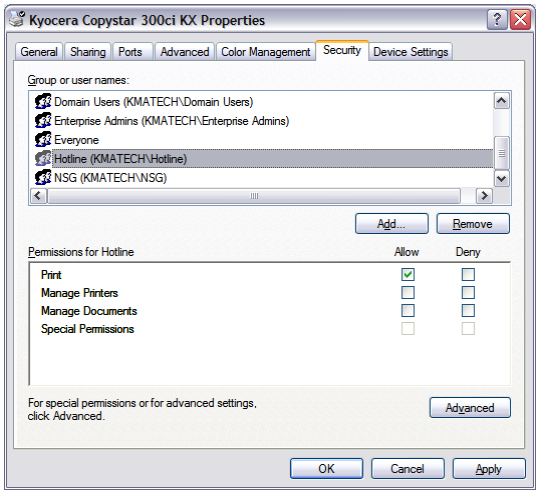
8. Select one file and Press the *Load* button on the bottom-right corner of the screen.

9. MFP panel will display “Access Lock: Settings Loaded OK”. Press the Exit button and then the Logout button for settings to take immediate effect.

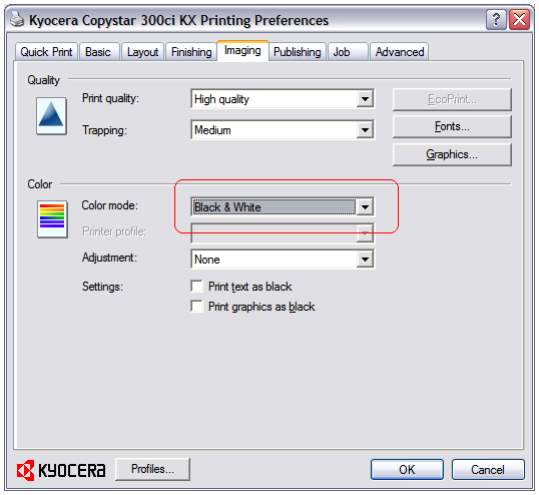


Step 4. Setup Print Authorization

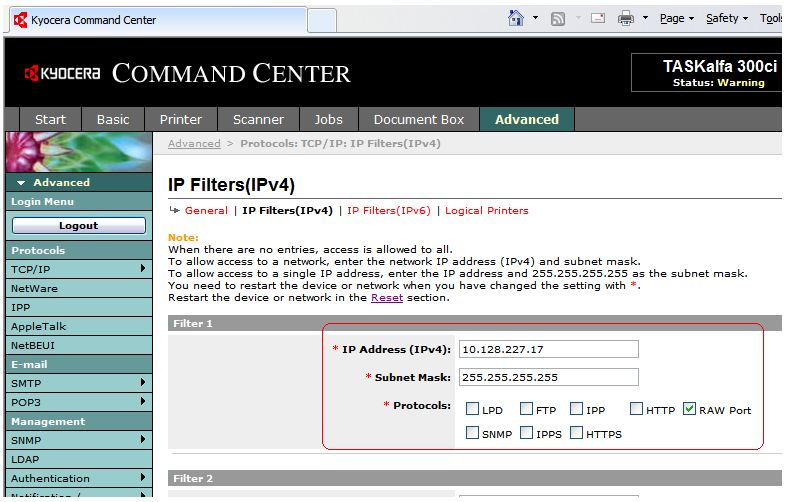
Printing from PCs is restricted using Microsoft Windows Sharing and Security settings. User groups can be allowed or denied printing privilege from within the Security tab in each printer’s properties.



To prevent color prints, set printing preferences on the print queue to *Black & White* printing. Two queues can be setup for each MFP, one queue setup to allow color prints, while the other is set to *Black & White* only.



To prevent peer-to-peer printing and channel all printing through the print server, setup IP filter on the MFP. This would allow only jobs originating from the print server to be printed.

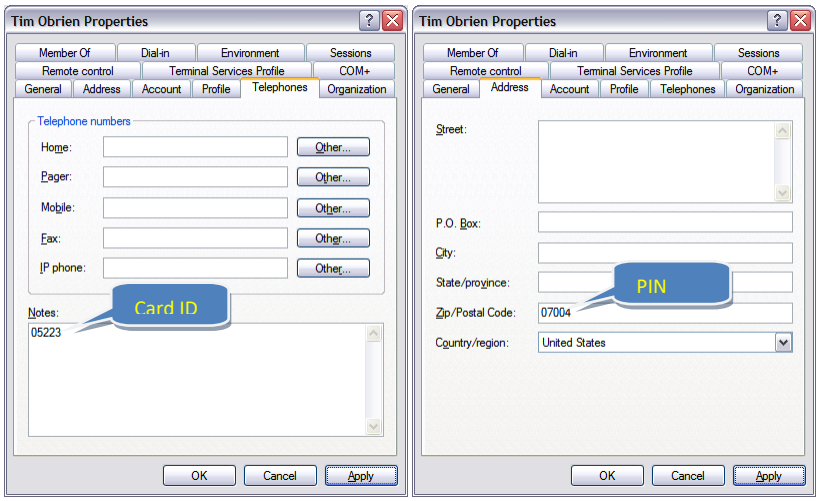


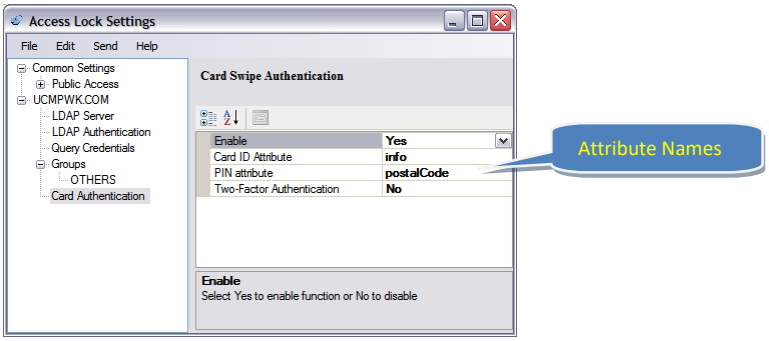
Step 5. Configuring Card Authentication

Network connected card readers from RFIdeas are supported for authentication. The following sections explain how to setup and configure card readers. When user swipes card at the reader, the card ID is transmitted to the MFP. The MFP then authenticates the user against LDAP.

Card ID (and optionally, PIN, for two-factor authentication) must be stored in user's LDAP attributes. For Microsoft Active Directory, use the *Active Directory Users and Computers* administrative tool to set user's attribute.

In the following example, the user's card ID is stored in Notes field, and PIN number is stored in Zip/Postal Code field. The LDAP attribute names for Notes and Zip fields are *info* and *postalCode* respectively. These must be entered in the settings utility as shown. PIN number attribute is required only if two-factor authentication is enabled. For a complete list of LDAP attribute names corresponding to active directory's fields, refer to Microsoft documentation.



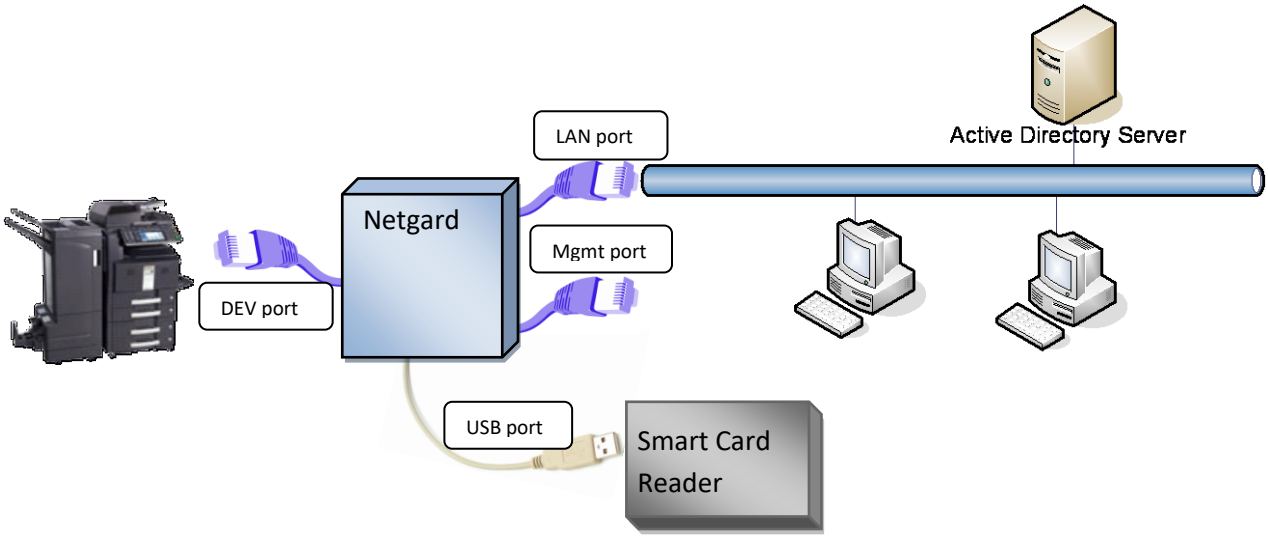


Appendix

Setting up Cryptek Netgard for CAC/PIV authentication

Network Configuration

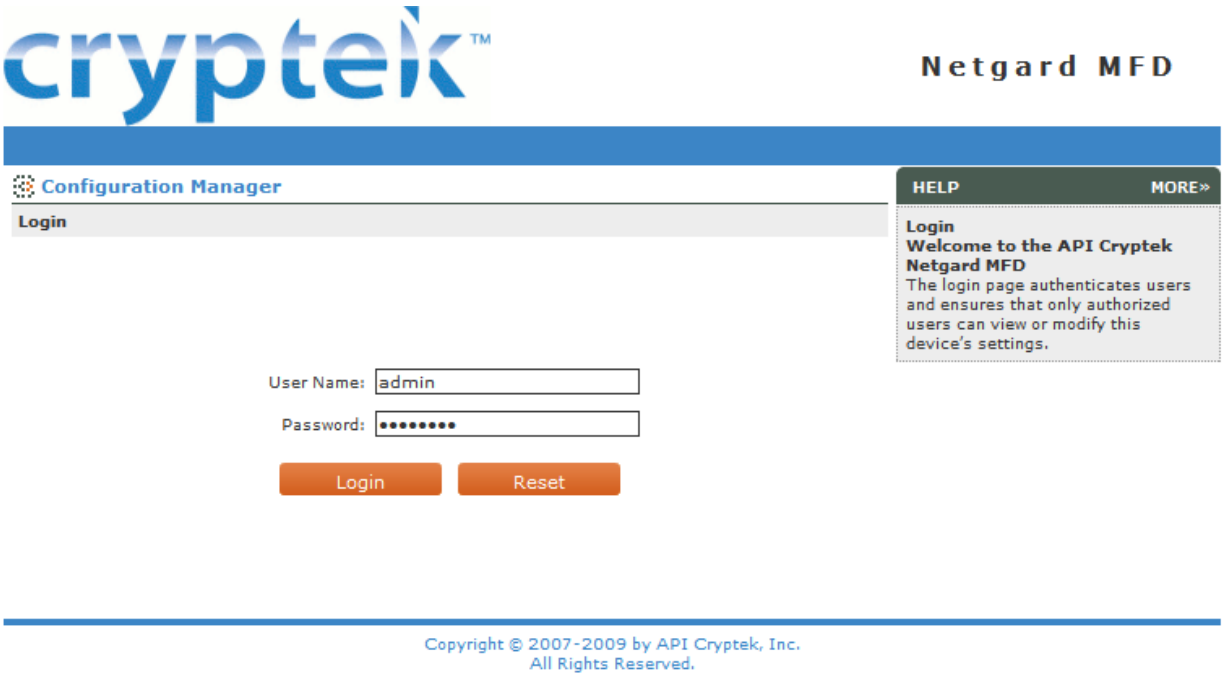
The Netgard device is placed in-between the MFP and the LAN. It acts as an ON-OFF switch, connecting or disconnecting the MFP from the LAN. When a user authenticates successfully using a CAC/PIV card, the Netgard connects the MFP to the LAN, allowing it to access network resources including shared folders and email servers.



- Dev Port: Connects Netgard to MFP.
    - Default network address of netgard on this port: 192.168.10.1.
    - MFP must be set up to use a static IP address of 192.168.10.30.
- LAN Port: Connects Netgard to LAN
    - Netgard address on this port is configured with DHCP or static IP compatible with the LAN.
- Mgmt Port: Management port, used to connect laptop directly to Netgard for configuration purposes.
    - Default network address of netgard on this port: 192.168.20.1
- USB Port: Smart card reader is connected to the Netgard

Netgard Setup and Configuration

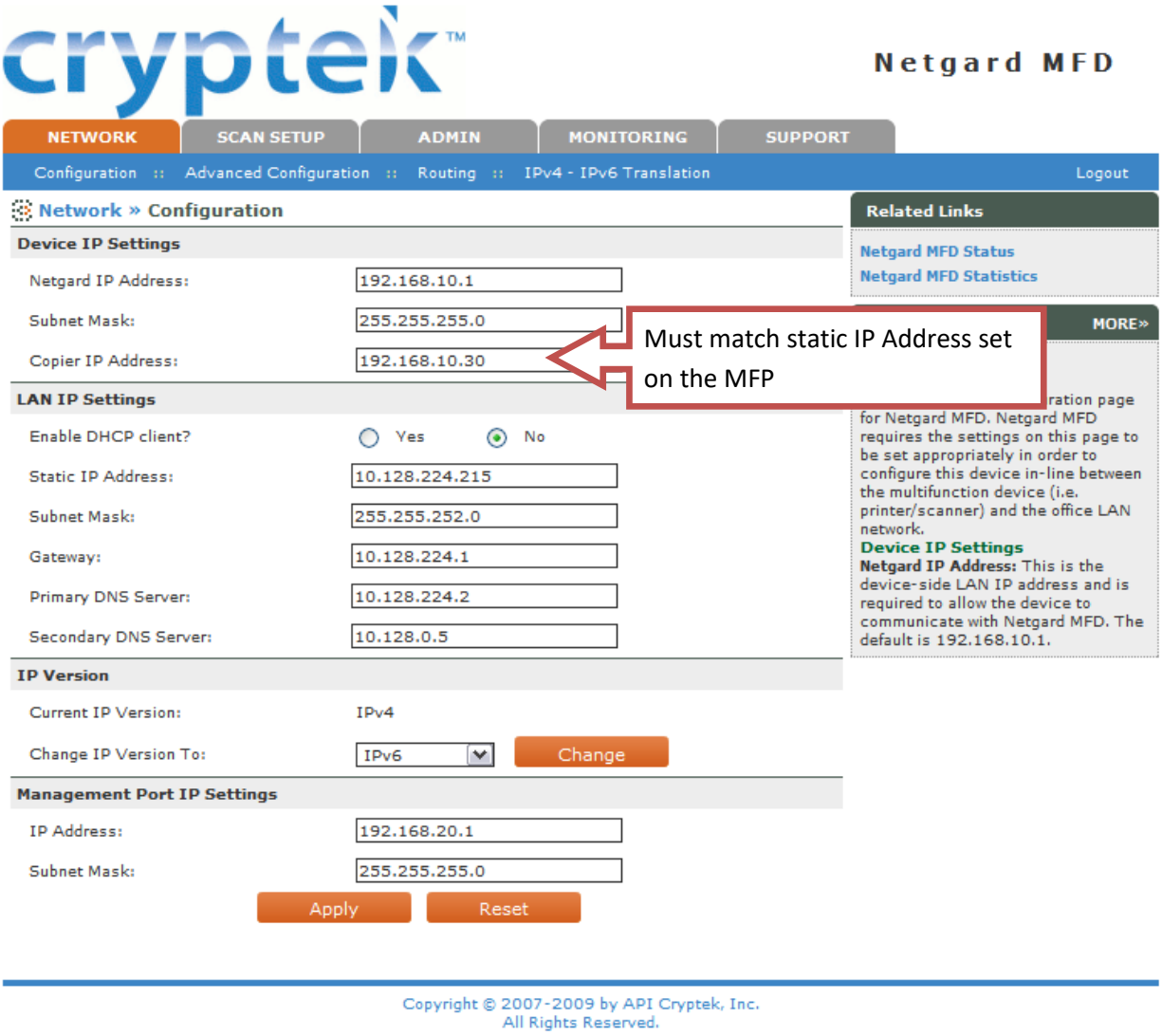
- To configure the Netgard, open a browser to https://<netgard_ip>:8080/.
- Login with management username and password (by default, username=admin and password=password).
- Refer to Netgard Administration Guide for details on how to do basic setup and configuration.



Configuring Netgard for Access Lock

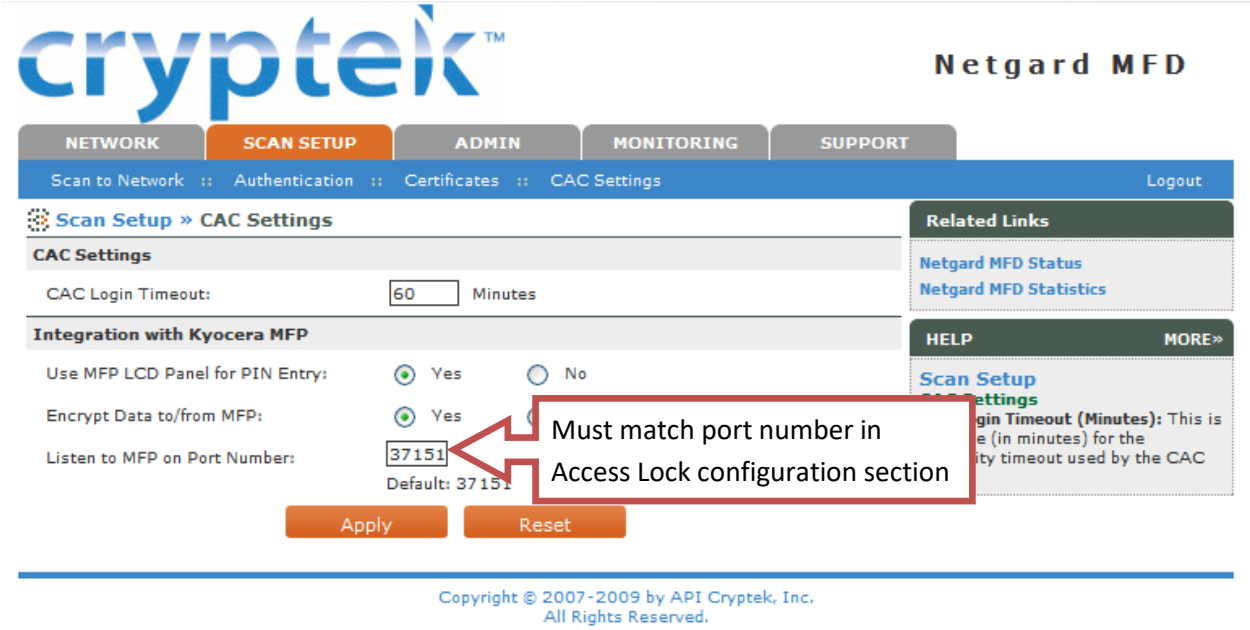
1. Configure Networking Settings

- Open Network → Configuration
- Configure Device IP section as shown in the screen shot below.
    - Setup MFP to use a static IP address (192.168.10.30)
- Configure LAN IP settings to suit the network environment.



2. *Setup CAC settings*

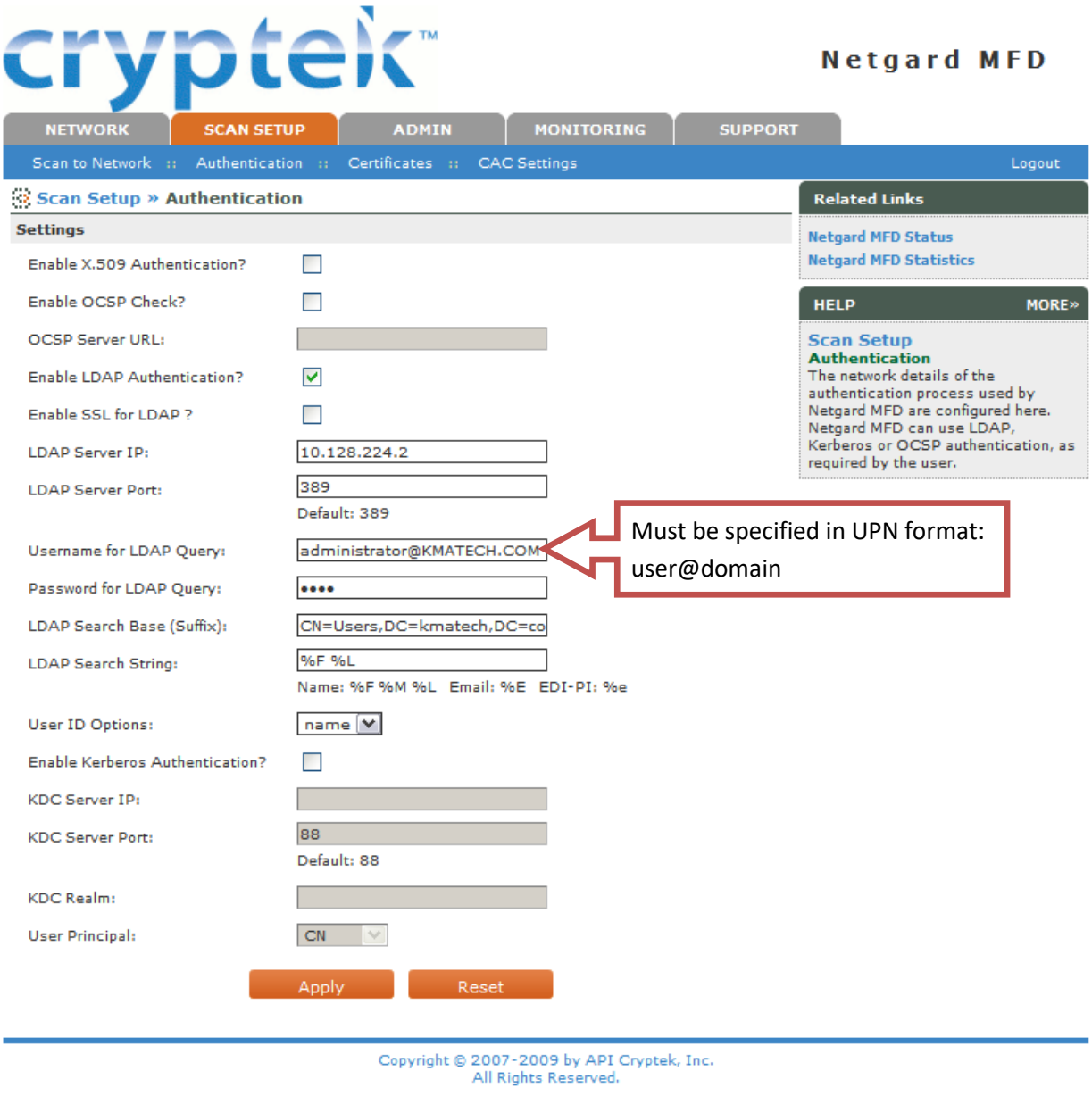
- Open Scan Setup → CAC Settings
- Select Yes to 'Use MFP LCD for PIN Entry'.
- Select Yes to 'Encrypt Data to/from MFP'.
- Enter 37151 for 'Listen to MFP on Port Number'.



3. *Setup LDAP Authentication*

NOTE: This step is required only if Look-up LDAP option is enabled in access lock configuration.

- Open Scan Setup → Authentication
- Enable 'LDAP Authentication'
- Enter Active Directory domain controller address for LDAP Server IP
- Set LDAP Server Port to the default value of 389.
- Enter a user account in UPN format (as shown below) and provide a password.
- Enter the LDAP search base suffix. User accounts contained in this LDAP tree can login.
- Set LDAP Search String to '%F %L' and select 'name' for User ID options (as shown below).

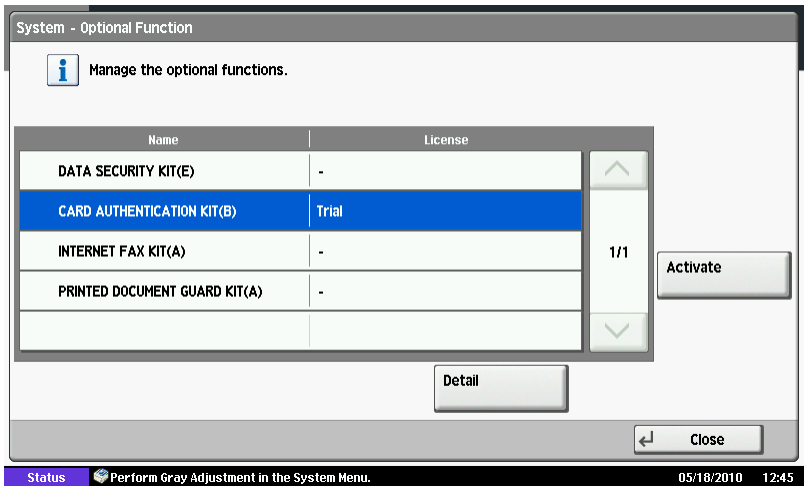


Setting up Proximity Card Reader (USB connected)

To utilize USB-connected card readers for authentication, Card Authentication Kit must be purchased from Kyocera for each MFP. The kit includes a card reader and software license to activate the card reader. Please contact your Kyocera dealer to obtain pricing, availability and compatibility information.

To activate Card Authentication Kit (B):

1. Open System Menu → System → Optional Function
2. Select Card Authentication Kit (B) and press the Activate button
3. If you have an activation code, enter it using the keypad, otherwise press the 'Trial' button to start a trial period. Card Authentication Kit (B) can be used in trial mode. Two 30-day trial periods will be available.



At the time of this writing, the following card types are supported. For compatibility information on other card types not listed below, please contact your Kyocera dealer.

Type of card
HID
Mifare
HID iClass

Setting up Proximity card reader (Network connected)

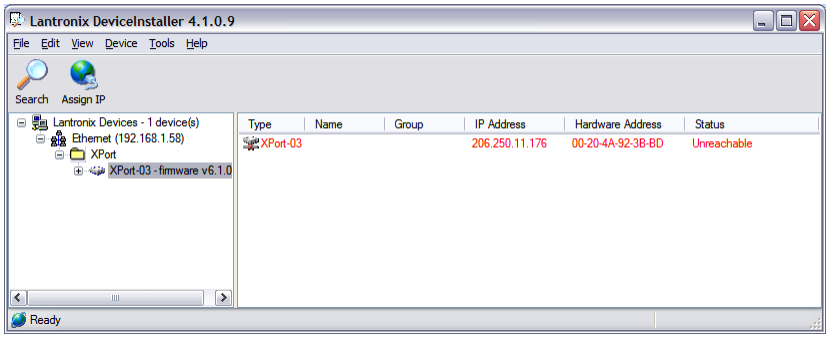
This section describes how to setup RFIdeas® PcProx network connected HID card reader to work with Kyocera MFPs. Please refer to RFIdeas® web site for details on purchasing compatible card readers.

NOTE: USB-connected card readers are not supported now.

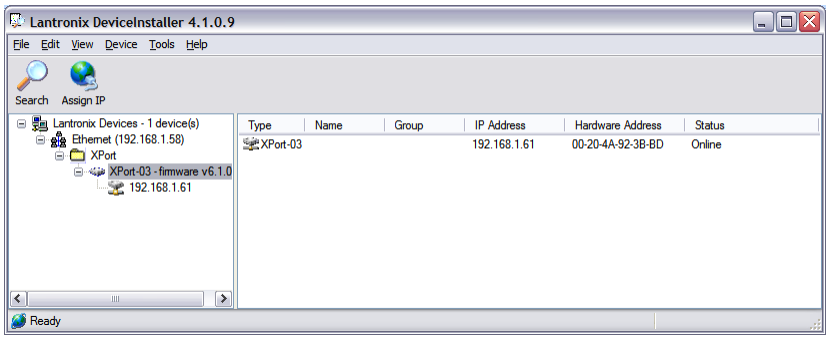
RFIdeas network connected HID card reader

Lantronix DeviceInstaller software can be obtained from RFIdeas website. This software helps locate and configure network connected card readers.

Open Lantronix DeviceInstaller software by clicking on Start → All Programs → Lantronix → Device Installer.

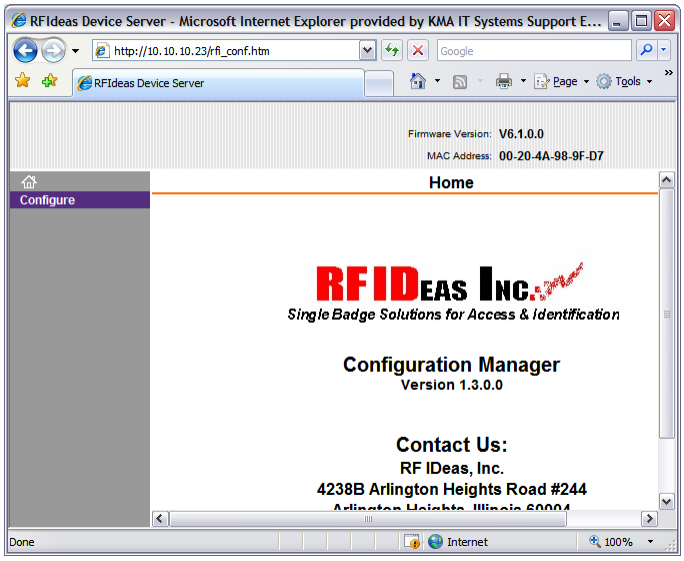


This utility will discover card readers connected to the network and display them in a tree-view as shown above. Select the device and click Assign IP button on the toolbar. This would bring up the Assign IP Address wizard. Follow the instructions in the wizard to configure DHCP or static IP address for the card reader.

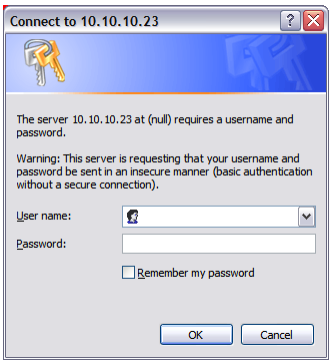


After the device has been assigned a valid IP address, check values for Default Gateway and Subnet mask to ensure correctness. Open the card reader's web page in Internet Explorer by entering the

devices' IP address.



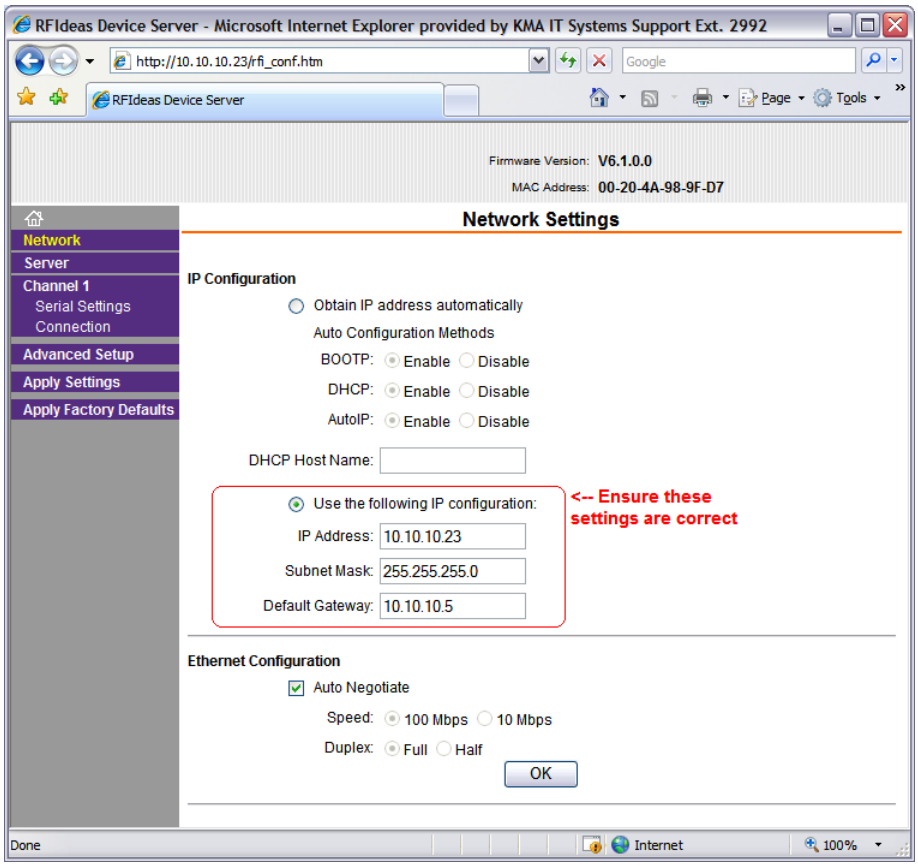
Click on the Configure link on the left of the page and when prompted for username and password, simply click OK, leaving the fields blank.



Configure each setting on the web page as shown below. In each page, after making the changes, click the OK button at the bottom. After all pages are configured, click the Apply Settings link to save changes and restart the card reader.

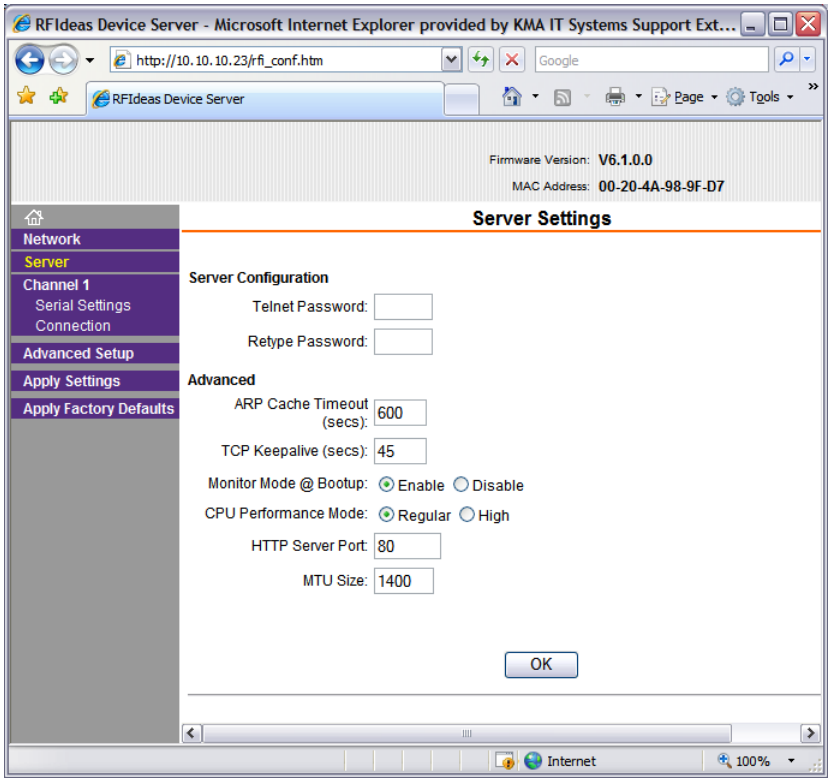
Network Setting

Click on *Network* link and ensure the *IP Address*, *Subnet Mask* and *Default Gateway* for the card reader are entered correctly.



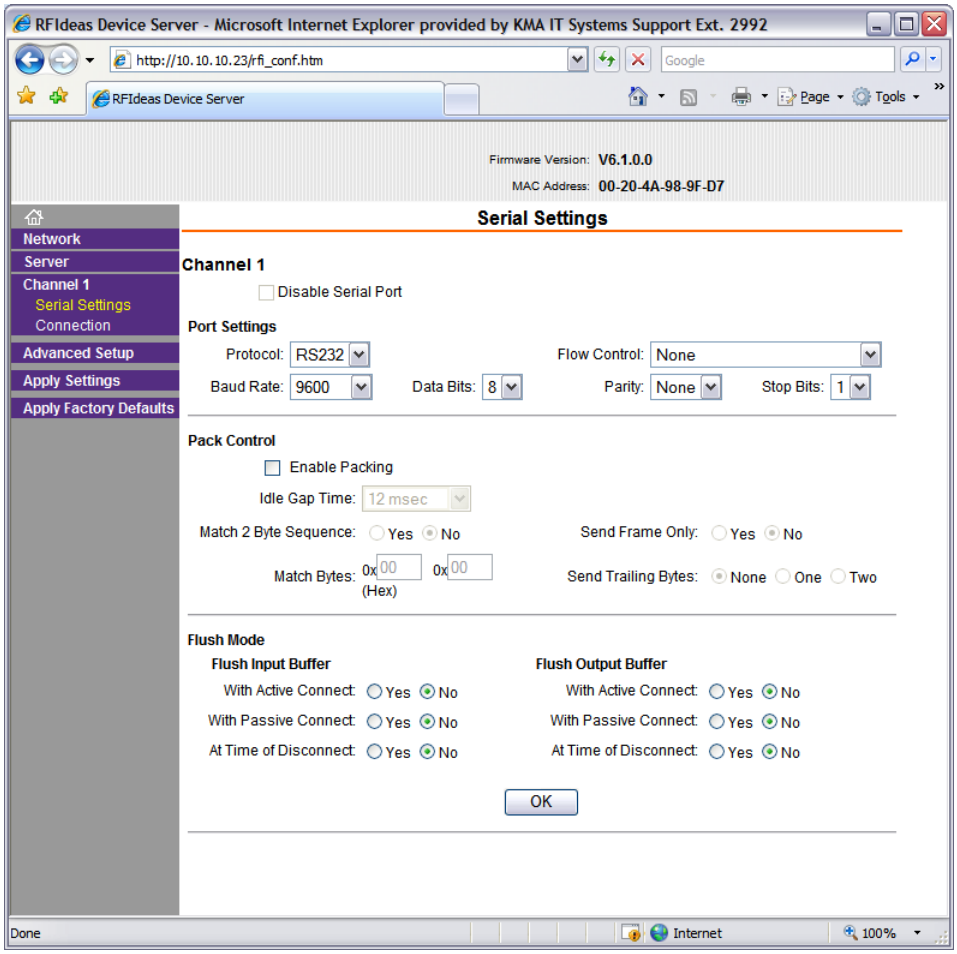
Server Settings

Click on the *Server* link and ensure the settings match values shown below.



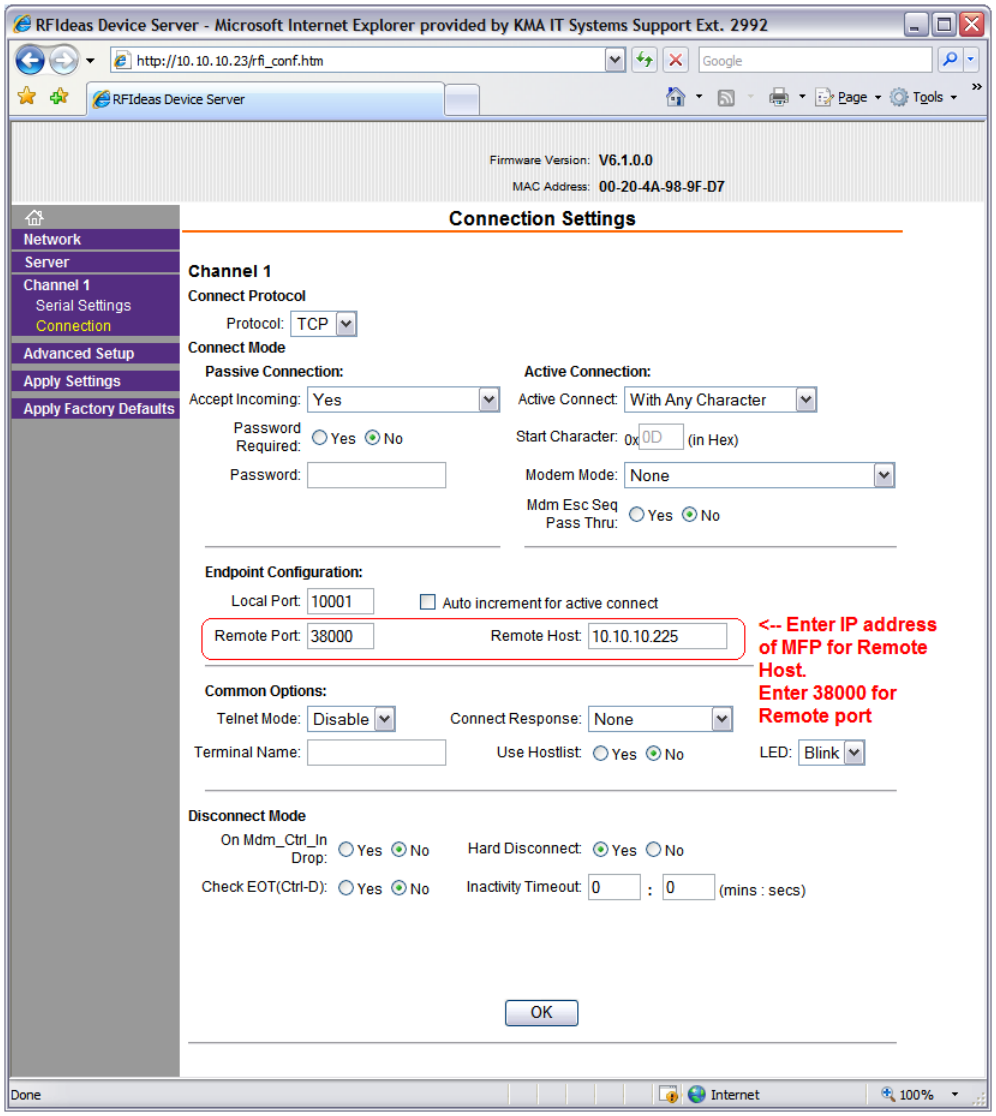
Channel 1: Serial Settings

Click on *Serial Settings* and ensure the settings match those shown below.



Channel 1: Connection

Click on the *Connection* link and enter the MFP's IP address for *Remote Host* and 38000 for *Remote Port*.



Click the OK button and then click the *Apply Settings* link to save settings changes to the card reader.

Rev. 5.1