# Print Director™

## Konica Minolta Setup Guide



Document revision date:
07/11/2018
colin@blueswift.co.za

Blue Swift
TECHNOLOGIES

# Table of Contents

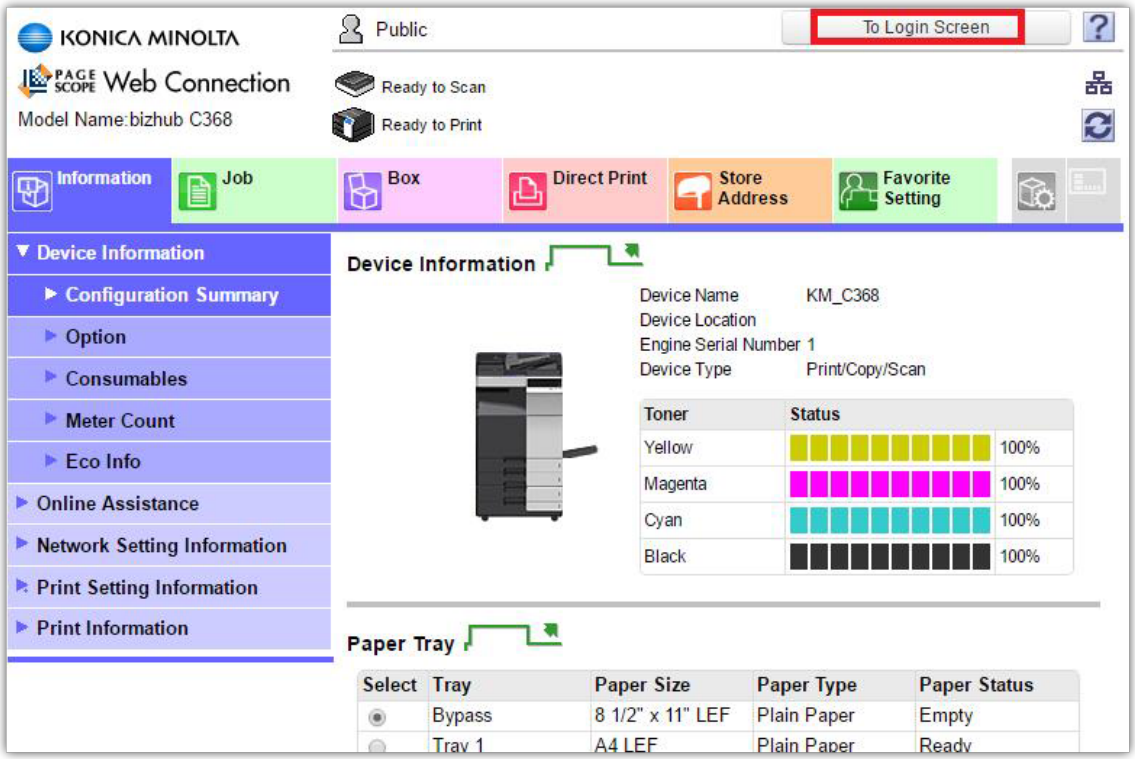
# 1 Preparing the MFP for Print Director embedded

Before we can install the Print Director applications on the printer, we need to configure the SSL settings in the printer's web-interface. There is a slight difference in the procedure between the A3 printers (e.g. 227, C368, C654e, etc) and the A4 printers (e.g. C3350).

If you are setting up an A4 printer, please skip to 1.2 Enable SSL on the MFP (A4 devices).

## 1.1 Enable SSL on A3 devices

Open a web browser. In the Address Bar, enter the IP of the MFP (e.g. http://192.168.10.10). The following page will be displayed:




Click the **Logout** button in order to log back in as the "Administrator" user. Choose the **Administrator** option and enter the admin password.

Enter the Administrator password (default is 1234567812345678) and click **OK**.

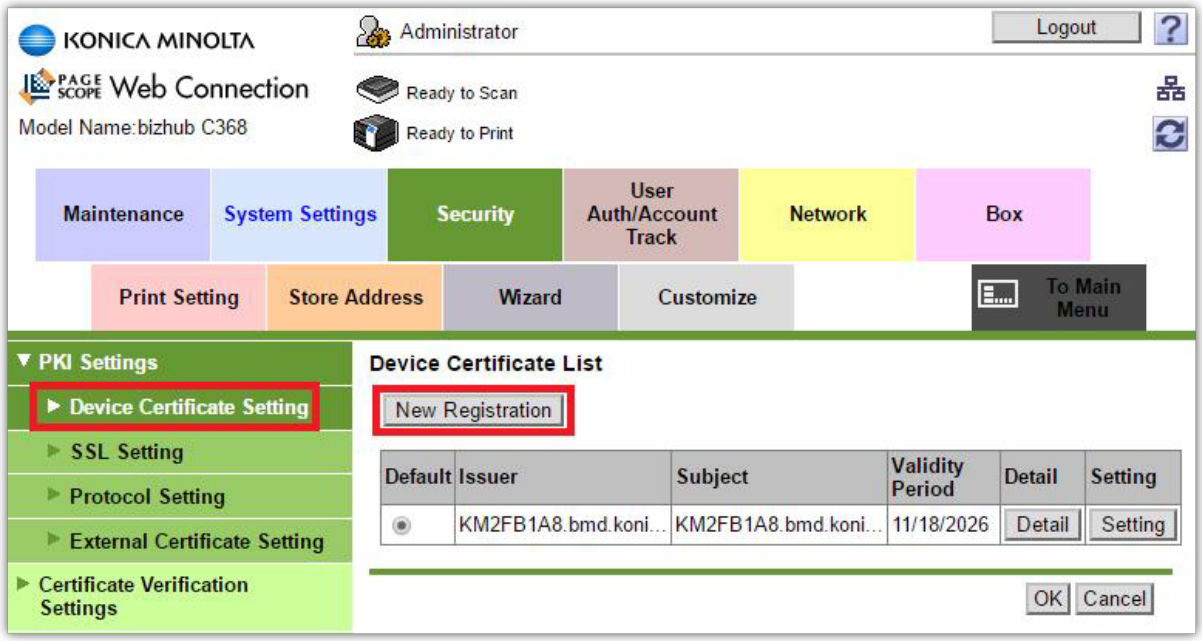

Click **Security** then under **PKI Settings**, choose **Device Certificate Setting**.

On the newer range of devices (e.g. C368) there may be a suitable certificate already installed. If the Validity Period is at least 5 years we can use it and the next section can be skipped. If unsure, create a new certificate.

### 1.1.1 Create a self-signed SSL certificate

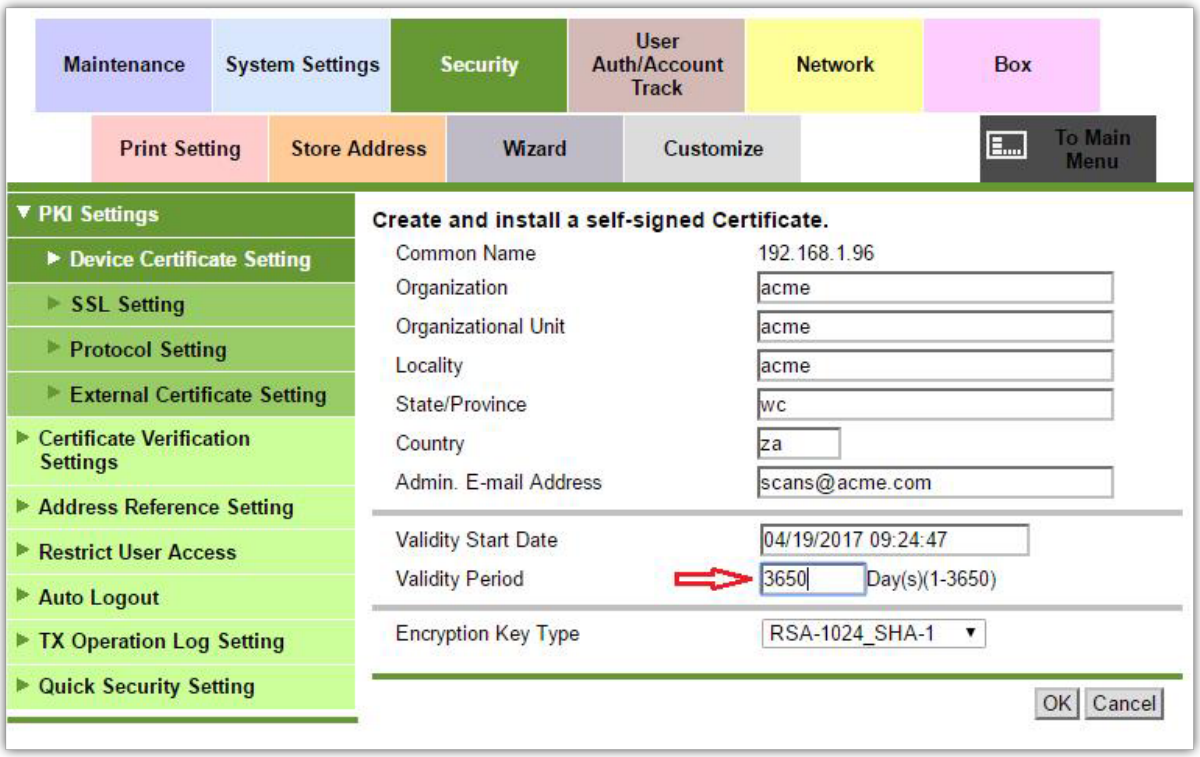
Skip this section if the pre-installed certificate is to be used.

Click **New Registration**.



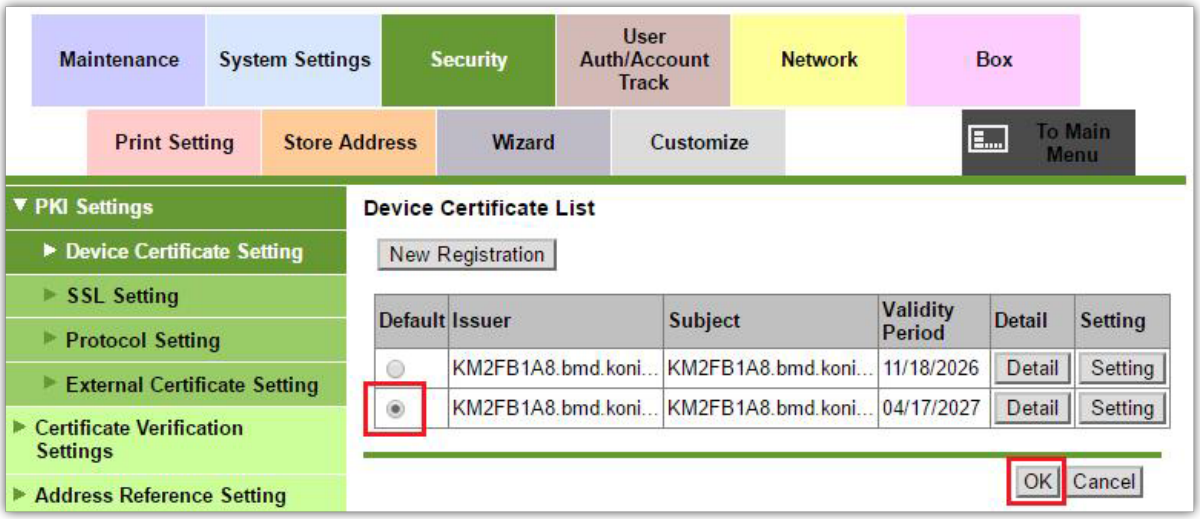
Choose **Create and install a self-signed Certificate** and click OK.


Fill out all the relevant fields. The information entered here is not important except for the Validity Period. Ensure that the **Validity Period** is set to the maximum **3650**.



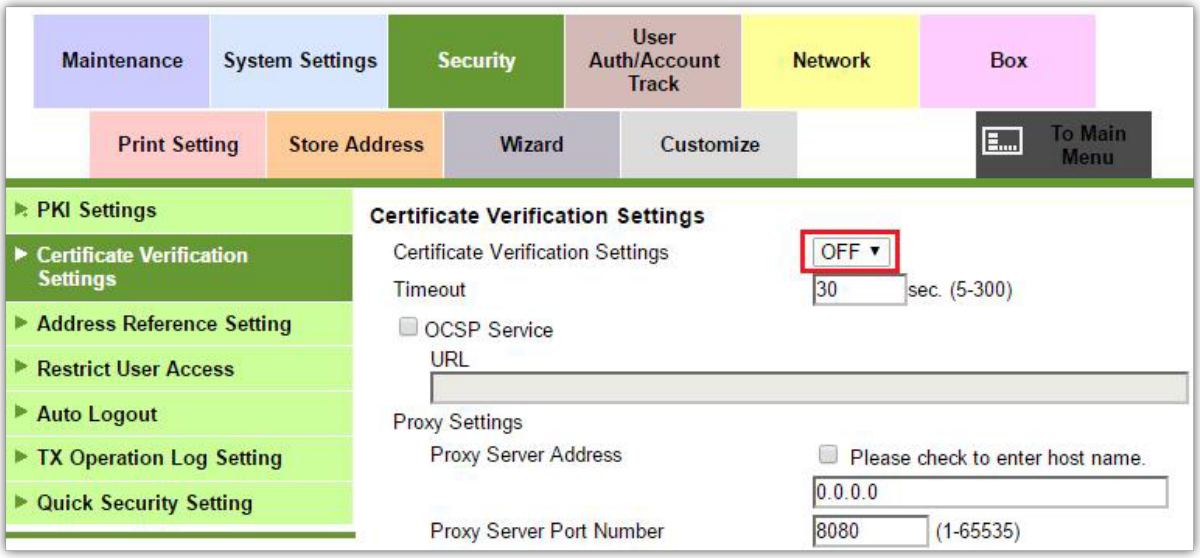
### 1.1.2 Ensure the certificate is the default certificate

Once the certificate has been created, choose the newer certificate and click **OK** as shown below. This will set the newly created certificate as the default.



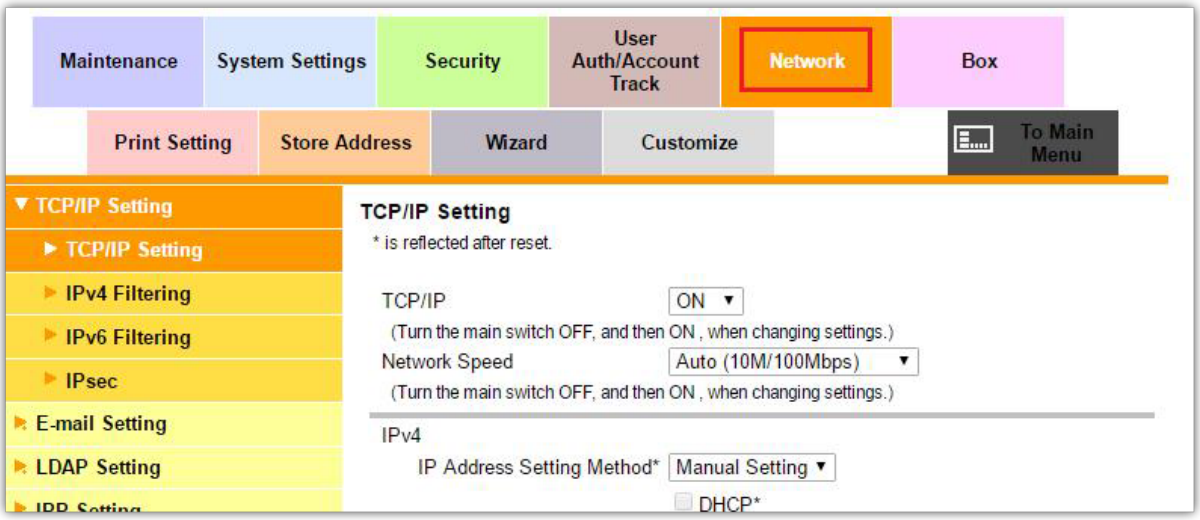

### 1.1.3 Disable certificate verification

Now click **Certificate Verification Settings** and change the setting to **OFF** and click **OK**.

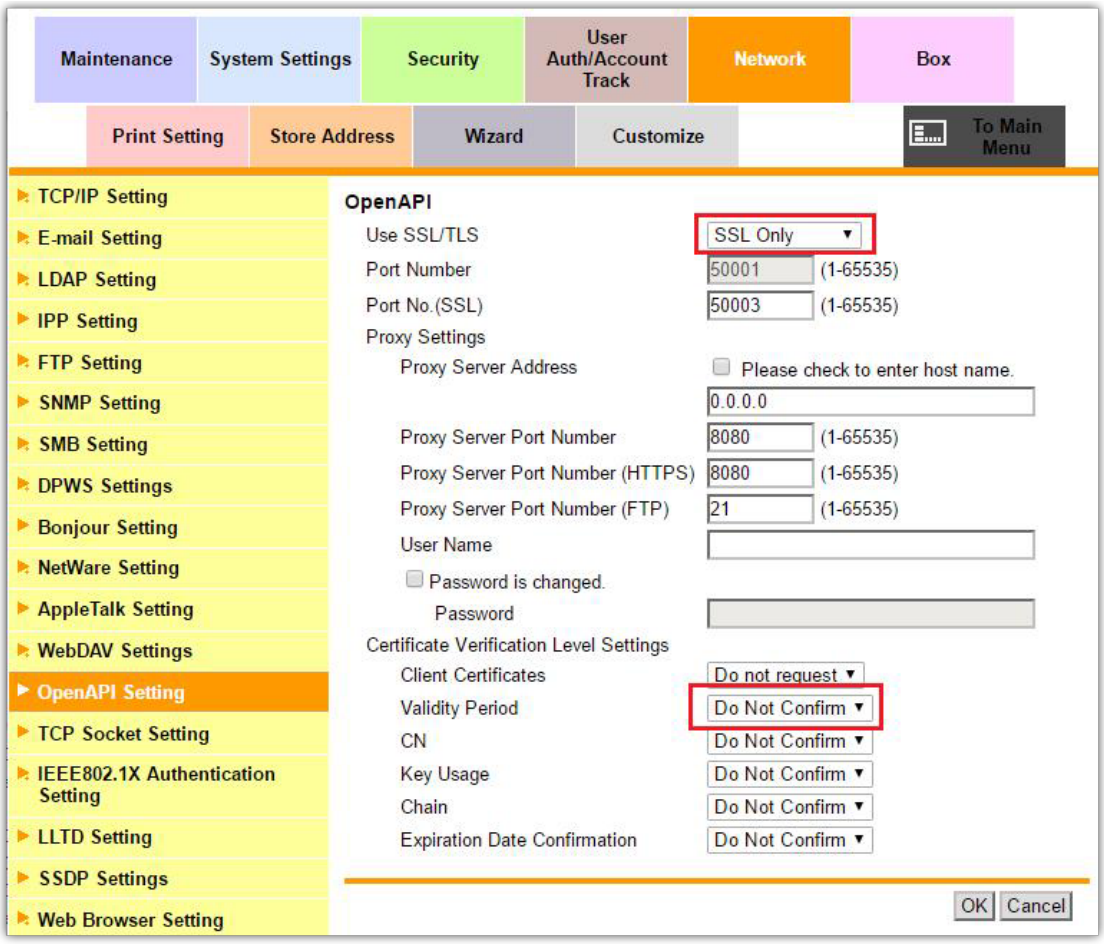


## 1.1.4 Set OpenAPI to SSL Only

Click the **Network Settings** menu.

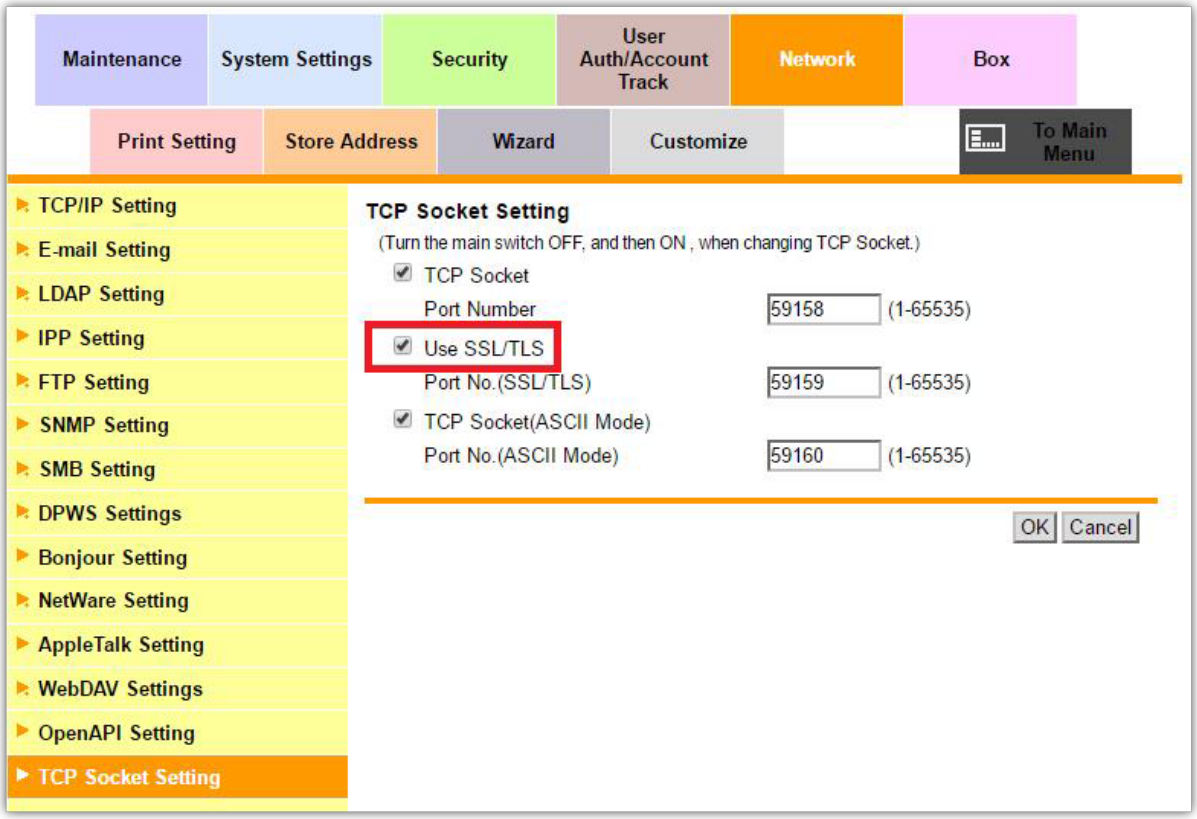



Choose **OpenAPI Setting**. Change the settings to reflect those selected below.




## 1.1.5 Enable Use SSL/TLS on the TCP Socket

Under Network Settings, choose **TCP Socket Setting**. Tick the checkbox labelled **Use SSL/TLS** and click OK. You will be prompted to cycle the power on the MFP. This message can be ignored – power cycling is not normally necessary.

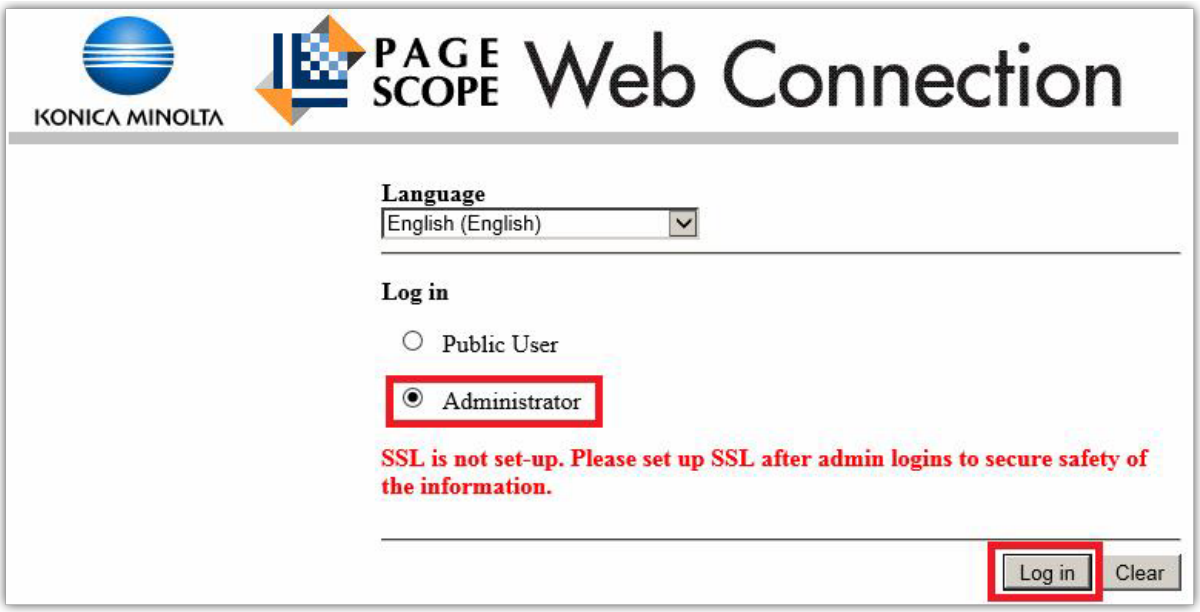



Now the MFP is ready to have the Print Director OpenAPI applications installed. Ensure that you have logged out from the admin settings of the web-interface. Go directly to 2 Configuring the Device in Resource Manager.

## 1.2 Enable SSL on A4 devices

This section is for A4 devices only (e.g. C3350). If you have already done the SSL settings, skip to 2 Configuring the Device in Resource Manager.

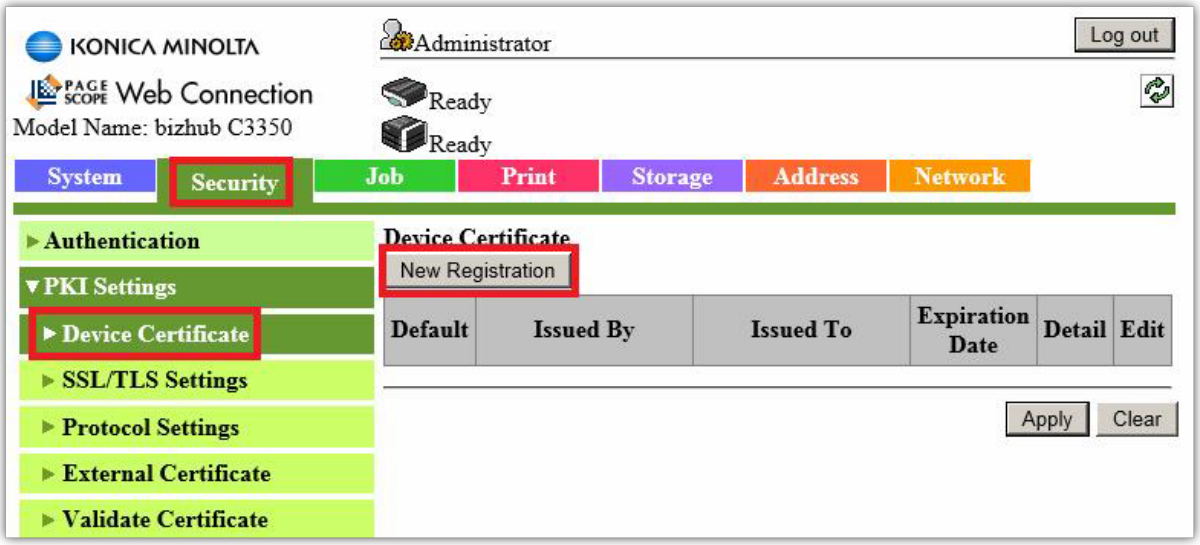
Open a web browser. In the Address Bar, enter the IP of the MFP (e.g. http://192.168.10.10). Choose the **Administrator** option and click **Log in**.



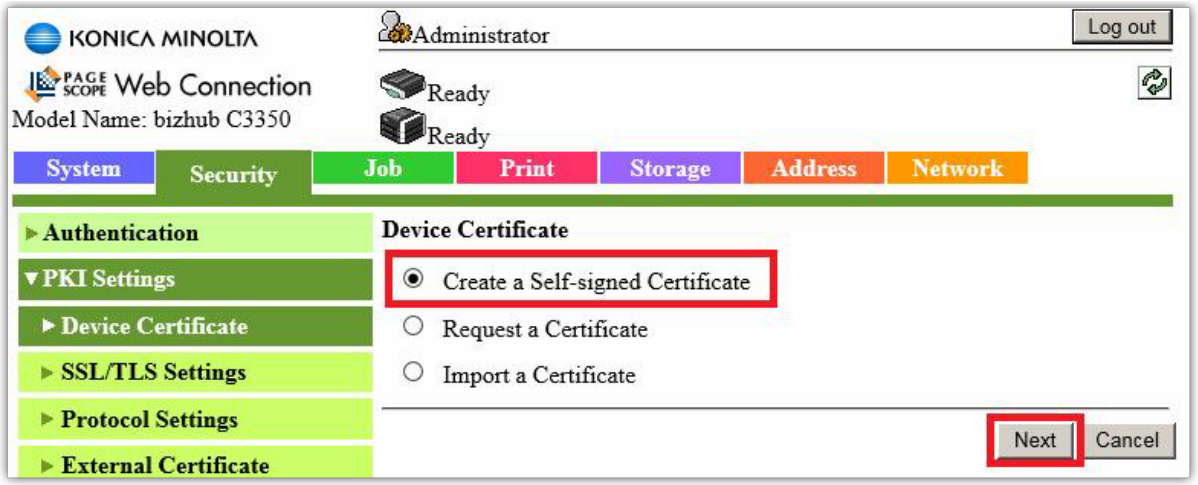
Enter the Administrator password (default is 1234567812345678) and click **OK**.


## 1.2.1 Create a self-signed SSL certificate

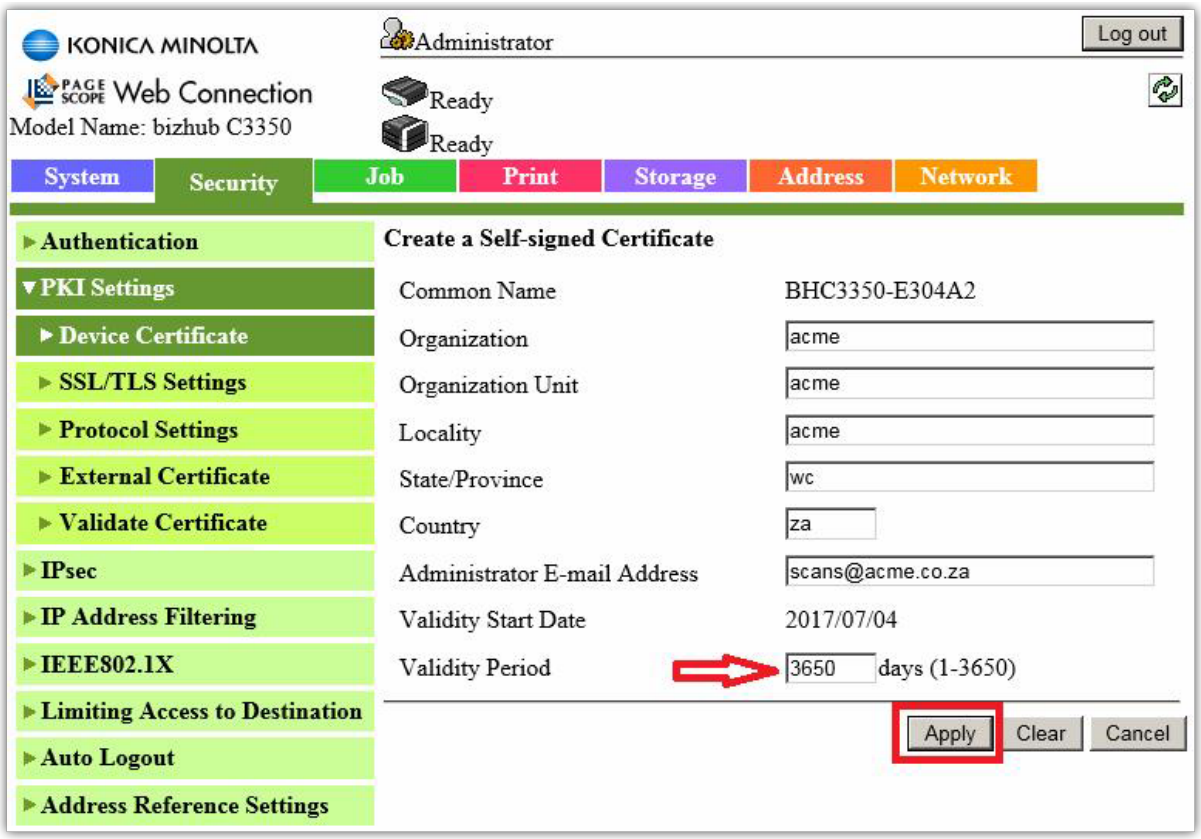
Click **Security** then under **PKI Settings**, choose **Device Certificate** and click **New Registration**.




Choose **Create a self-signed Certificate** and click **Next**.

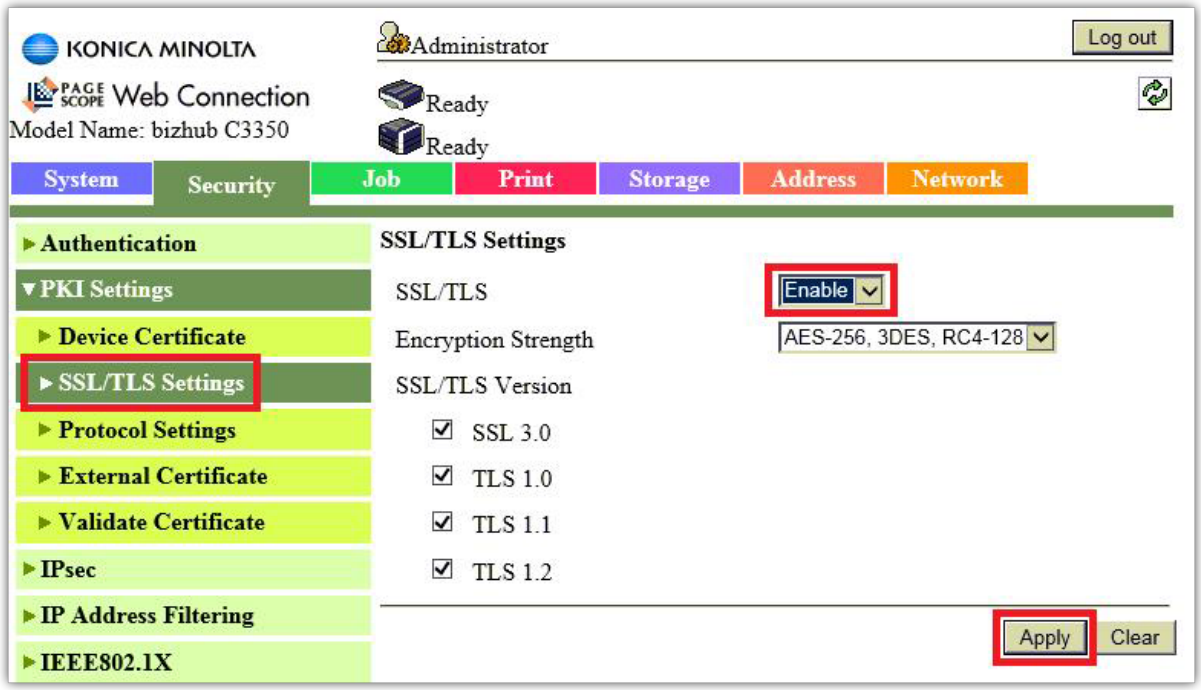



Fill out all the relevant fields. The information entered here is not important except for the Validity Period. Ensure that the **Validity Period** is set to the maximum **3650**.



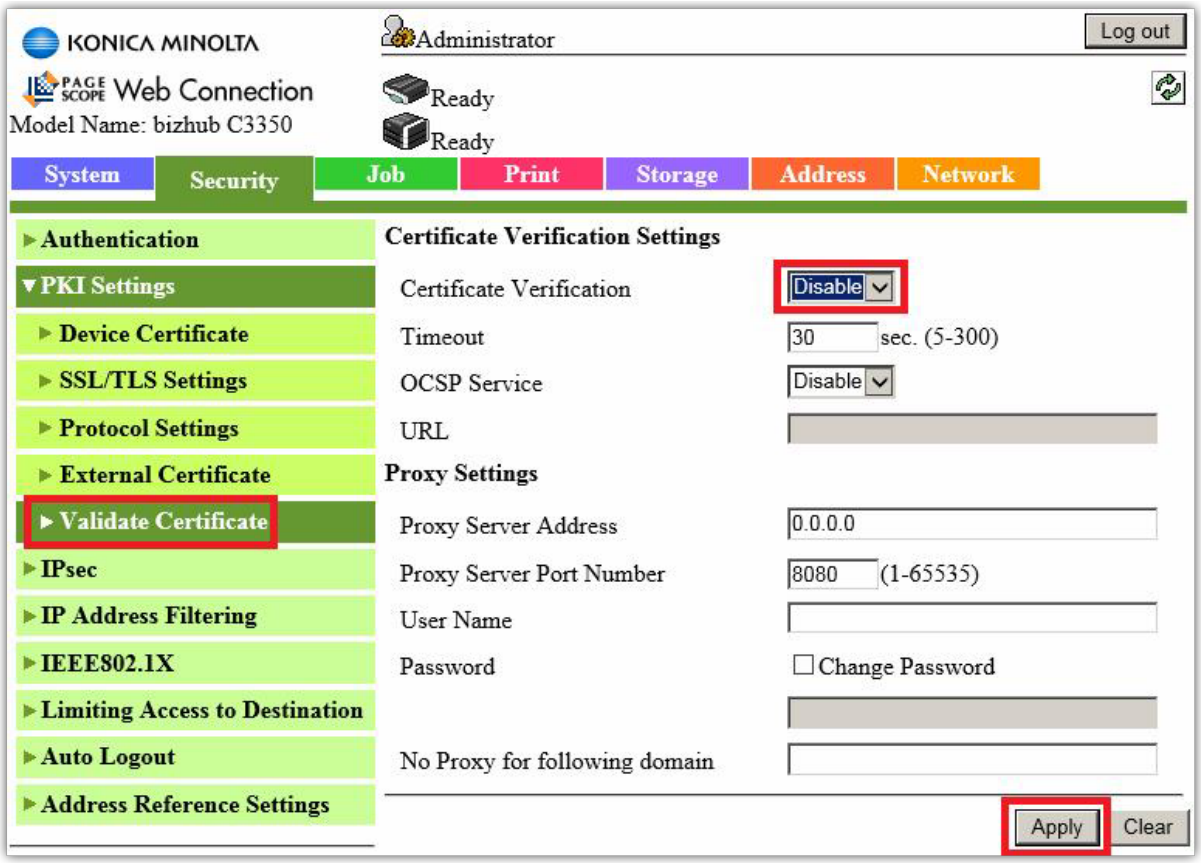

## 1.2.2 Set SSL/TLS to Enable

This step is not required on the A3 devices but it is required on the A4 devices. Under **PKI Settings**, click **SSL/TLS Settings**. Change the **SSL/TLS** dropdown to **Enable** and click **Apply**.



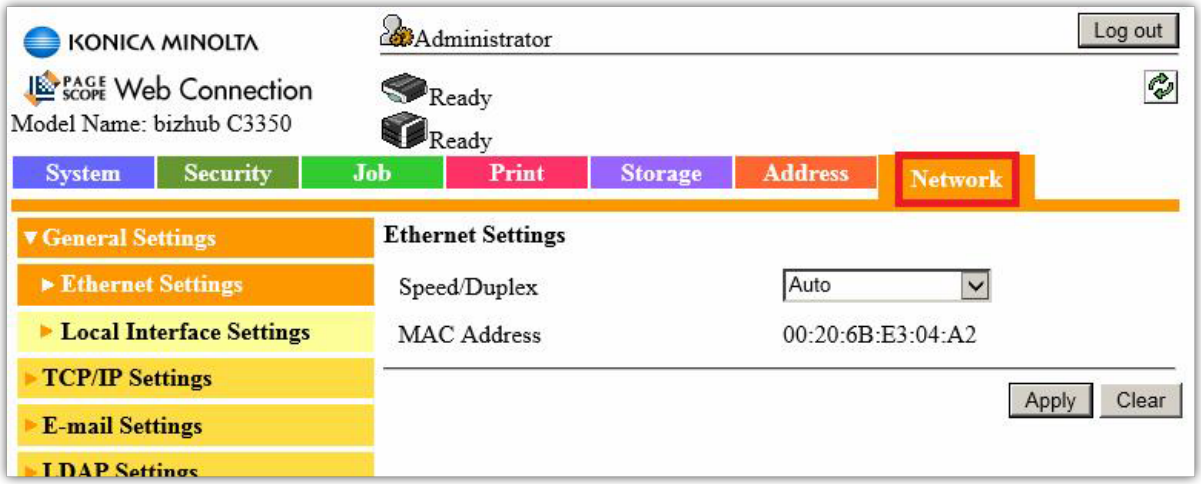
### 1.2.3 Disable certificate verification

Now click **Validate Certificate**, change the **Certificate Verification** dropdown to **Disable** and click **Apply.**

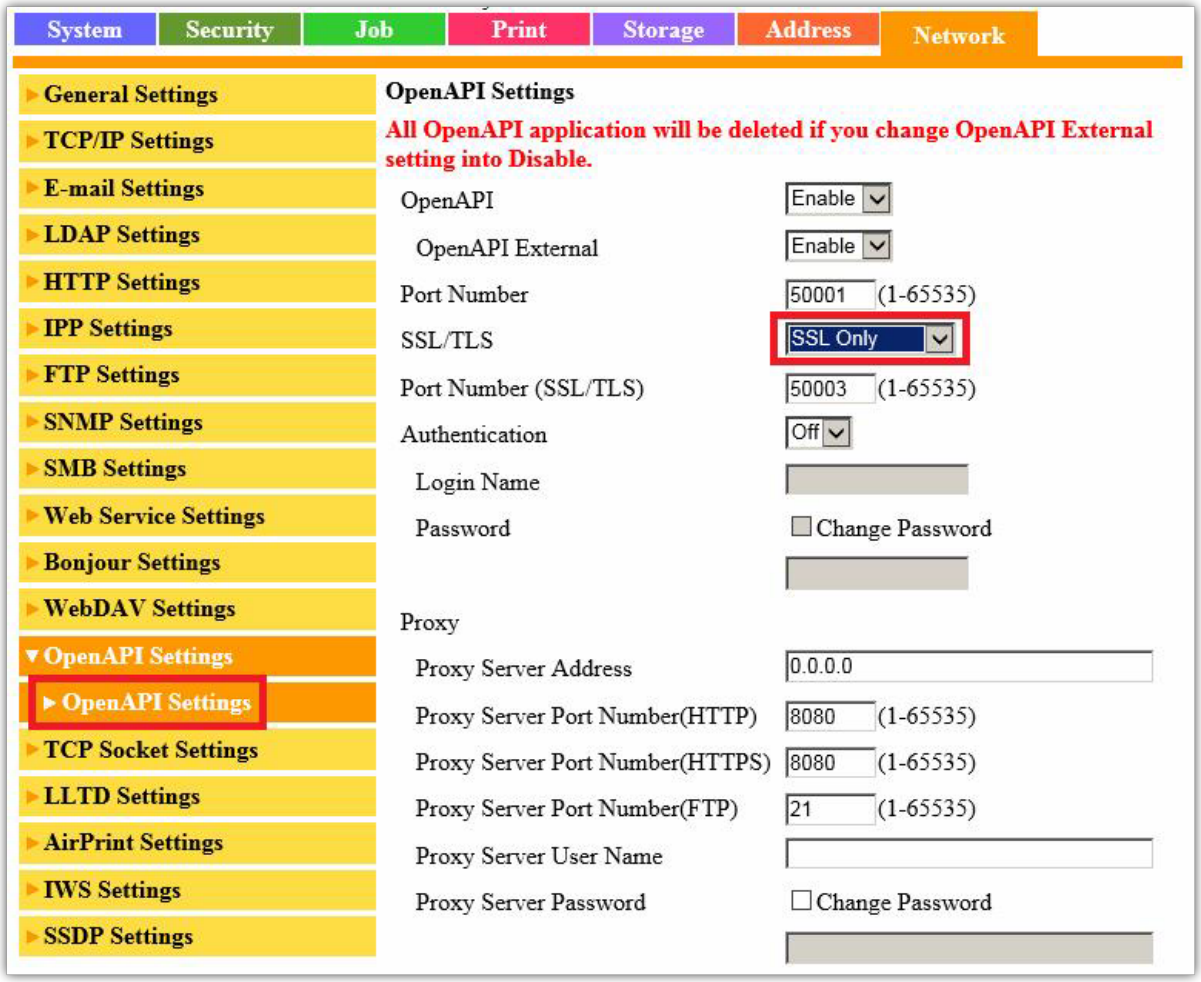



### 1.2.4 Set OpenAPI to SSL Only

Click the **Network Settings** menu.

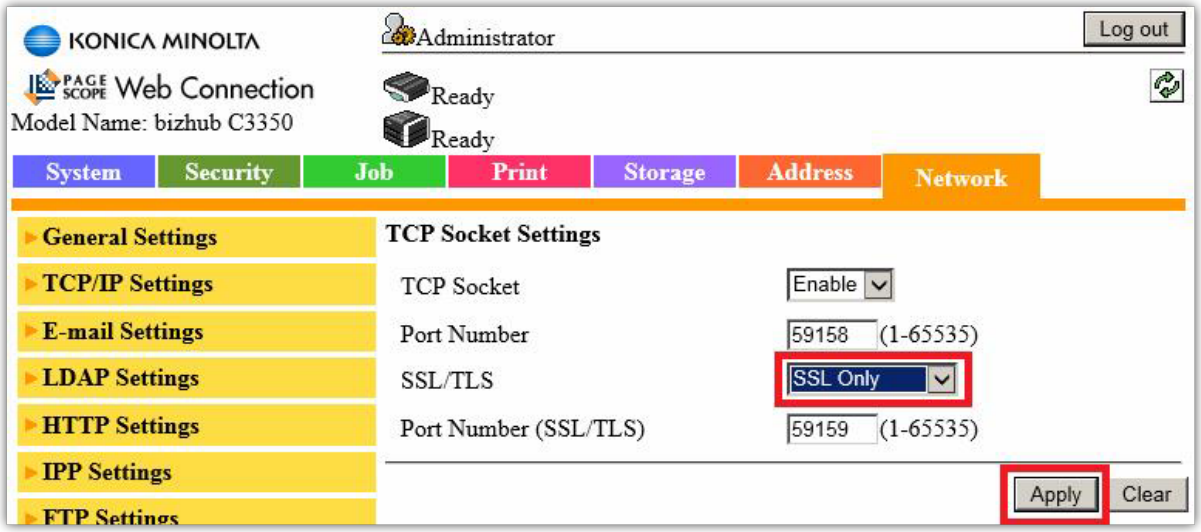


Choose **OpenAPI Setting**. Change the **SSL/TLS** dropdown to **SSL Only** and click **Apply**.




## 1.2.5 Set SSL/TLS to SSL Only on the TCP Socket

Under Network Settings, choose **TCP Socket Settings**. Change the **SSL/TLS** dropdown to **SSL Only** and click **Apply**. You will be prompted to cycle the power on the MFP. This message can be ignored – power cycling is not normally necessary.



Click Log out. You must be logged out of the web-interface in order to configure the device in Resource Manager.

# 2 Configuring the Device in Resource Manager

To enable the integrated applications on the MFP, Resource Manager needs to connect to the MFP and receive responses from the MFP. Note that firewall software such as Windows Firewall will popup when a network connection is made and the user can choose to unblock the application. If it does not automatically pop up, it may require an exception to be manually created.

## 2.1 Create a firewall exception for Resource Manager

To create an exception for Resource Manager, follow these steps:

- Open the **Control Panel**
- Open **Windows Firewall**
- **Click Allow an app or feature through Windows Firewall**
- Click the **Exceptions** tab
- Click **Add Program**
- Click **Browse**
- Browse to **C:\Program Files\Blue Swift Technologies (x86)\Print Director 2\Resource Manager\ResourceManager.exe**
- Click **Ok** and **Ok** again to exit Windows Firewall

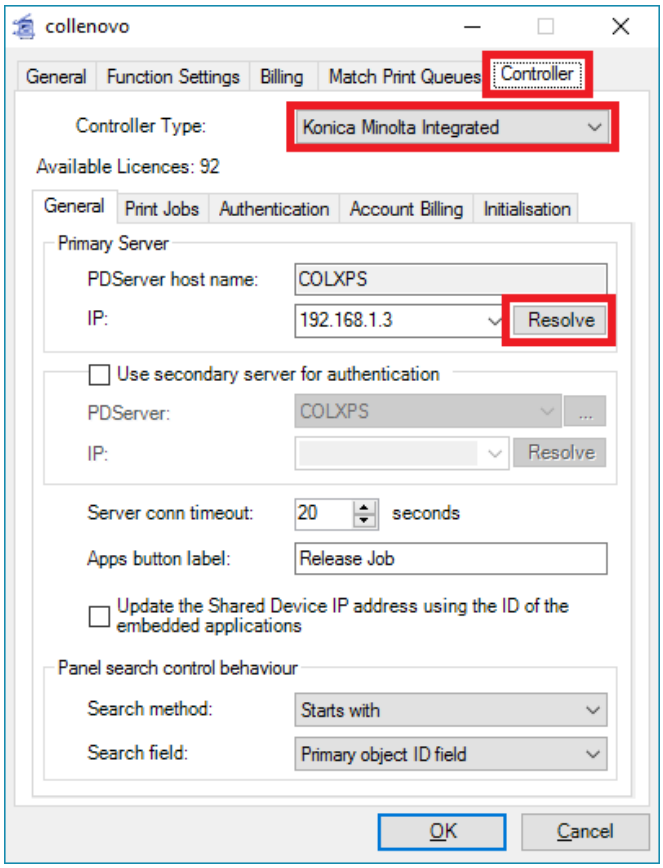
If the workstation has other firewall software running locally, refer to the documentation in order to create an exception for ResourceManager.exe.

## 2.2 Initialising Konica Minolta Integrated applications

Once an exception has been added to the firewall for Resource Manager we can continue to initialise the applications on the MFP. To do this, follow these steps:

- Open Resource Manager (**Start** > **Programs** > **Print Director 2** > **Resource Manager**).
- In the tree view, navigate to **Device Management** > **Shared Devices**.
- If a definition for the MFP in question has not already been created, follow these steps. Otherwise double click the existing device and skip to the next step.
    - In the right hand pane, click **Add**.
    - Enter a descriptive name in the **Device Name** text box.
    - Enter the IP address of the MFP in the **Host or IP** text box.
    - Click the **Ping** button to ensure that the device is accessible over the network.
- Click the **Controller** tab.
- In the **Controller Type** drop down, choose **Konica Minolta Integrated**.

## 2.2.1 General tab




### 2.2.1.1 PDServer IP Address

Firstly, ensure that the **PDServer IP address** is correct. This IP is obtained by doing a DNS resolution on the Managing PDServer hostname for the Device. If the workstation has multiple network adapters it is possible that this IP address is inaccessible from the MFP. If the IP is not correct, click the **Resolve** button. The IPs for each adapter will appear in the drop down. Choose the correct IP address from the dropdown.

### 2.2.1.2 Secondary PDServer

A Secondary PDServer can be configured as an option. This should be considered if the network is not 100% reliable. When a user logs on to the MFP, it will attempt to connect to the Primary PDServer. If no response is received within the timeout (default is 20 seconds) a **Connection Error** message will be displayed on the MFP front panel. If a Secondary PDServer has been configured, instead of showing a Connection Error message, it will attempt to connect to the Secondary PDServer.

If a Secondary PDServer is to be configured, tick the checkbox and choose the PDServer from the drop down. Ensure that the correct IP address is displayed. Note that this will only affect authentication and not PullPrint (Secure Document Release). PullPrint can only connect to the Primary PDServer.

### 2.2.1.3 Apps button label

If another OpenAPI application exists on the MFP (e.g. **Document Navigator**), change the **Apps button label** to something more meaningful (e.g. **App List**). This is because when the user touches the applications button it will show a list of applications (e.g. Document Navigator and PD Release

Job). When there is only one application installed (e.g. PD Release Job) it doesn't show a list and goes straight into the application so the label can be left as **Release Job**.

#### 2.2.1.4 Update the Shared Device IP address using the ID of the embedded applications

If this checkbox is ticked, it means that the next time the printer connects to the server (e.g. a user logs in) the software will check the Shared Device's IP address and compare it to the IP address from where the connection came. These should normally be the same. However, in the event that the printer's IP address has changed (because of DHCP or manual change) it will be different to the one specified for the Shared Device.

The advantage to ticking this checkbox is that the Shared Device IP address will automatically be updated if the physical printer's IP address changes. This means that queues can be matched correctly and future initialisations will connect successfully.

If however, the printer connects to the server through a router using NAT, the IP that the server will 'see' will be that of the router and not the physical printer's IP. In this case, this checkbox must be unticked. Otherwise the IP address for the Shared Device will be changed to that of the router.

#### 2.2.1.5 Panel search control behaviour

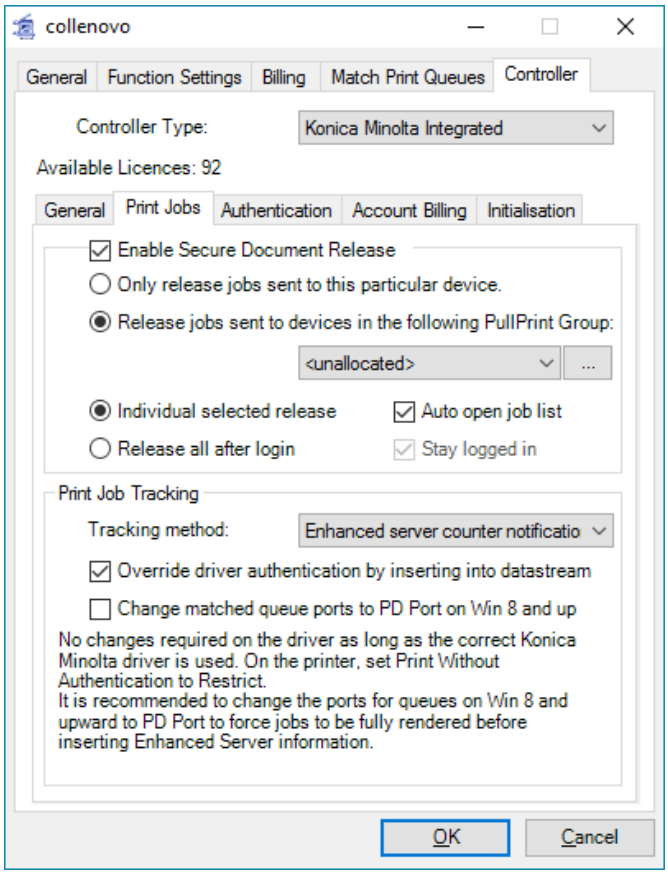
**Panel search control behaviour** affects the way items are searched. If a search control is used for Users, Accounts or Matters the default search method is **Starts With**. This can be changed to **Contains**. This means that if a user is searching for an account called **Johnson**, and enters **son**, the account will be shown in the results. If it is left on **Starts With**, **son** will not be matched**.**

**Search field** affects which field is searched. Normally for a User search, only the Controller User ID field is searched. For example, if a User's Controller User ID is JOHSMI001 and their full name is John Smith, when the user searches it will only match characters contained by JOHSMI001. So if they search for John it will not match unless the setting is changed to **Object name** or **Object ID and name**. Similarly, for an Account search it will only match Account Codes by default. If the setting is changed to **Object name** or **Object ID and name** it will search using the Account Names as well. This is especially useful when the Account Codes are numbers which are difficult to remember. It is much easier for the user to search on the Account Name.

Here is the definition of Object ID and Name for each object type:

- User: Object ID = Controller User ID Object Name: User Full Name
- Account: Object ID = Account Code Object Name: Account Name
- Matter: Object ID = Matter Code Object Name: Matter Name

## 2.2.2 Print Jobs Tab




### 2.2.2.1 Secure Document Release and "Follow me" printing

If Secure Document Release (jobs are held until user requests the print at the MFP after authentication) is going to be used on this MFP, tick the **Enable Secure Document Release** checkbox. This means that jobs will be held at the print server (or workstation under direct-to-ip printing) until the user releases them at the MFP.

If the client would like to release jobs sent to other MFPs (Follow Me printing) choose the **Release jobs sent to devices in the following PullPrint Group** option. All MFPs that use compatible drivers should be put in the same PullPrint Group. Typically one PullPrint Group is created for colour devices and another is created for monochrome devices. To create a PullPrint Group, click the ... button next to the **PullPrint Group** drop down. Here one can create/edit/delete PullPrint Groups. Ensure this MFP is placed in the **PullPrint Group** that contains other MFPs that have compatible drivers

Jobs can be released automatically as the user logs in by choosing the Print all jobs after login option. Otherwise jobs are released by touching the Release Job button after logging in.

### 2.2.2.2 Print Job Tracking

By default, print jobs are tracked using **Enhanced server counter notification.** The other option is **Datastream interpretation** which reads the spool files that passes through queues that are matched to devices. There are pros and cons to each method.

#### Track print jobs via Enhanced server counter notification (OpenAPI print tracking)

This is the recommended method for tracking print jobs because it is close to 100% accurate. It also

allows for spool file authentication which means no one can bypass the software and print directly to the printer. Ensure that the **Override driver authentication by inserting into datastream…** checkbox is ticked.

However, there are some cases where Enhanced Server tracking is not supported:

- If the printer is fitted with a Fiery controller.
- If the users need to print 1200dpi printing.

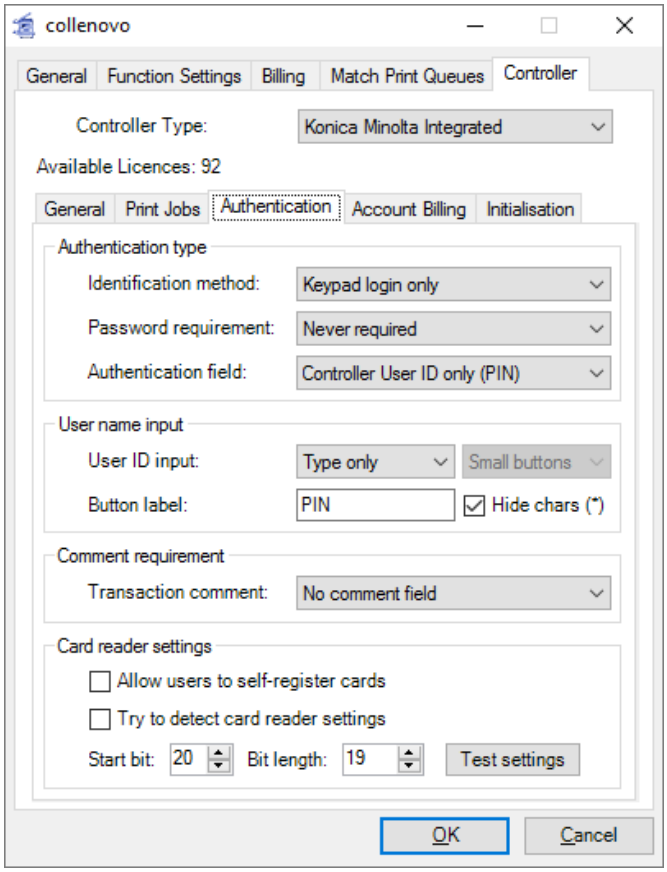
In the cases above, datastream tracking must be used.

### Track print jobs through print queues (datastream tracking)

These are the disadvantages to datastream tracking:

- There will be a 5% variance in the total pages printed compared to the meter reports (i.e. what was actually printed). This is because once the job has left the print server (or workstation in direct-to-ip printing) the software records the transaction. If the job is subsequently deleted at the MFP the transaction will not be removed.
- There will be a larger colour variance because the datastream interpretation detects a whole job as colour even if it has only one or two pages of colour.

## 2.2.3 Authentication Tab




### *2.2.3.1 Authentication type*

In the **Authentication type** frame, choose the method by which users will be authenticated (card swipe, keypad entry or both). Also, choose the password requirements from the **Password requirement** dropdown. Note that if users will be entering a PIN number, set the password requirement to **Never required**.

The **Authentication field** dropdown specifies which database field is used to match a user. By default this is the Controller User ID. This can be changed to the Login Name (AD Account) or both.

### 2.2.3.2 User name input

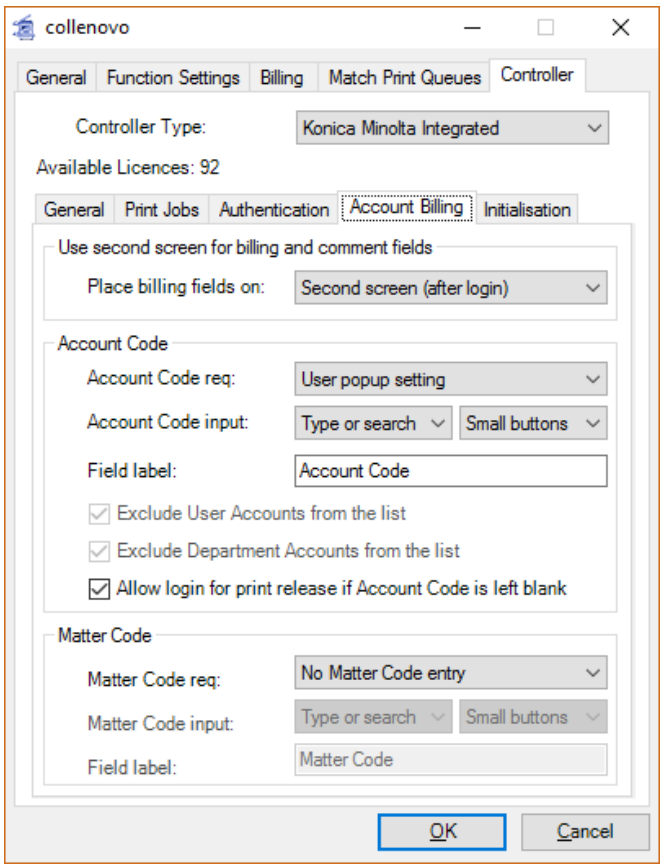
In the **User name input** frame one can specify how the touch-screen entry of the User Name can be accomplished. The User Name can be typed, selected or searched. One can also change the label on the User Name button and hide the characters of the User Name with asterisks, similar to a password field.

### 2.2.3.3 Comment requirement

An extra field can be added to the login screen of the MFP to allow the user to enter a comment. This comment will be recorded against any transactions made while logged in. The comments will be displayed in the reports and can be used when importing into legal accounting systems.

If a comment is entered in the printing popup on the user's workstation, the one entered in the popup will take preference.

## 2.2.4 Account Billing Tab




This tab is only relevant for sites using the PD Pro version of the software.

Print, copy, scan and fax transactions can be billed to third party accounts and Matters. On this tab the user specifies what billing fields are displayed on the front panel of the MFP.

#### 2.2.4.1 Use second screen for billing and comment fields

If this is selected, the account, matter and comment fields will not appear on the Login Screen which is the standard idle screen of the printer. They will appear on a screen that is displayed immediately after the user logs in.

The advantage of this is that if the billing fields' requirement is set to **User popup setting**, certain users may not see the second screen at all. If a user's popup setting is set to **No client popup** or **Popup invoice only** they will not be shown the second screen and they will be logged-in straight away. This leads to less confusion and quicker login for users who do not need to bill jobs to accounts.

If a printer is using card-swipe login, and the billing fields are on the initial screen, the user must remember to enter the billing information before they swipe their card. If the fields are on the second screen, the user can swipe first and then enter the billing information when the second screen is displayed.

Lastly, using the second screen allows the printer to filter out accounts that the user does not have access to when they search or list accounts. If it is on the initial screen, the software doesn't know who the user is when they search for accounts so the results will contain accounts to which they do not have access.

#### 2.2.4.2 Account Code

If the **Account Code requirement** is set to **No Account Code entry**, the field will not be displayed on the MFP front panel. Also, the Matter Code field will not be displayed. This means that all transactions will be billed either to the User's User Account or Department Account depending on the **auto-billing** setting for that particular user. It can be set to Account Code optional, in which case it will be displayed but can be left blank when logging in, and the auto-billing setting will apply. Also, it can be set to User popup setting so if the particular user's popup setting is **No client popup** or **Popup invoice only** they can leave the field blank.

In the **Account Code input method** one can specify how the touch-screen entry of the Account Code can be accomplished. The Account Code can be typed, selected or searched. One can also change the label on the Account Code button.

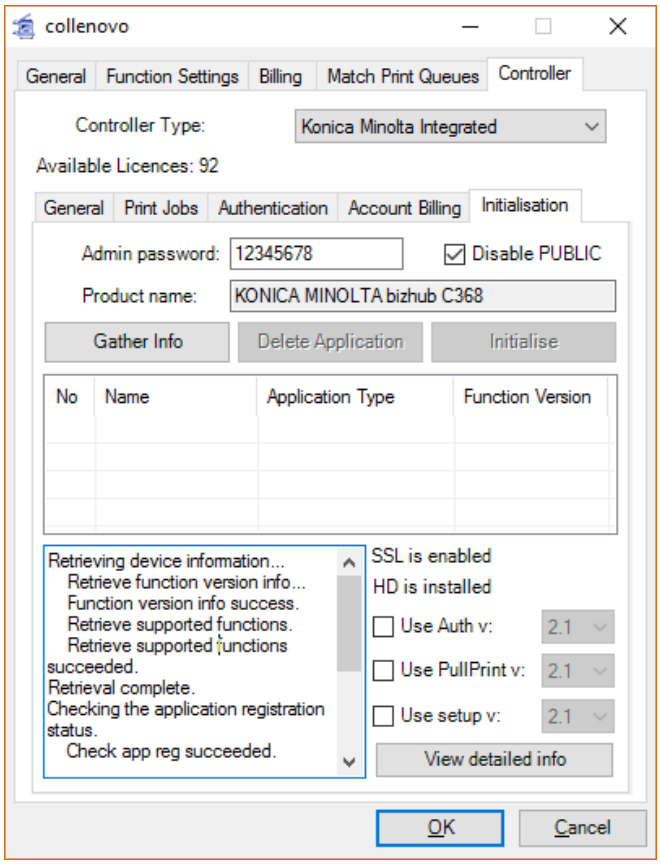
#### 2.2.4.3 Allow login for print release if Account Code is left blank

If the user has entered an Account Code in their printing popup, this will always take preference over what is entered when logging at the printer to release the job. So if a user is logging in simply to release their print jobs, they should not need to enter an Account Code. If this checkbox is ticked, it will allow the login with a blank Account Code, but only the Release Job function will be available. The user won't be able to make copies or fax or scan (if the fax and scan function is being tracked).

#### 2.2.4.4 Matter Code

Similarly to the Account Code requirement, the Matter Code field can either be not displayed, optional, required or User popup setting.

### 2.2.5 Initialisation Tab




Once all the settings have been specified, the integrated applications can be initialised. Note that if any of the settings are changed after initialisation has taken place, the applications must be deleted and re-initialised.

Ensure the correct **"Admin" user password** is entered. Click the **Gather Info** button to confirm connectivity to the MFP and to confirm that no integrated applications have already been installed. If any applications appear in the list, highlight any conflicting applications and click the **Delete Application** button. Click the **Initialise** button.

Inspect the output in the bottom textbox. This will show if any of the stages of initialisation failed. If there were any failures (e.g. because of a timeout), delete the applications and try again.

Now that the integrated applications have been initialised on the MFP, test the connectivity at the MFP panel. Don't forget to refresh the PDServer as the Shared Device has just been created (**PDServers** > right click server and choose **Refresh**).

If there are any connectivity problems, ensure that the PDServer service is running (and no firewalls are blocking port 50002) and that the integrated applications were initialised with the correct PDServer IP address.

## 2.3 Changing settings that require re-initialisation

If any of the settings on the Controller tab are changed *after* the integrated applications have been initialised, a delete and re-initialise may need to be performed. Any changes to the following settings will require a re-initialise:

- Primary or secondary PDServer IP address

- Server connection timeout
- Applications button label
- Authentication type
- User name input
- Account Code (all settings except **Exclude User Accounts…**)
- Matter Code (all settings)

To re-initialise:

- Double click the MFP in question under **Shared Devices** in Resource Manager.
- Click the **Controller** tab.
- Click the **Initialisation** tab.
- Ensure the correct password is entered in the **"Admin" password** textbox.
- Click **Gather Info**. After some communication with the MFP, two entries will appear in the application list.
- Highlight both these applications and click **Delete Application**.
- Once the process of deleting is complete, click **Initialise**.

# 3 Configure the MFP and print drivers for datastream print tracking

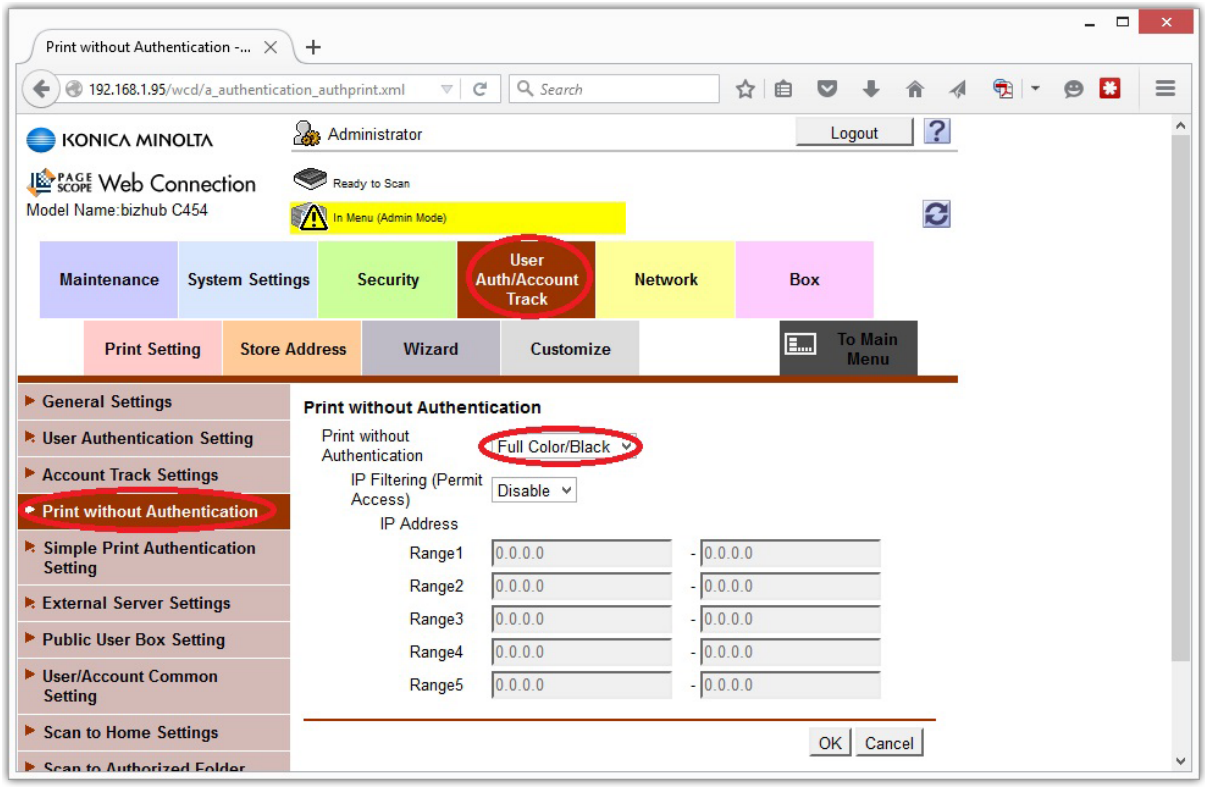
For datastream print tracking to take place, all authentication for printing must be disabled on the MFP and on the printer driver. Sometimes initialising (or re-initialising) an Authentication application on the MFP causes **Print without Authentication** to become restricted even though it has been allowed previously.

Note that this is only necessary if you are using Datastream tracking (perhaps because of a Fiery controller).

## 3.1 Allow print without Authentication

NB: not necessary under Enhanced Server tracking.

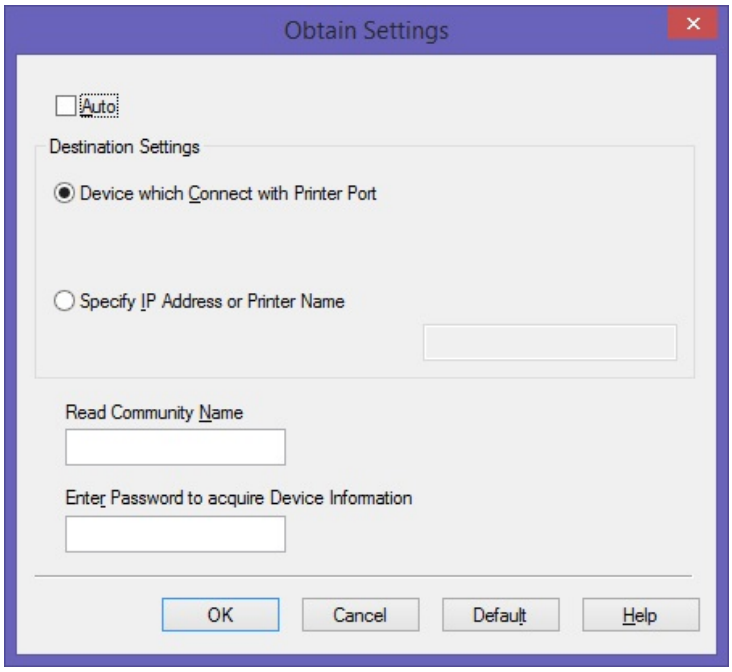
Login to the Administrator settings of the MFPs web interface (see above for steps). Click the User Auth/Account Track menu. Click Print without Authentication. Change drop down to Full Color/Black and click OK.



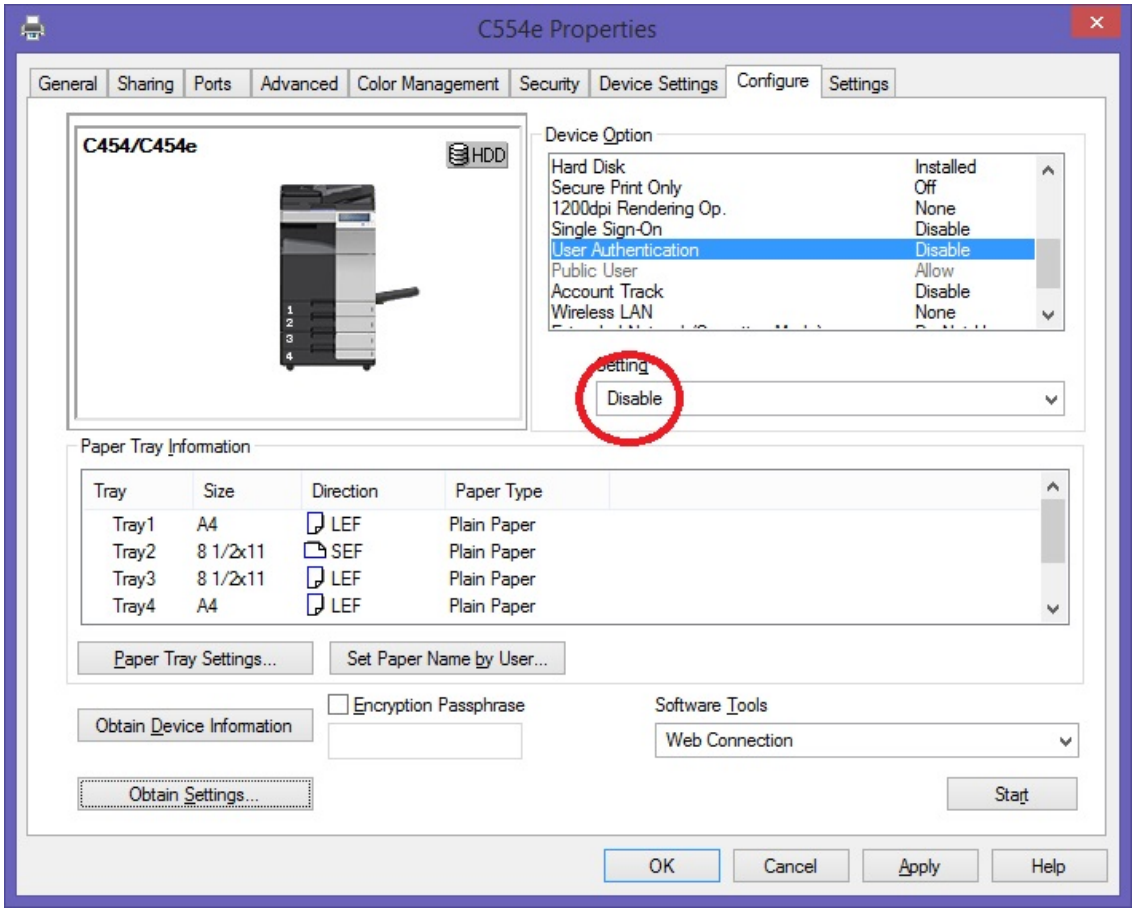

## 3.2 Disable User Authentication on the printer driver

NB: not necessary under Enhanced Server tracking.

On the print server, open **Printers and Faxes**, right click the printer and choose **Properties**. Click the **Configure** tab. Click the **Obtain Settings…** button (bottom left) and untick the **Auto** checkbox and click **OK**.



In the **Device Option** frame, scroll down to **User Authentication,** set it to **Disable**.




# 4 Troubleshooting

## 4.1 Timeout occurs when initialising integrated applications

- Ensure that SSL has been enabled on the MFP and the OpenAPI and TCP Socket Settings have been correctly configured on the MFP.
- Ensure that an exception exists in any firewall software for Resource Manager. See Create a firewall exception for Resource Manager.
- Ensure that the Shared Device has the correct IP address configured:
    - Open Resource Manager.
    - Click **Device Management** > **Shared Devices**.
    - Double click the device in the right hand pane.
    - On the **General Settings** tab ensure the correct IP address appears in the **Host or IP** text box. Click the **Ping** button to confirm network connectivity.
    - Open web browser and browse to the IP address to confirm that it is the correct device.

## 4.2 Panel displays Connecting to Server continuously until timeout

- Ensure that the PDServer service is running on the server.
- Ensure that TCP port 50002 is not blocked by a firewall on the server.

- Ensure that TCP port 50002 is not being used by another process:
    - Open a Command Prompt.
    - Type **netstat -a -o** and hit enter.
    - In the list of open ports, look for TCP port **50002**. Note the PID in the **PID** column.
    - Open the Task Manager.
    - Click the **Processes** tab.
    - Ensure the PID column is displayed. If not, click **View** > **Select Columns** and tick the **PID (Process Identifier)** checkbox.
    - Look for the PID noted in the *netstat* list and ensure it is PDServerService.exe. If it is another application, either this application must be terminated (and PDServer restarted) or the port that PDServer listens on must be changed. To change the port that PDServer uses to listen for OpenAPI communication, follow these steps:
        - Open Resource Manager.
        - In the menu bar click **Tools** > **System Configuration**.
        - Click the **Networking** tab.
        - Enter the new port number in the **PD Server – KM Integrated port** textbox.
        - Refresh the PDServer.
        - All MFPs that have KM Integrated applications registered will have to be re-initialised. See Changing settings that require re-initialisation.
- Ensure that the integrated applications were initialised with the correct PDServer IP address and that the PDServer's IP address has not changed since initialisation. See Changing settings that require re-initialisation.

## 4.3 Print jobs appear in the job list on the panel, but are deleted

If a print job arrives at the printer but is not printed, check the Job History list to see what caused the problem:

- Touch the **Job List** button in the top left of the panel.
- Touch the **Job Details** button in the bottom left.
- Touch the **Job History** button.
- If there are any jobs in this list that have a status of **Deleted due to error**, highlight the job and touch **Detail**.
- If it says Login Error in the Detail screen, it means that the print job couldn't be authenticated on the PDServer. Under Enhanced Server tracking, it may be that this job is not going through the server (i.e. direct to IP printing). Or under Datastream tracking, Print without authentication may be restricted – see Configure the MFP and print drivers for datastream print tracking