XPR Enterprise for Pcounter

Konica Minolta Embedded

Configuration Guide

AIT Ltd
2 Hawthorn Park
Coal Road
Leeds LS14 1PQ
UK

T: 0113 2730300
F: 0113 2730302
E: info@ait.co.uk
W: www.ait.co.uk

Table of Contents

Requirements

The Microsoft .NET Framework version 3.5 SP1 needs to be installed on the target machine.

An active (client) licence is needed by each device. The number of licences allowed is determined when you purchase your support licence for the product. During the 30 day evaluation period you may licence up to 500 devices.

The product should be installed on the same server as the Pcounter administration software; in a Windows environment this will be the Pcounter data server. The server must have a valid Pcounter Pro licence.

Please ensure that all the devices are configured correctly and are running the required firmware to support OpenAPI version 2.3.x connections. Refer to the 'readme file' for information on how to configure the devices for OpenAPI.

Installation/Uninstallation

Installation of this software will provide a 30 day evaluation period.

To install, open the installation MSI file – **XPR Enterprise Konica Minolta Embedded x.x.x.x.msi** and follow the wizard.

To uninstall, go to the **Windows Start** menu and select **All Programs** then **XPR Enterprise, XPR Enterprise Konica Minolta Embedded** and finally **XPR Enterprise Konica Minolta Embedded- Uninstall.** This will take you through the removal process.

Opening XPR Enterprise Konica Minolta Embedded

From the **Windows Start** menu, select **All Programs** then **XPR Enterprise, XPR Enterprise Konica Minolta Embedded** and finally **XPR Enterprise Konica Minolta Embedded - Configuration.** Alternatively click the **XPR Enterprise Konica Minolta Embedded - Configuration** shortcut on your Windows Desktop.

Overview

XPR Enterprise Konica Minolta Embedded enables embedded devices to charge for services such as printing, photocopying and scanning against a user's Pcounter account. It supports both Pcounter for Windows and Pcounter for Netware.

Home

Once the application is running the home page will be displayed. This page shows the applications product information.

Figure 1

Navigation

Use the options in the navigation menu on the right of the application to configure XPR Enterprise Konica Minolta Embedded.

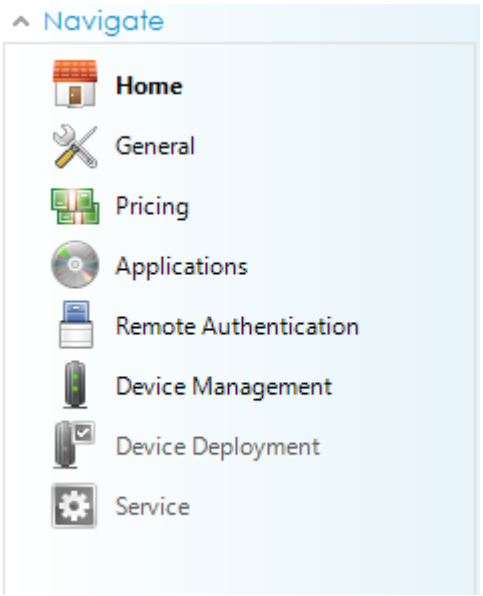

Figure 2

General

General settings are system wide and apply to every device configured to run the OpenAPI applications.

Configuring Pcounter

XPR Enterprise Konica Minolta Embedded supports both Pcounter for Windows and Pcounter for Netware. To configure Pcounter, select the appropriate operating system and press the configure button.

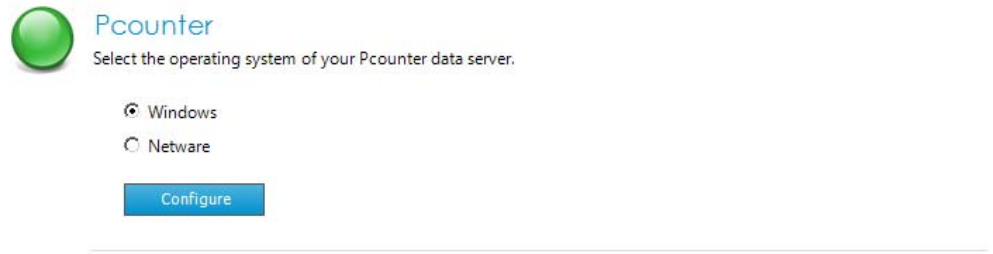

Figure 3

Charge Groups

During the authentication process the user may be prompted to enter a charge group (Client Code) to be associated with their transaction. This selection of charge groups can be switched off by selecting *None.* Alternatively the user may be prompted to enter a charge group associated to them or a charge group from the complete list by selecting *User or All* charge groups.

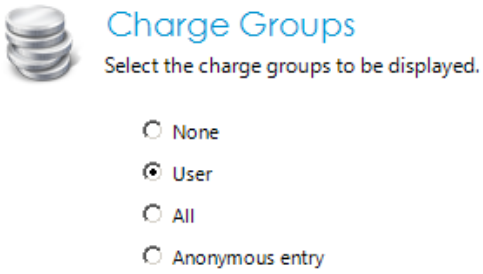

Figure 4

Charge Group Alias

An alias may be set for charge groups. This alias will need to be entered prior to deploying to any devices. This alias will then be displayed on the device during use.

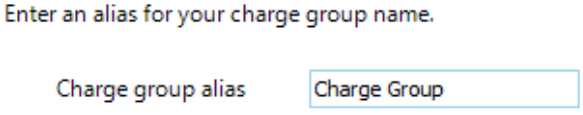

Figure 5

Charge Group Entry

If charge groups have been selected, it is possible to force a user to enter a charge group during the authentication process. If the require charge group checkbox is not selected then a user can bypass entering a group to be associated with the transaction.

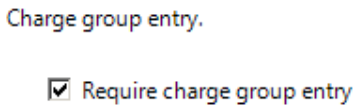

Figure 6

Charge Group Display

The charge group display option will determine what is displayed in the charge group list.

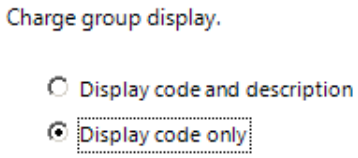

Figure 7

Charge Sub Groups

Charge Sub Groups may also be selected during the authentication process. The user may be prompted to enter a charge sub group(Sub Code) to be associated with their transaction, providing the selected charge group has one or more associated charge sub groups. This selection of charge sub groups can be switched off by un-checking the **Use sub groups** checkbox. If charge sub groups exist for a charge group and this setting is disabled, any sub groups will be ignored.

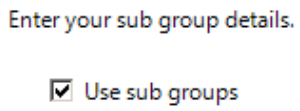

Figure 8

Charge Sub Group Alias

As with charge groups an alias can also be set for charge sub groups. This will also need to be set prior to deploying to any devices and will be displayed during use.

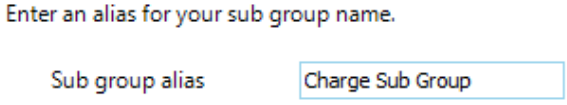

Figure 9

Charge Sub Group Entry

This setting will force a user to enter a charge sub group, providing their selected charge group has some associated sub groups.

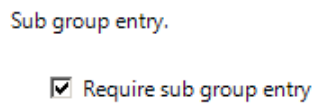

Figure 10

Charge Sub Group Display

The charge sub group display option will determine what is displayed in the charge sub group list.

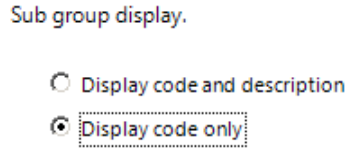

Figure 11

Device Administration

Set the device administration password and the OpenAPI logging level before deploying the OpenAPI applications. The password you set must be the same as the administrator password on the device. It is recommended that same password is used for all devices, otherwise you will need to change the password here before you deploy to each device, which could be a lengthy process if you have a large number of devices.

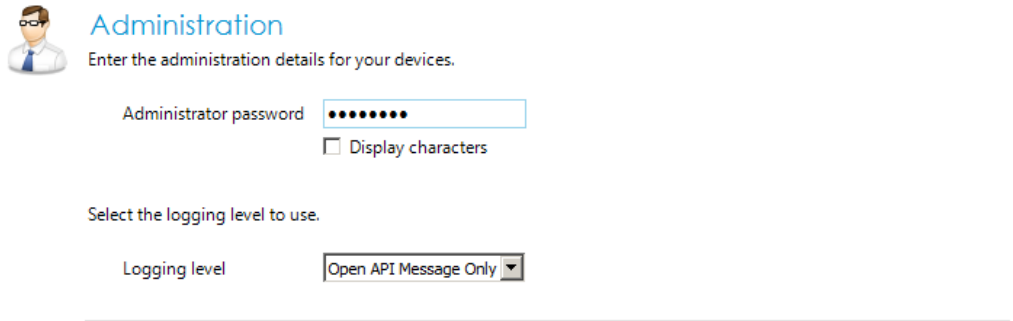

Figure 12

Functionality

Each device has native application functionality for copy, print, scan etc. This functionality can be switched on or off. These settings are system wide and will apply to all devices.

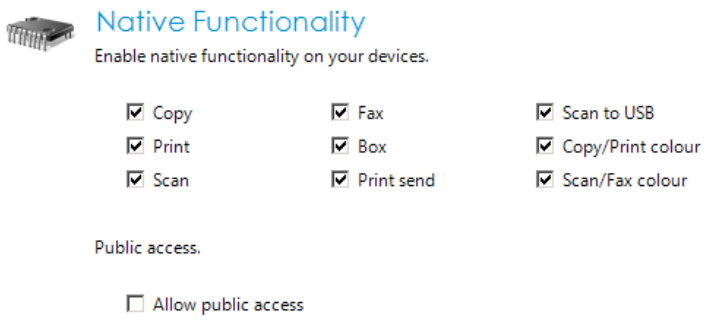

Figure 13

Cluster Settings

XPR Enterprise Konica Minolta Embedded has full support for Microsoft clustering. To enable cluster support, the application will need to be installed on to both nodes. The node that sets cluster support will be nominated as the master. All settings should be made on this node. On the slave node run the service configuration and set cluster support on. This node will just read its configuration set from the master.
Ensure that both nodes have the correct path to the central shared location.

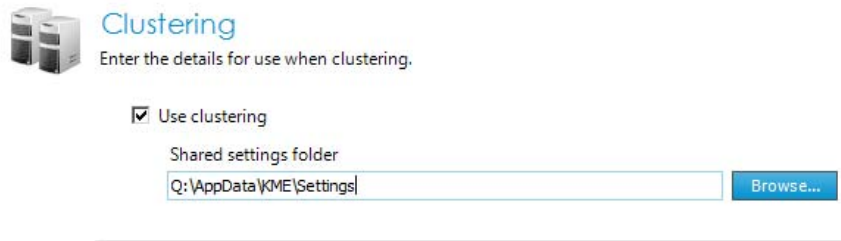

Figure 14

Host IP Address

If the server hosting XPR Enterprise Konica Minolta Embedded has more than one network card installed, the address bound to one of the cards can be selected as the host address for communication. If only one card is installed this will default to the address bound to that card and it will not be editable.

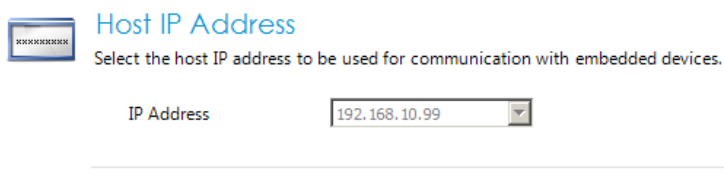

Figure 15

Pricing

A funding limit, currency and pricing for each document type can be set for all the varying copy, scan and fax options available.

Session Funding Limit

If a session funding limit is applied, this value will override a user's balance and associated credit limits during a user session on a device. This is a global setting and will affect all users on all devices once set.

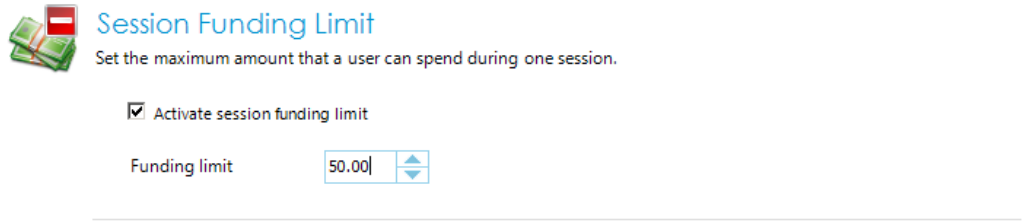

Figure 16

Currency

The currency is used for display purposes and is shown on the Konica Minolta device against the users balance.

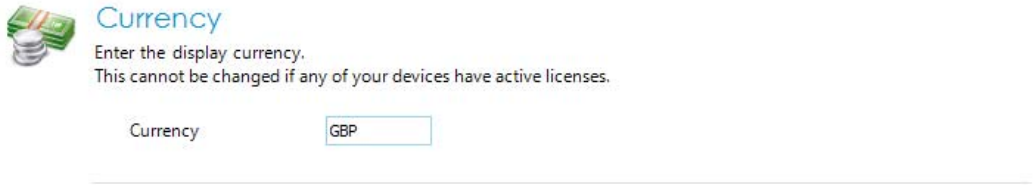

Figure 17

Copy Pricing

Pcounter copy pricing is applied to the device but it is only divided into 4 different paper sizes. This is a limitation of the Konica Minolta OpenAPI.
The sizes are:

- Up to A5
- A5 – A4
- A4 – A3
- A3 and above

The price will be taken for the paper size within the ranges shown above.

Some Konica Minolta devices are capable of applying a finishing method to the copy job. This can also be charged for if used.

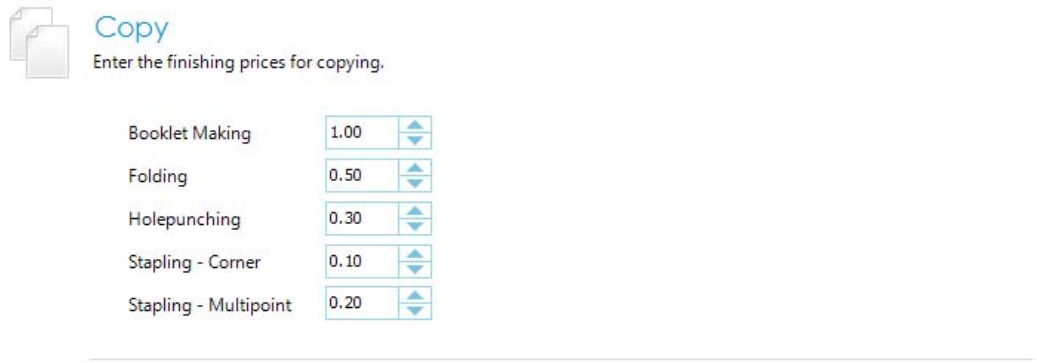

Figure 18

Scan Pricing

Scan pricing can be accounted for as Network Fax, Pull Scan and Push Scan. The Scan to Email and Scan to User Folder applications use the Push Scan method, However if you are using the native scan functions these can also be accounted for as Network Fax or Pull Scans depending on the native scan function selected.

Colour scanning can also be charged for by using the multiplier on the base scan price.

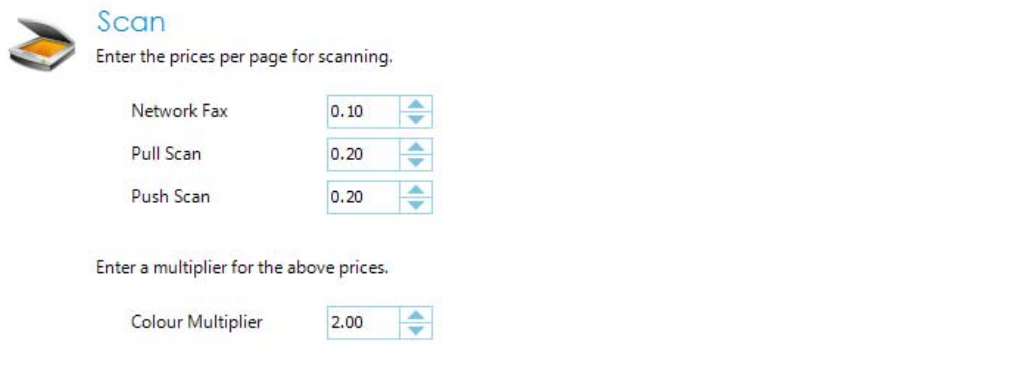

Figure 19

Fax Pricing

The Konica Minolta devices support 4 different resolutions of fax documents. These can all be priced individually with a connection and a communication duration charge applied. There are also two fax lines available, that can be used to allow a different connection and communication charge.

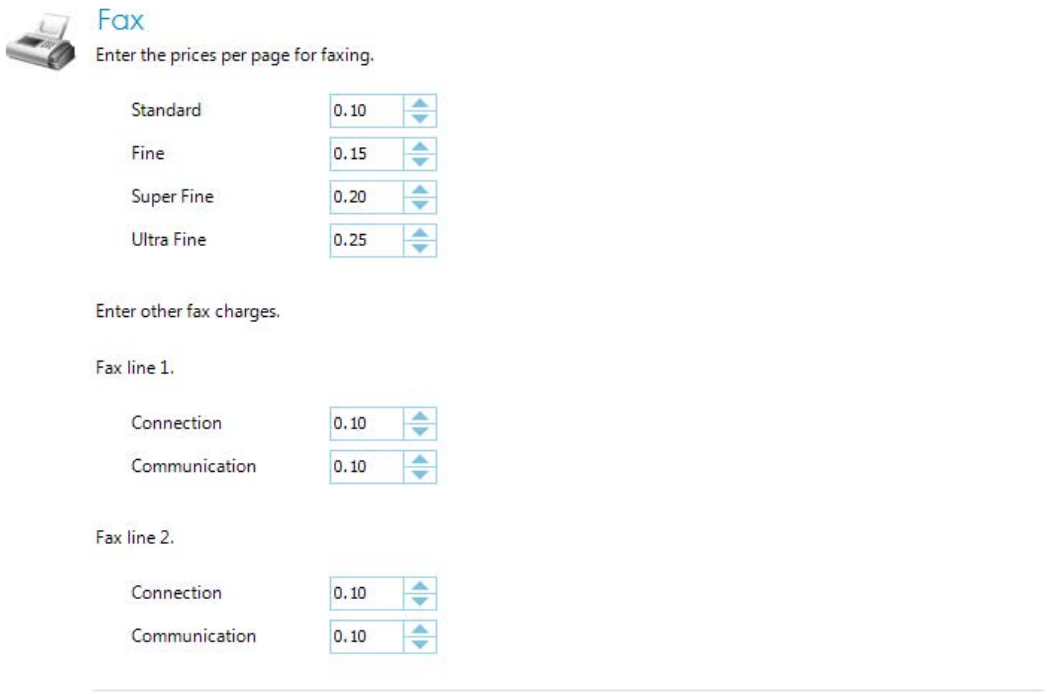

Figure 20

Applications

It is best to use the default values for port and timeout settings unless the ports are already in use. Ports and timeout settings are applied to each of the applications to be installed.

Authentication

The communication settings for Authentication are shown below.
If the Authentication application port number is changed this must be reflected on the device. Authentication uses SSL so please refer to the device documentation on how to enable the device for OpenAPI, how to create the SSL certificate.

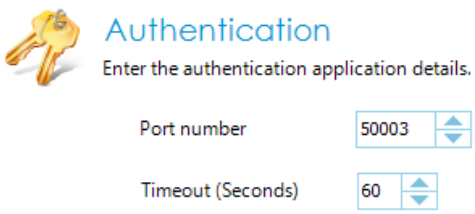

Figure 21

User Login settings and port numbers cannot be changed by simply stopping the service. These settings will only be modifiable if none of your devices have active licences. To alter these settings, the applications and licences must be de-registered from **all** devices and then re-registered with the new settings applied.

Authentication Type

The user login method needs to be specified when the applications are deployed. This login method will be used on each selected device.
Authentication can take place directly on the Konica Minolta device by keying either your network username and password or your user ID and PIN number. Alternatively a user can also authenticate via a network authentication device.

Username and Password Authentication

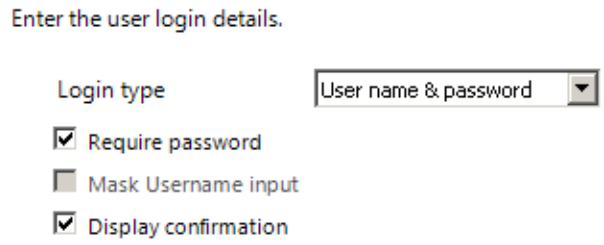

Figure 22

User ID and PIN Authentication

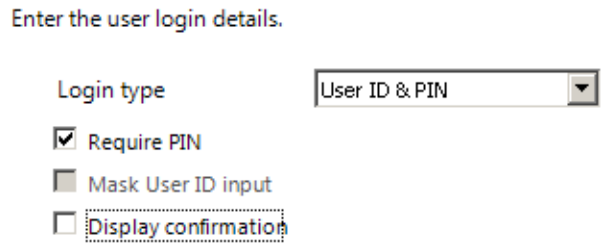

Figure 23

If the second credential (Password or PIN) is not required, an option to mask the input of the first credential can be selected. This will mask the users input with asterisks when entering either their Username or User ID.

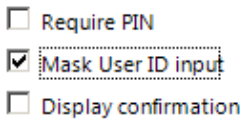

Figure 24

Self-Registration

Enabling the Self-Registration option will allow users to assign a card to their Pcounter account. This option is only available if the system is using IP or USB card readers for authentication. If this option is enabled and a user presents an unknown card to the reader, the user will be prompted to assign the unknown card to their account.

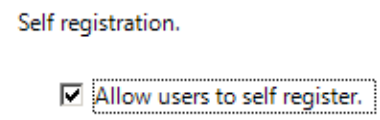

Figure 25

Print

The communication settings for Print are shown below. The port number should only be changed if it is already in use. All print communication can be secured by enabling SSL for print. This must be selected at deployment.

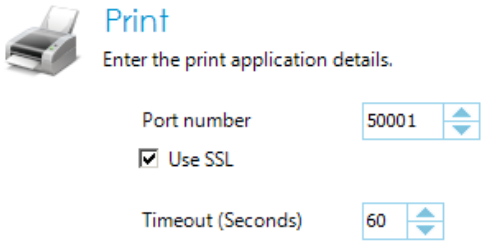

Figure 26

Quick Print

Quick print is a feature allowing print job release as soon as the user has authenticated on the Konica Minolta device. There is an option to allow for unlimited balance users only or all users.
If this is enabled for all users the users balance has insufficient funds to release all print jobs, only what they can afford will be released and the additional print jobs will remain in the queue.

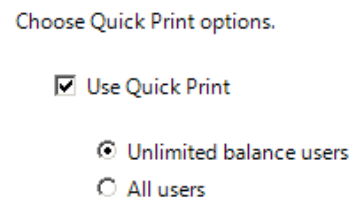

Figure 27

Apply Selected Groups for Print

Charge group and sub group selection can be done during print job submission via the popup dialogue; however charge group and sub group selection during the authentication process on device can now be assigned to print jobs by selecting this option.

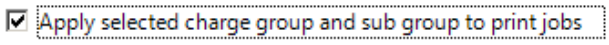

Figure 28

Scan

The communication settings for Scan are shown below. The port number should only be changed if it is already in use. All scan communication can be secured by enabling SSL for scan. This must be selected at deployment.

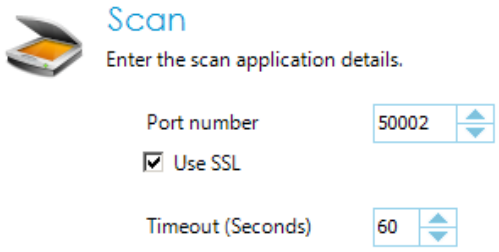

Figure 29

Scan job logging

Scan job logging can be enabled by selecting the option shown below. If selected, the logs will show the user, scan job, destination, date/time and device the job was processed on.

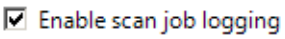

Figure 30

Scanning Options

Scanning options allows scan job resolution, colour types and document formats to be enabled or disabled on the Konica Minolta device. These are global settings and will be reflected on every device running XPR Enterprise Konica Minolta Embedded.

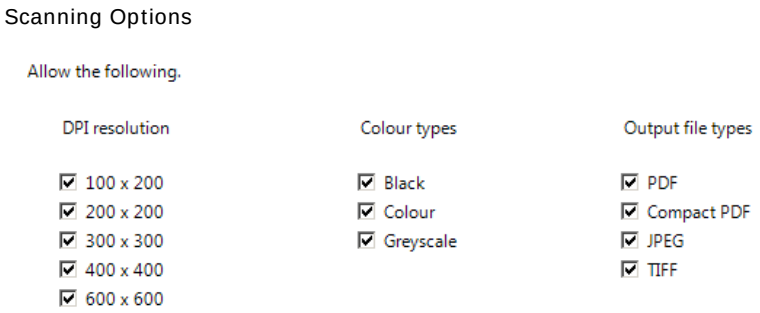

Figure 31

N.B.
All the above settings affect all scanning on the Konica Minolta device, however only the PDF file format is a supported document type for both the XPR Enterprise Konica Minolta Embedded Scan to Email and Scan to Folder applications.

FTP Settings

FTP is the method used to transfer scan jobs from the Konica Minolta device to the file system. It is therefore essential to ensure that these settings are correct as they are sent to the Konica Minolta device during installation.

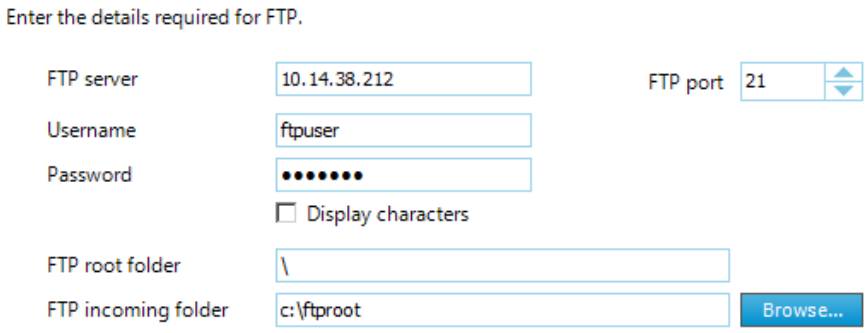

Figure 32

Active Directory Settings

If the scan applications are using Active Directory to obtain user settings, the following information must be provided to allow the login user to obtain this information. The user must have sufficient rights to read the directory information.

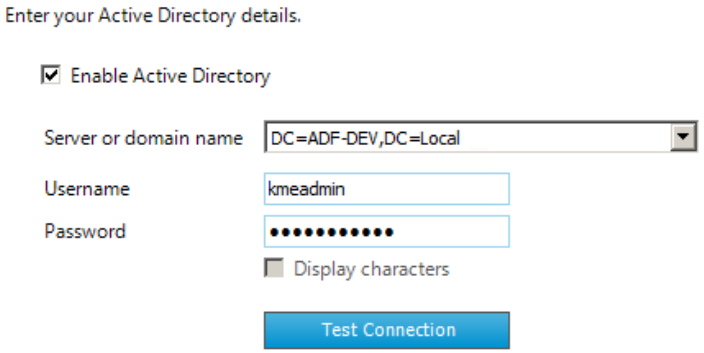

Figure 33

Scan to Email Settings

Scan to Email can either obtain the users email address from their active directory account, or derive the email address.
If the email address is derived, the **Email Domain Name** value is used. It takes the currently logged on username and will prepend it to specified value, for example:

user1 + @ + yourdomain.com = user1@yourdomain.com

SMTP Server and login details need to be correctly specified. If the SMTP server requires authentication, select the **Use SMTP Authentication** box and input the correct password for the sender account.

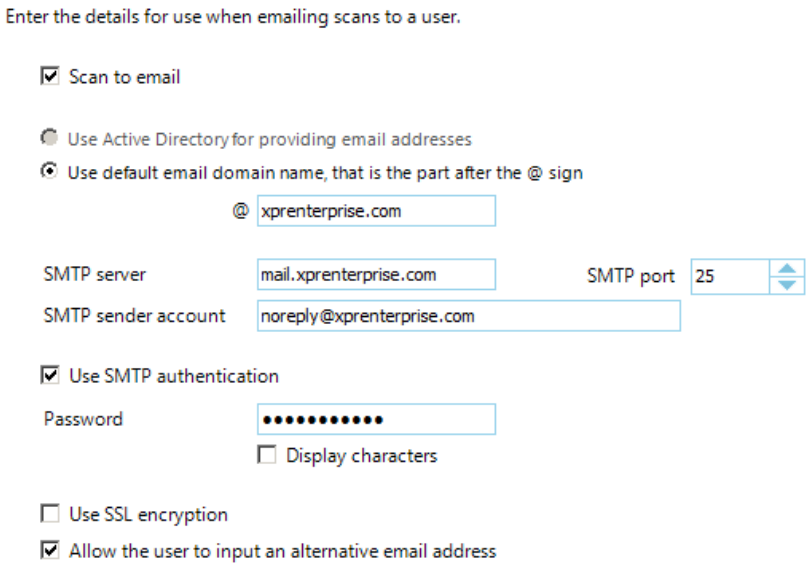

Figure 34

If the box is selected to Allow Alternate Email Address, the user has the ability within the application to input a different email address for sending the scanned document to.

Scan to User Folder Settings

Scan to Folder can either obtain the users home folder from their active directory account, or derive the folder path.
If the folder is derived, the **User Root Folder** value is used. It takes the currently logged on username and appends it to specified value, for example:

UserRootFolder + \ + user1 +\

It is also possible to specify a sub folder within the user's home folder.
This can be obtained from a field within their active directory account or set directly as the user sub folder name. If the sub folder is used, it will be appended to the path regardless of how the user's home folder was derived.

Scan to User Folder Settings (Derived from Active Directory)

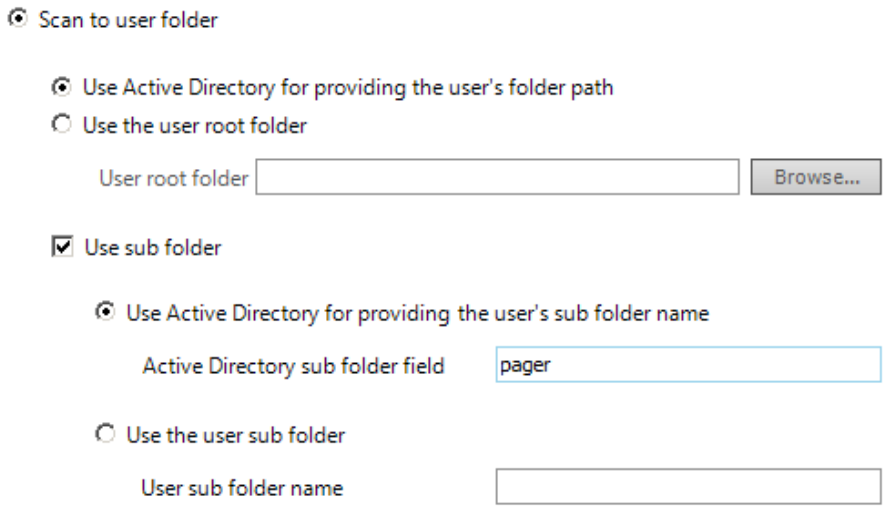

Figure 35

Scan to User Folder Settings (Derived from User Root Folder)

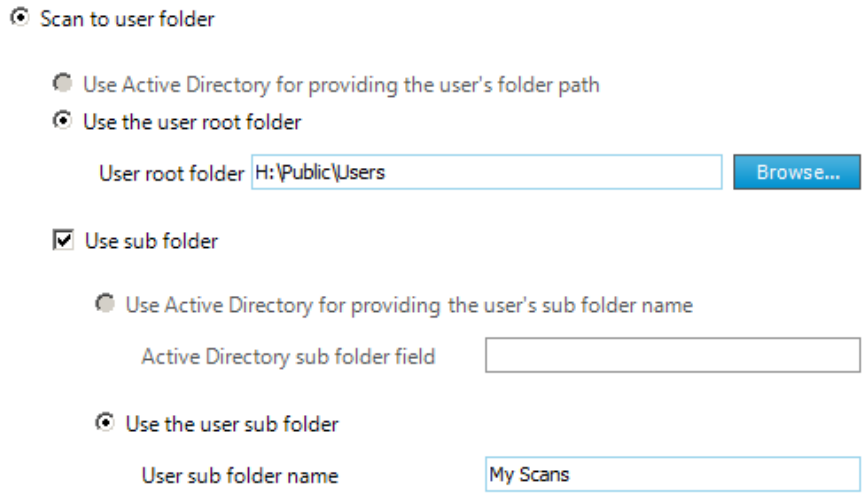

Figure 36

Scan to Group Folder Settings

Scan to Group Folder requires a root folder to be specified. All scan jobs can be processed into this folder. Alternatively a sub folder can be used by looking up the folder name from a field value held in active directory against the logged in user.

This would be appended to the group root folder, for example:

ScanGroupFolder + \ + ActiveDirectoryFieldValue +\

Scan to Group Folder Settings

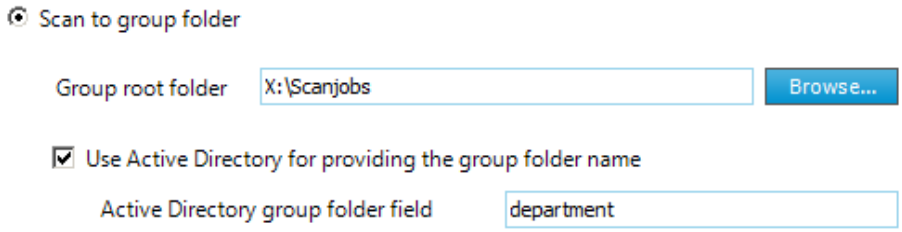

Figure 37

Remote Authentication

Remote device authentication provides the ability for users to logon to a device by either presenting their card to an attached card reader or presenting their finger to an attached biometric scanner. None of these options should be enabled if the system is not using any remote authentication devices.

IP Card Reader Authentication

If IP card readers are being used to authenticate users the **Enable IP card readers** needs to be selected. This will ensure the server listens for IP card reader remote connections on the specified port. If this option is not selected, an IP card reader cannot be assigned to a device.

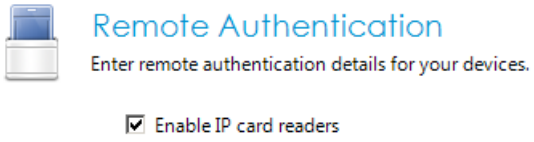

Figure 38

IP Biometric Authentication

If biometric scanners are being used to authenticate users the **Enable IP biometric devices** needs to be selected. The biometric device server address must be specified. This will ensure the server listens for IP biometric remote connections on the specified port. If this option is not selected, an IP biometric scanner cannot be assigned to a device.

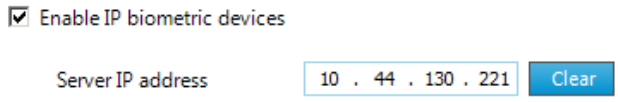

Figure 39

IP Device Communication

All IP authentication devices need to use the same port shown below. This needs to be reflected on the XPR Enterprise Biometric Server if the system is using biometric authentication and the IP card readers also need to use this port for communication.

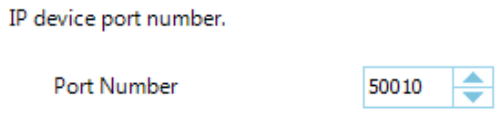

Figure 40

USB Card Reader Authentication

If USB card readers are being used to authenticate users the 'Enable USB card readers' needs to be selected. The output settings for the device must also be specified. These settings will need to be determined based on the card number assigned to the users account.

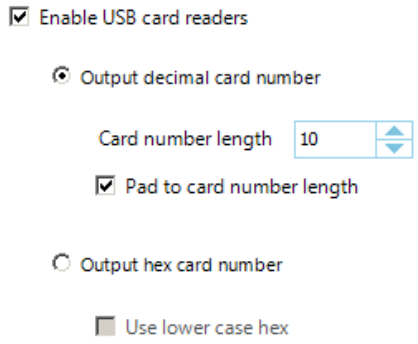

Figure 41

Konica Minolta USB Card Readers

If Konica Minolta USB readers are in use on any devices, the following information must be supplied for reading the output for authentication.

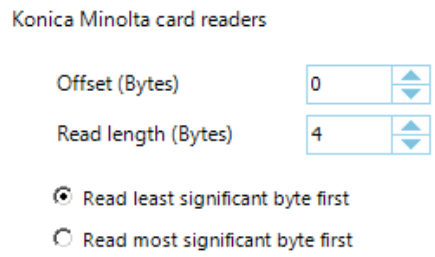

Figure 42

YSoft USB Card Readers

If YSoft USB readers are in use on any devices, the following information must be supplied for reading the output for authentication.

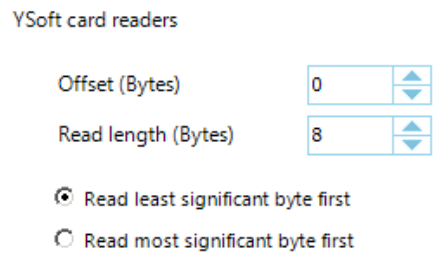

Figure 43

Card Reader PIN Entry

If the **Require PIN** option is selected, all users will be prompted to enter their PIN number on the device after they have presented their card to the attached card reader. This option applies to IP and USB card readers.

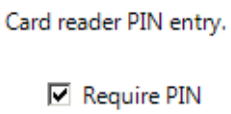

Figure 44

N.B.
If this option is selected and self-registration is active, the user will also be required to select a PIN number during the self-registration process.

Device Management

XPR Enterprise Konica Minolta Embedded must be deployed to each device but before that can be done; the communication and deployment settings must be specified.

Manage Search Protocol

Click **Search Protocol** from the Manage menu option to select and manage the device search. The Search Protocol specifies the method used to locate devices across your network.

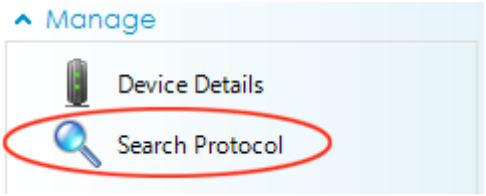

Figure 45

Search Types

There are three supported methods for device searching.
UPnP (Universal Plug and Play), SNMP Ping and SNMP Broadcast. The SNMP methods support both version 1 and version 3.

UPnP Searching

This is probably the most reliable search and requires no configuration but will only search across the subnet from where the search is instigated.

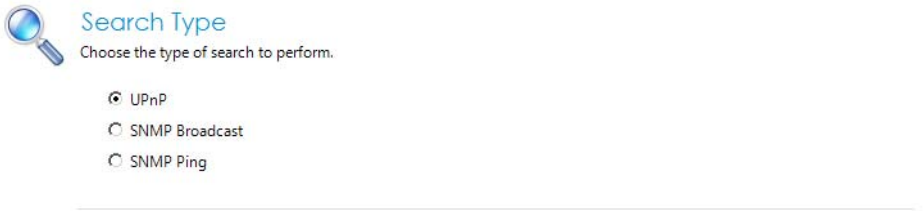

Figure 46

SNMP Ping Searching

SNMP Ping is a more powerful search allowing the IP search range to be specified. However, this method is non-specific i.e. it will return embedded device addresses and the addresses of other, non-embedded devices, so care must be taken when selecting devices for deployment.

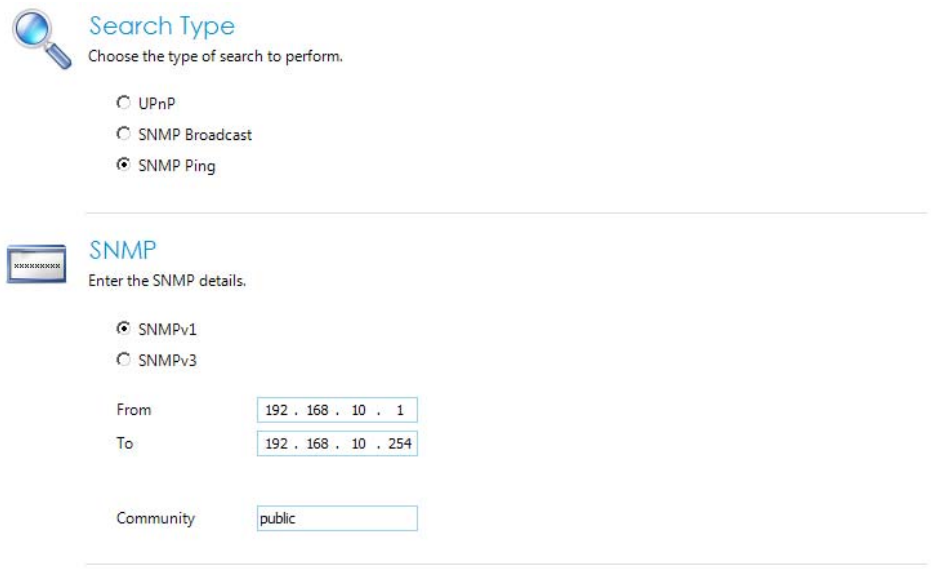

Figure 47

SNMP Broadcast Searching

SNMP Broadcast allows for the searching of subnets for devices by specifying the broadcast address. This, like SNMP Ping, may return non-embedded device addresses.

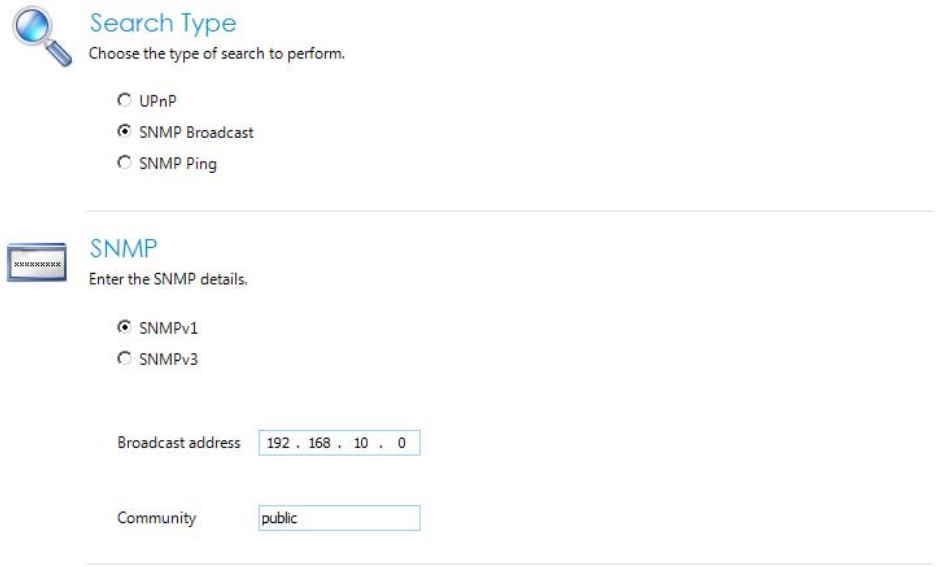

Figure 48

N.B.
As mentioned previously, both SNMP methods support V3; please refer to SNMP documentation and ensure that the specified user has context rights etc.

Device Searching

Device searching is necessary to locate the devices across your network. Once the devices have been found, they can be selected to receive and run the embedded applications. Select **Search for Devices** from the Actions menu. This will invoke a network search for devices based on the search method selected earlier.

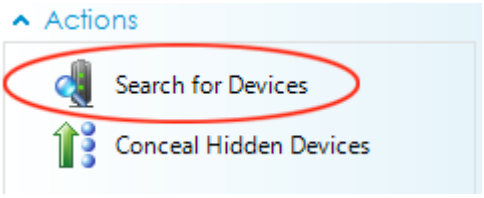

Figure 49

Search Completed

Once the search has completed, any devices found will be displayed in the grid as shown below. The address of the device and the model are returned from the search. A description can also be entered to identify the device location.

Devices Found

Figure 50

Device Details

Select 'Device Details' from the Manage menu option to set device specific settings prior to deployment of the application.

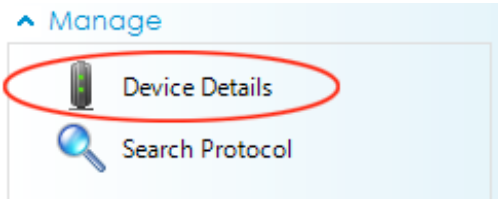

Figure 51

Identity

A description can be given to a device and the model details returned from the device search can also be edited/updated. These details will appear against the device in the device management and deployment grids.

Figure 52

Device Print Queue

Once a print queue has been associated with a device it will be displayed in the device management grid.

Figure 53

Manage Device Print Queue Association

Pcounter **Device Type**, **Configuration Profile** and **Pull Queues** can also be selected for each device's queue configuration.

Click the **Add Association** button and navigate to find the print queue.

Pcounter Device Configuration

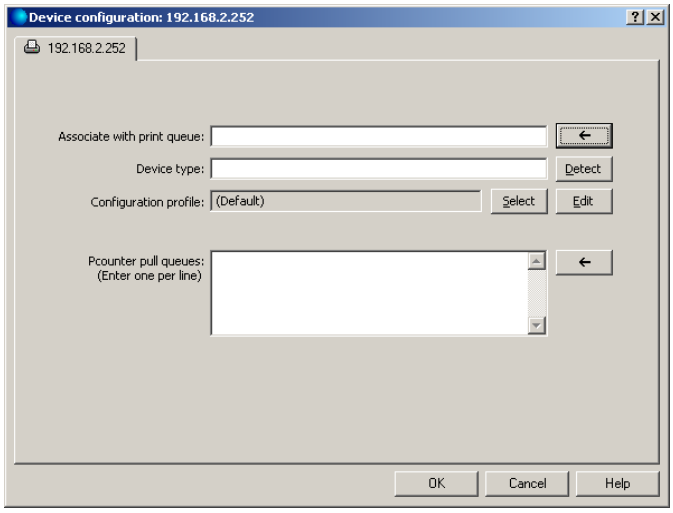

Figure 54

Print queue associations can be removed or edited by clicking the Edit Association or Delete Association buttons.

Remote Authentication Device

If remote authentication devices are being used, select the correct device type. IP card readers and biometric scanners will need their IP address entering.

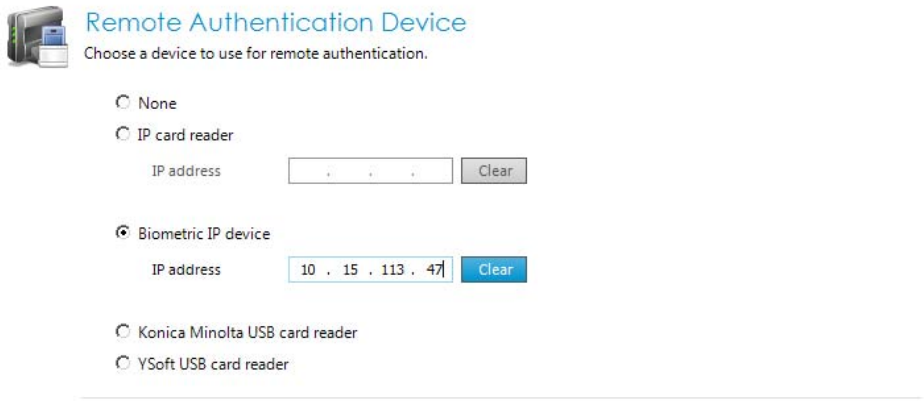

Figure 55

Application Deployment Settings

These settings allow the default application to be specified and the function version level for each of the applications. The device licence can also be enabled/disabled here.

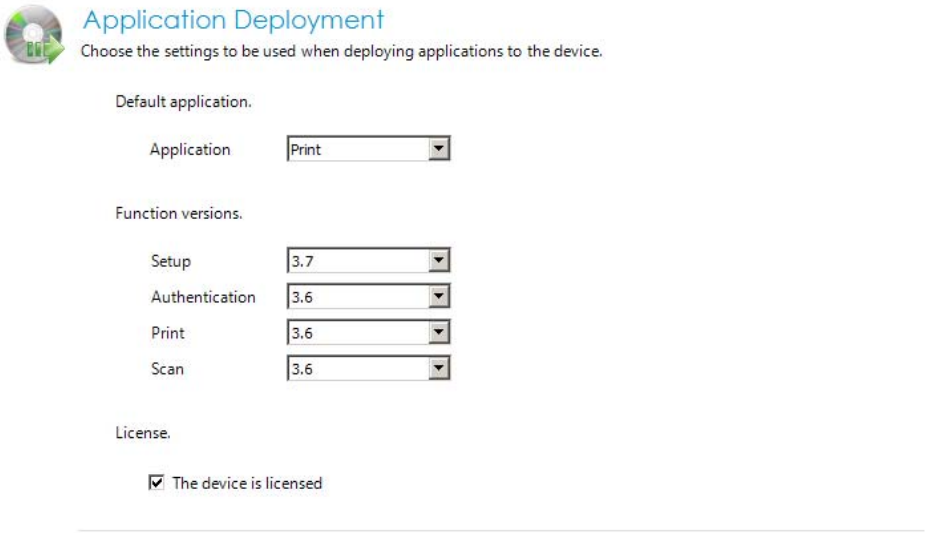

Figure 56

The default application is the application that is active as soon as the user has successfully authenticated on the device. This feature is not available on all devices by default. Please refer to the Konica Minolta device documentation for the MyPanel device requirements.

Device Deletion

Deleting a device will completely remove a device from the application and will return the device licence to the number of available licences.

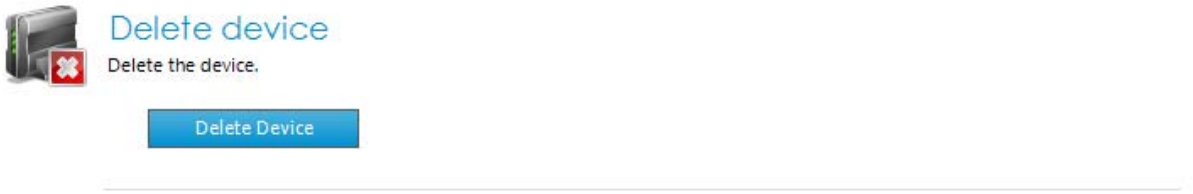

Figure 57

Next/Previous Device

From the device details page each device that is licenced can be configured by using the Previous and Next menu items from the Navigate Devices section.

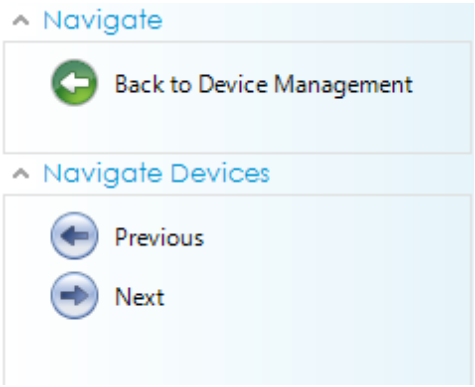

Figure 58

Hiding/Showing Devices

If there are any devices displayed in the grid that do not need to be displayed they can be hidden by checking the Hidden checkbox in the grid. The hidden checkbox can only be selected when the device isn't licenced.

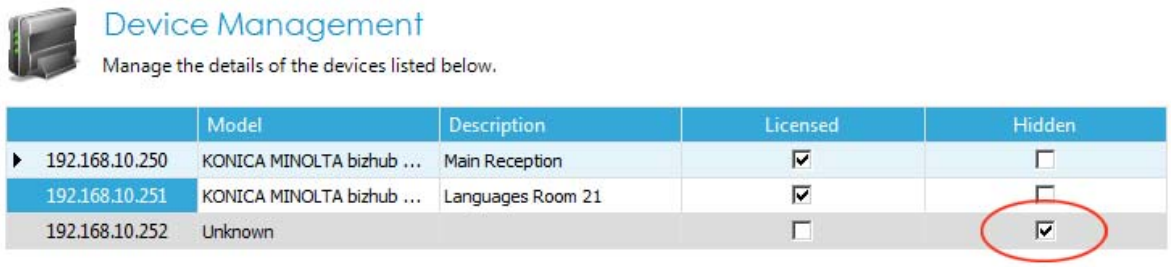

Figure 58

Any devices that are flagged as hidden in the grid can be removed from view by selecting the 'Conceal Hidden Devices' option from the Actions menu. This menu option will toggle if selected and hidden devices can be returned to view by selecting the 'Display hidden Devices' option.

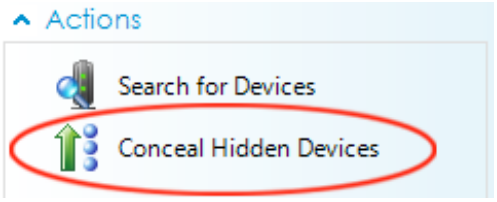

Figure 59

Device Deployment

Checking the **Authentication Registered** checkbox will check all of the other checkboxes for that device. These will also be highlighted in yellow indicating that the request is pending.
Authentication is mandatory as this is the application that forces user login. The Print and Scan applications are optional.

Device Deployment Pending

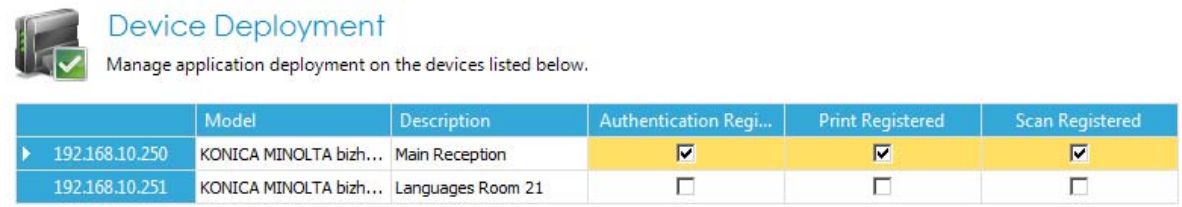

Figure 60

Select the 'Apply Changes' option from the Actions menu to deploy the selected applications to the selected device.

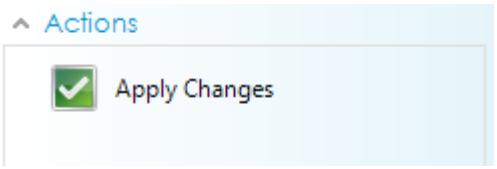

Figure 61

Request Successful

After a deployment request has been submitted, the application will attempt to deploy to each device based on the settings you specified.
When this task is complete, the grid should display your changes highlighted in green. This indicates that the request was successful. The boxes will always show the device status (Checked = Active, Unchecked = Inactive).
Click the IP address in the grid to see a list of deployment events.

Device Deployment Successful

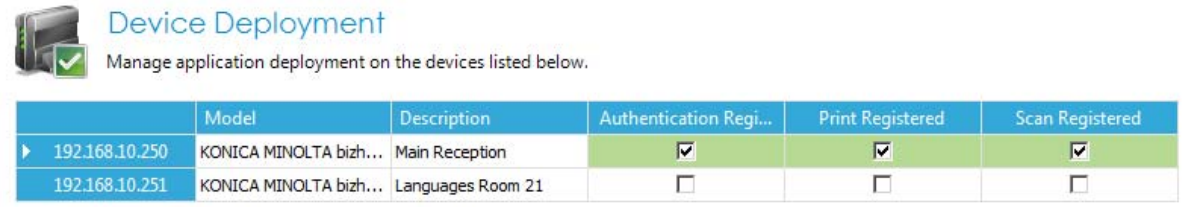

Figure 62

Request Failed

There are many reasons why an application may fail to register on a device. Such failures are shown by highlighting the individual requests in red.
Click the IP address in the grid to see a list of deployment events.

Device Deployment Failed

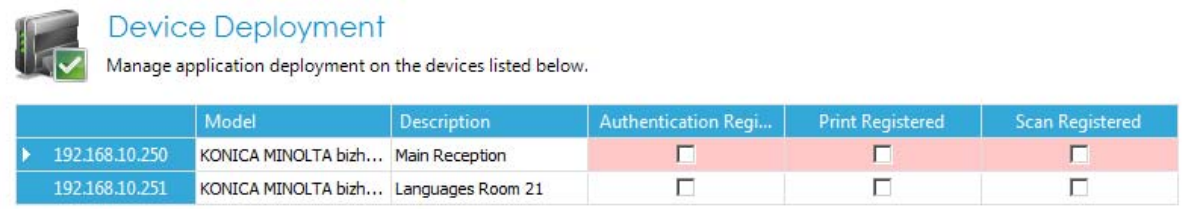

Figure 63

Licensing

In order to run the XPR Enterprise Konica Minolta Embedded applications, an active licence is needed by each device. The number of device (client) licences allowed is determined when you purchase a support licence for the product. During your 30 day evaluation period you may licence up to 500 devices.

Licence Status

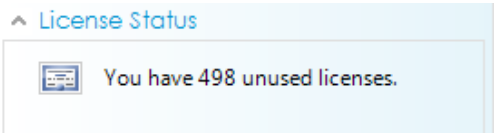

Figure 64

Service

When all of the above steps have been completed, the service can be started.
The service will listen for incoming requests on your chosen IP ports.

Starting and Stopping the service

The service can be started and stopped from the Actions menu or the Windows Service Manager (Services.msc). Stopping the service will suspend communication between the application and the devices.

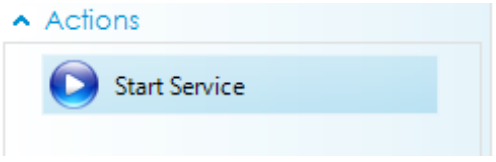

Figure 65

Listening

When listening is initiated for each application, your active devices should be able to communicate and function.

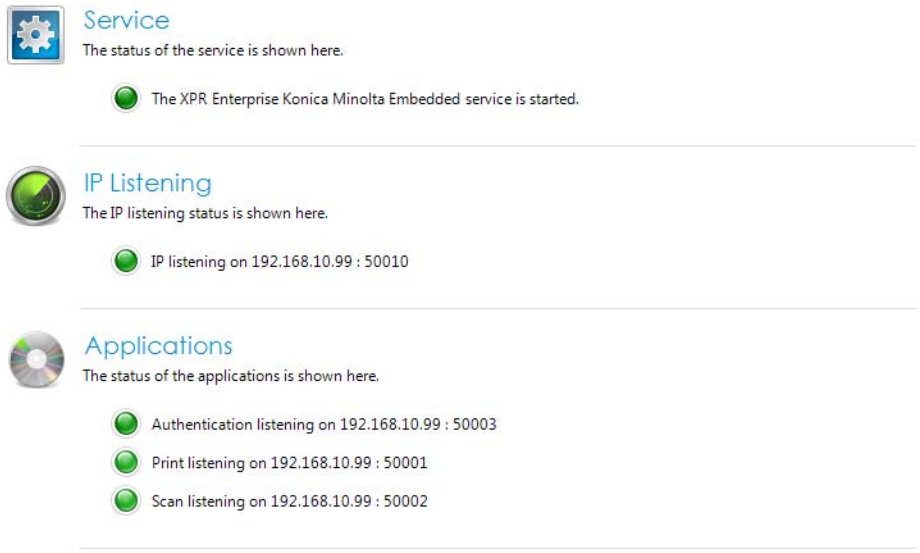

Figure 66

N.B.
Firewall software on the host server must be configured to allow for sending and receiving on the specified ports.