Print Audit 6

Print Audit Embedded for Print Audit 6

Version: 2

Date: 03-Dec-2018 17:21

Table of Contents

There are a number of documents to help you with your Print Audit Embedded implementation with Print Audit 6. Use the links below to find help for Installation and configuration.

Also remember that you can browse our Knowledge Base for additional help.

Browse Documents:

Browse Other Product Documentation:

Print Audit 6 Infinite Device Management Print Audit Secure Rapid Assessment Key Embedded for Sharp

Embedded for Kyocera Mita Embedded for Lexmark Embedded for Xerox Embedded for HP

Copy Audit Touch Copy Audit Numeric

Embedded for HP Documentation

Print Audit Embedded installs directly onto supported HP OXPd® -enabled multifunction peripherals, allowing users to control and recover all printing, copying, faxing and scanning costs. Review the documentation below for help installing and configuring Print Audit Embedded. You can also use the Knowledge Base to find more information.

Browse Documents:

Collapse allExpand all Collapse all

Browse Other Product Documentation:

Print Audit 6 Infinite Device Management Print Audit Secure Rapid Assessment Key Embedded for Sharp

Embedded for Kyocera Mita Embedded for Lexmark Embedded for Xerox Embedded for HP

Copy Audit Touch Copy Audit Numeric

Embedded for HP-Install and Setup

Print Audit Embedded for HP is used alongside Print Audit 6 to provide authenticated access to HP MFPs, for the purpose of securing device functionality, and tracking usage. Users can be required to authenticate at the MFP by login, PIN, or card swipe identification before they may access MFP functions.

When additionally used in conjunction with Print Audit Secure, users will also be able to select and release secure print documents directly from the MFP panel.
This guide provides instructions to install and configure Embedded for HP with Print Audit 6.

When used with Print Audit 6, Embedded for HP will track:

- walk-up copying
- scanning
- faxing
- printing from the document server

When Print Audit Secure is added, Embedded for HP can additionally provide:

- Secure release of all printing
- Follow Me printing

Components

Embedded for Hewlett-Packard consists of two main components:

1. Print Audit 6 - Embedded for HP Configuration:

Embedded for HP is configured using the Embedded Systems plug-in for the Print Audit 6 Administration tool. Support for Embedded for HP exists in Print Audit 6.10 or newer.

2. Embedded Client:

This software is installed on a Windows web enabled server while the embedded application runs on the MFP's embedded web browser. The Embedded Client provides a user interface directly on the panel of the HP MFP to enable the tracking of copies, scans or faxes, or the printing of documents stored in the MFP's Document Server.

In addition to tracking the number of pages in a copy, scan, fax, or print job, the Embedded Client tracks additional information about the job. For example, the Embedded Client can request a PIN Code from the user to identify and track who is creating the photocopy. Or, it can request a Client Code to identify which customer or cost center should be billed for a fax transmission.

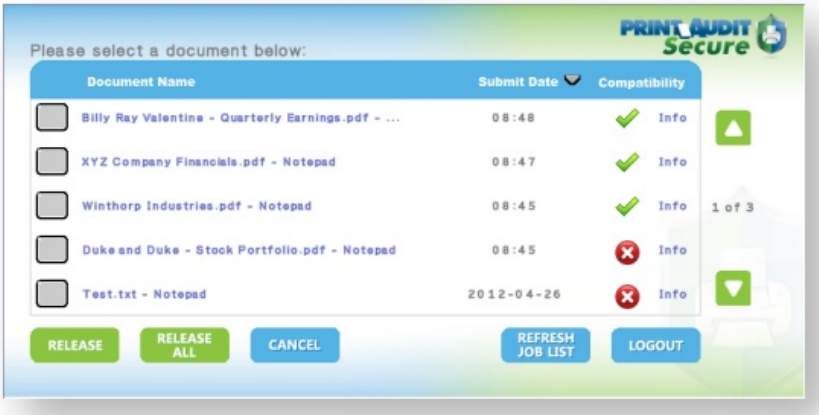
Print Audit 6

Print Audit 6 is a client application that tracks all printing directly from the desktop where the print job was issued. Every job, along with its attributes, are collected and stored in the Print Audit database, where it is available for reporting on printing volume and trends.

Print Audit 6 is available in 3 different modules, Analysis, Rules, and Recovery, which respectively, enable Analysis Reporting from the collected print data, the ability to create printing rules for rules-based printing, and the ability to allocate the cost of print jobs to a user, customer, or cost center.

When used with Embedded for HP, Print Audit 6 can also track copy, scan, and fax jobs, and jobs that are printed from the document server.

Print Audit Secure



Print Audit Secure on Sharp OSA-enabled device

Print Audit Secure allows for print jobs to be held on the server until an authenticated user releases them from the MFP panel, or from a Print Audit Secure release station. When a printer is managed by Print Audit Secure, incoming print jobs are prevented from being automatically output, by holding them in a secure queue on the server. When used with Embedded for HP, users will authenticate at the MFP, view their held jobs on the MFP panel, select one or more jobs and release or delete them directly from the MFP front panel.

Authentication Devices

Print Audit Embedded for HP supports Authentication Devices, such as swipe card or proximity card readers, within an Embedded for HP environment. When an Authentication Device is configured in an environment with Embedded for HP, users must authenticate at an Authentication Device before they are allowed to access the supported HP MFP controlled by the device.

Licensing

To enable the Print Audit Embedded for HP the following is required:

1. **One Print Audit Embedded for HP license per controlled HP MFP** - Print Audit Embedded for HP is licensed on a per-MFP basis. To install Embedded for HP on 15 MFPs, licenses must be purchased for each of the 15 MFPs. MFP licenses can be purchased as part of any Print Audit license, and are additional to the Print Audit 6 client licenses needed to track print jobs originating from Microsoft Windows and Apple Macintosh workstations. In the event that there are insufficient licenses, Print Audit will stop tracking some or all of the MFPs—MFPs will continue to function as normal, but no information will be tracked.

2. **HP MFPs** - Print Audit Embedded for HP is only supported on OXPd enabled HP Enterprise devices which support OXPd v1.7.1 or higher.
3. **Print Audit 6.10 or higher** - Print Audit Embedded for HP requires Print Audit 6 to configure the MFPs. Consult the Print Audit 6 Installation Guide for more information.

Optional

1. **Print Audit Secure 1.1 or higher** - Consult the Print Audit Secure Installation instructions for more information
2. **One Authentication Device per HP MFP** - Print Audit Embedded for HP supports HID proximity and contactless smart cards for authentication. Users can enter validation data by presenting the card at the card reader. If any authentication devices are to be used in the environment, one authentication device is required per MFP.

Limitations

Print Audit Embedded would ideally function identically across all makes and models. However, due to differences among the proprietary platforms, it is sometimes not possible to implement all features and functionality of the product. The following are a list of known limitations, when using Print Audit Embedded for HP.

1. **Ability to Return to Print Audit Embedded:** Once a user has logged in and Print Audit Embedded unlocks the device, allowing a user to choose a task on the panel, there is no method to return to the Print Audit Embedded application. Therefore, it is not possible for a user to attribute jobs to more than one custom field per logged on session, as is possible with other versions of Print Audit Embedded.
2. **Limitations with Account Limits:** Limiting jobs based on quota is not supported on OXPd v1.7.1 devices at present.
3. **Cost Allowances:** There is no method to preventing a user from exceeding their account limit, if there was available credit in their account when they logged in. If they exceed their limit, they could go beyond their minimum balance. However, if the user attempts to login with no available balance, they will be denied from using the device.
4. **Restricting functionality**: Restricting functionality (ie: restricting color copies) is not supported.

1. Installation - Embedded for HP

This section only addresses the installation requirements and configuration of Print Audit 6 for use with Embedded for HP. For complete instructions on installing and configuring Print Audit 6, please refer to the Print Audit 6 Installation information found online. Refer to that documentation to perform the following steps to install Print Audit 6 in conjunction with Print Audit Embedded for HP.

System Requirements

- **Windows Server 2008 R2 or newer** - requires Internet Information Services 6 or better.
- **MS-SQL Server 2005 Express or better -** running embedded applications on with an Access database is not recommended.
- **Print Audit 6.10.0 or newer**
  - Download the latest version from http://www.printaudit.com/software-updates.asp
  - The Print Audit 6 Database Communicator, Database and Administrative tools must be installed on a Windows 2008 or newer computer.
- **Microsoft .NET Framework v4.0**.
- **Internet Information Services (IIS)**.
- **Windows Communication Foundation**.

Optional

- Print Audit Secure 1.3 is supported with Embedded for HP.

Before you Install

- Print Audit Embedded for HP will run on OXPd enabled HP Enterprise devices which support OXPd v1.7.1 or higher.

Steps to Install

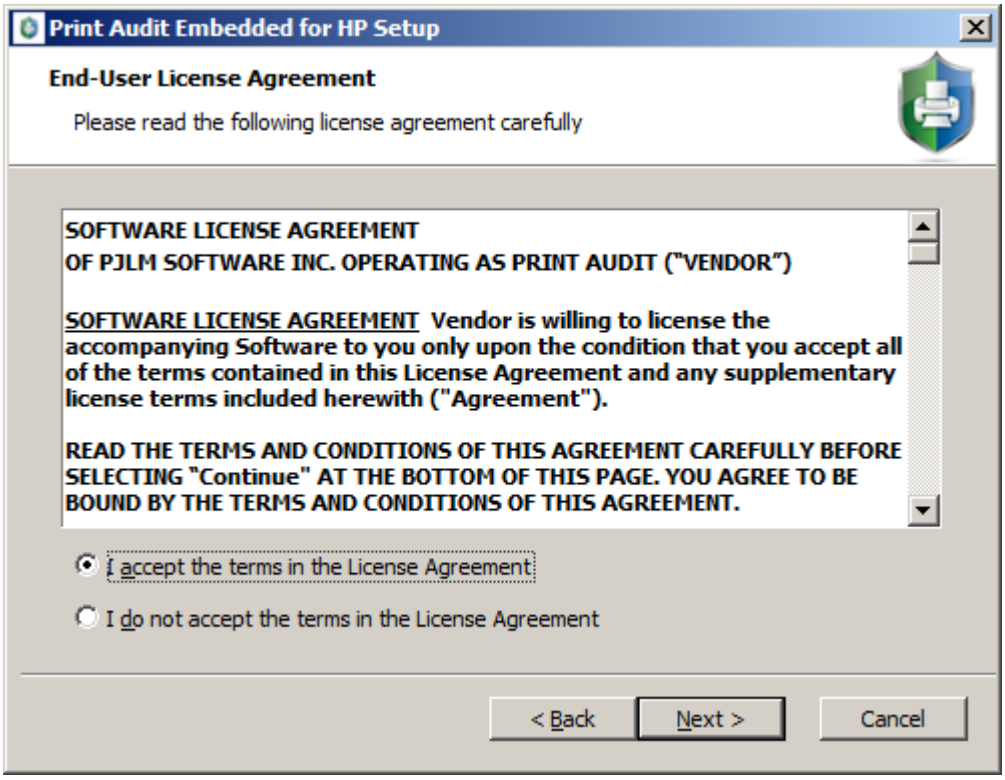
1. Obtain a Print Audit Embedded License for each MFP you need to install on.
2. Install and configure Print Audit 6 with the appropriate licensing.
3. Download the HP Embedded Application from the Print Audit web site.
4. Install the Print Audit Embedded for HP installation package on the server.
5. Deploy the Print Audit Embedded for HP to the device using the web portal using the URL *http://<server-ip-address>/HP.Embedded.App/Config.*
6. Create the record for the MFP in the Print Audit Administrator Embedded section.
7. Verify operation and tracking of the MFP.

Installing the Print Audit Embedded for HP installation package on the server

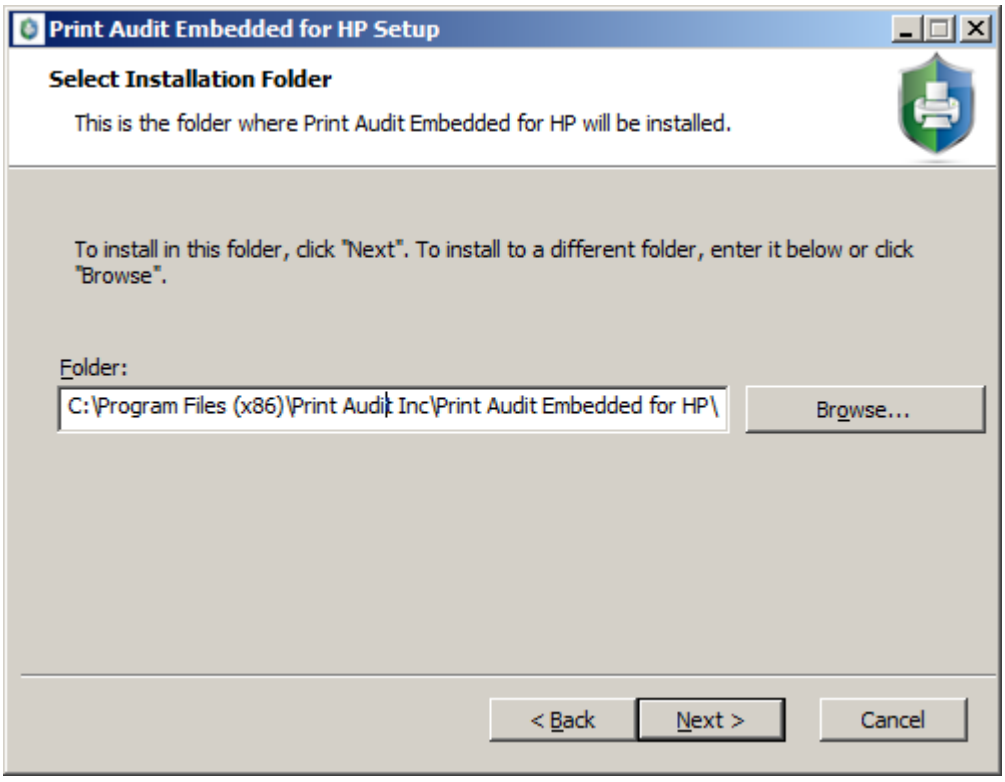
The installation package has a wizard like user interface that will guide you through the installation process.

1. Double click on the HP_Embedded_Setup.exe to begin the installation.
2. On the "Welcome to the Print Audit Embedded for HP Setup Wizard", click Next.

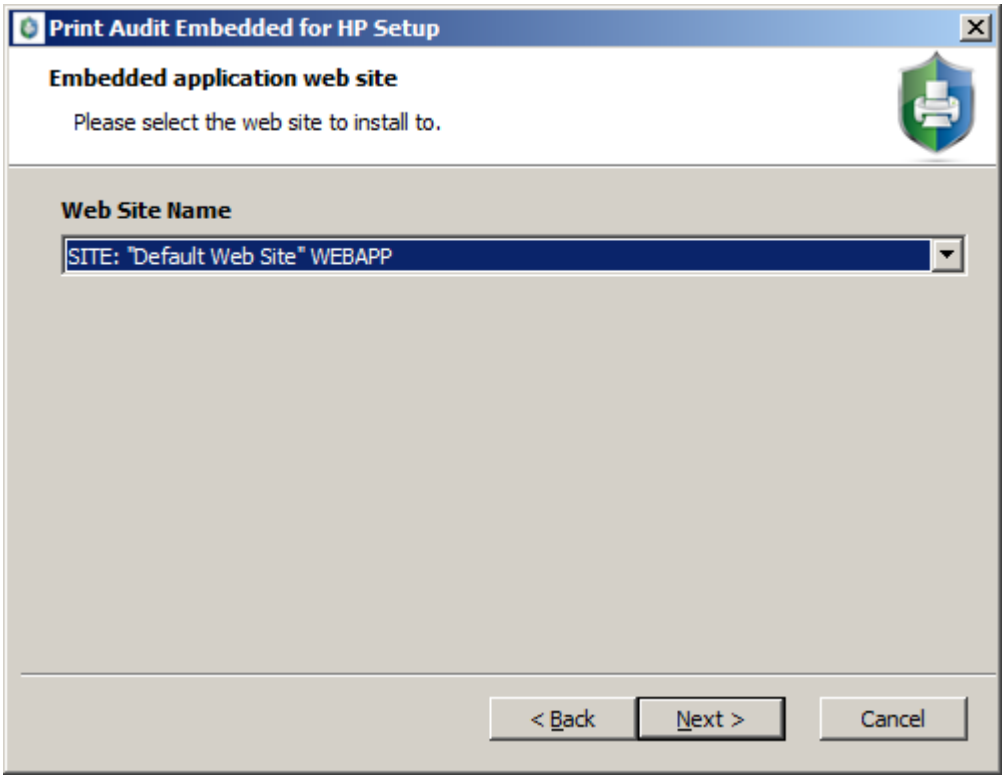
3. Read the End User License Agreement and select the checkbox if you accept. Click Next.



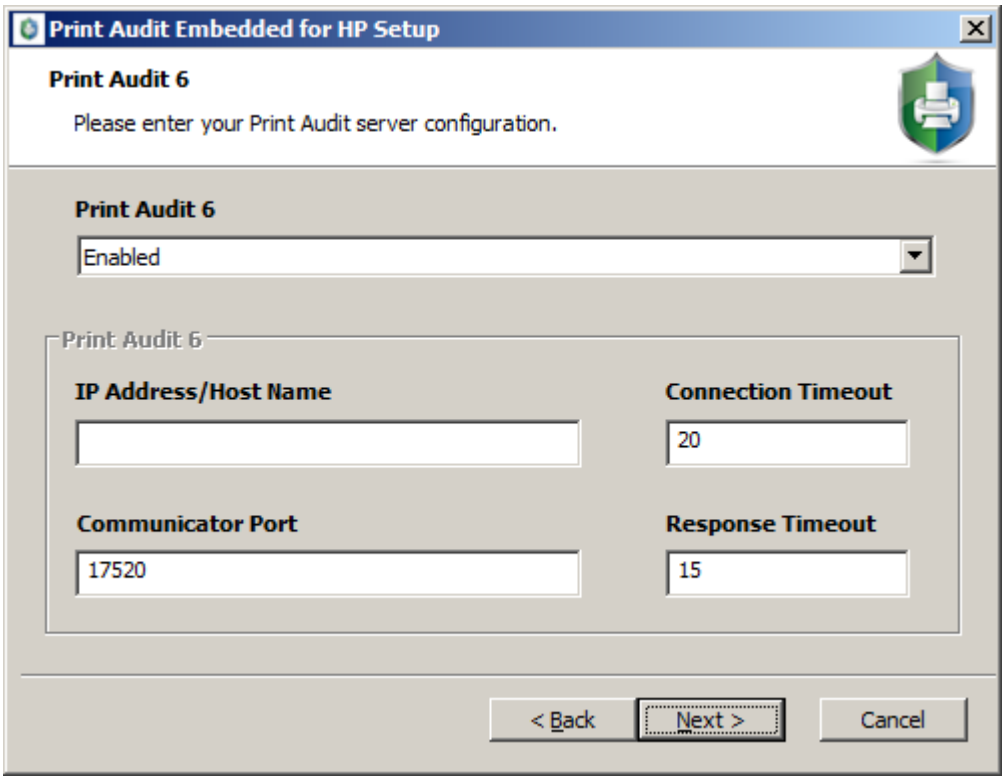
4. Select the install location. A default location will be available to you. Click Next when finished.



5. Select the Website name where the Embedded for HP web service will be created. It is recommended to use the Default Web Site. Click Next.



6. Enter the Print Audit 6 configuration details. Click Next when finished



a. From the dropdown box, choose Enabled or Disabled to enable/disable the Print Audit Embedded for HP application for use with Print Audit 6.

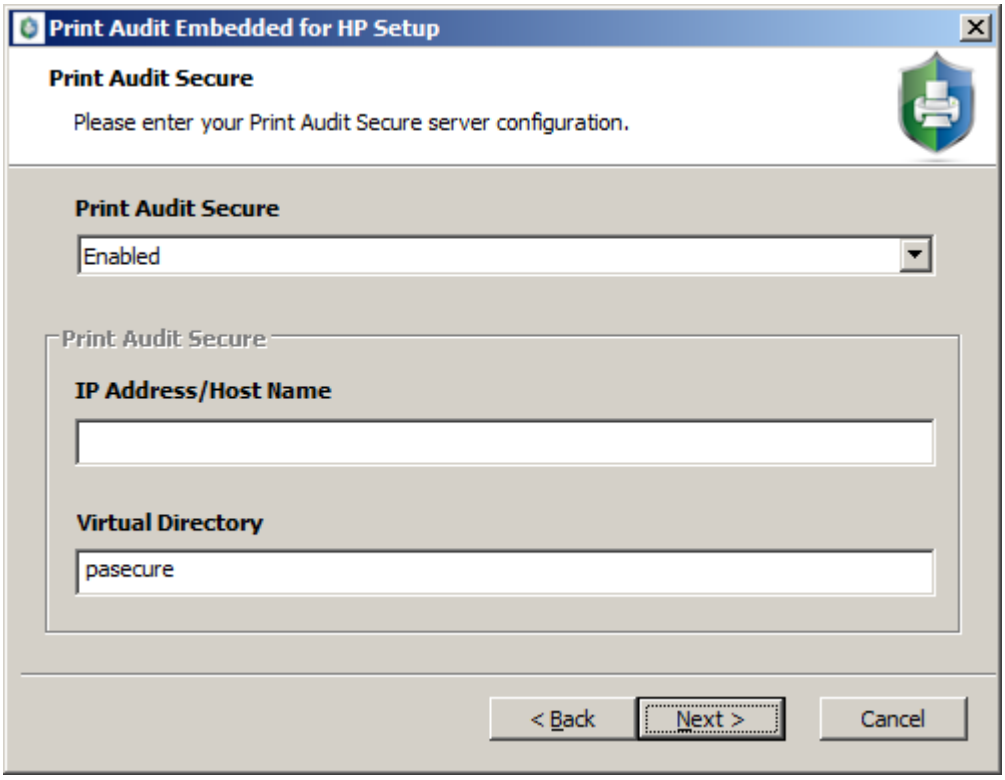
b. IP address/Host Name - the IP Address or Host Name of the server running the Print Audit 6 Database Communicator.

c. Communicator port - the port number the Database Communicator is set to listen on. The default is 17520.

d. Connection Timeout - the time in seconds that the Print Audit Embedded for HP application will wait before a connection to the Database Communicator fails. The default is 20 seconds.

e. Response Timeout - the time in seconds that the Print Audit Embedded for HP application will wait before a response from the Database Communicator before failing. The default is 15 seconds.

7. Enter the Print Audit Secure Server details. Click Next when finished.

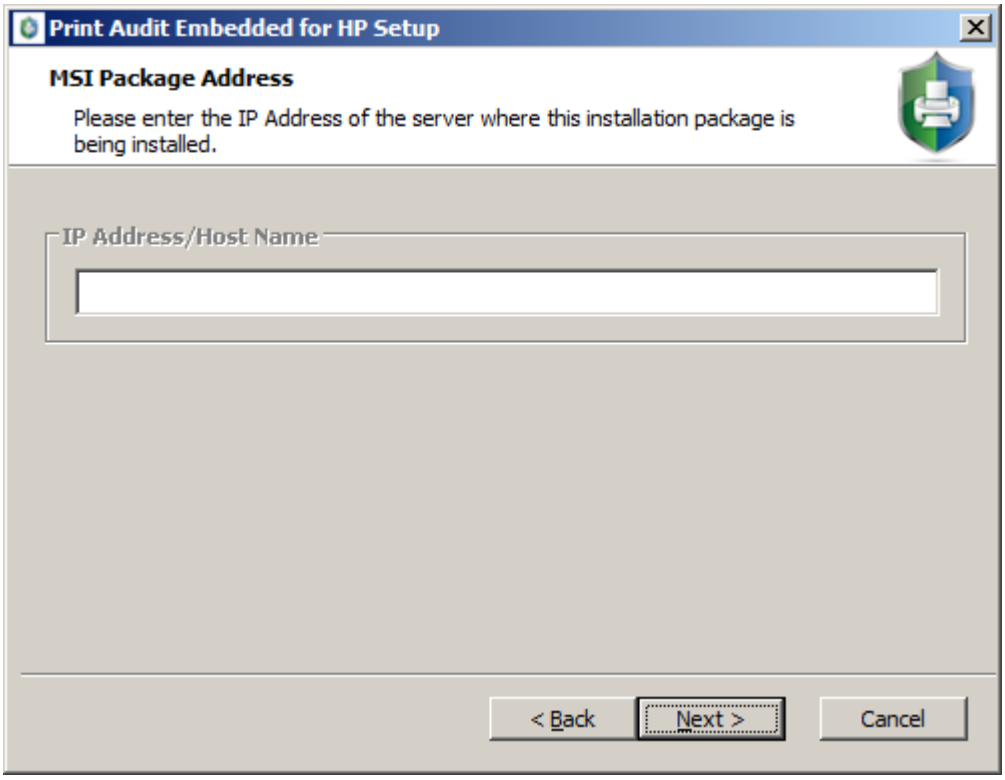


a. From the dropdown box, choose Enable or Disabled to enable/disable the Print Audit Embedded for HP application for use with Print Audit Secure.

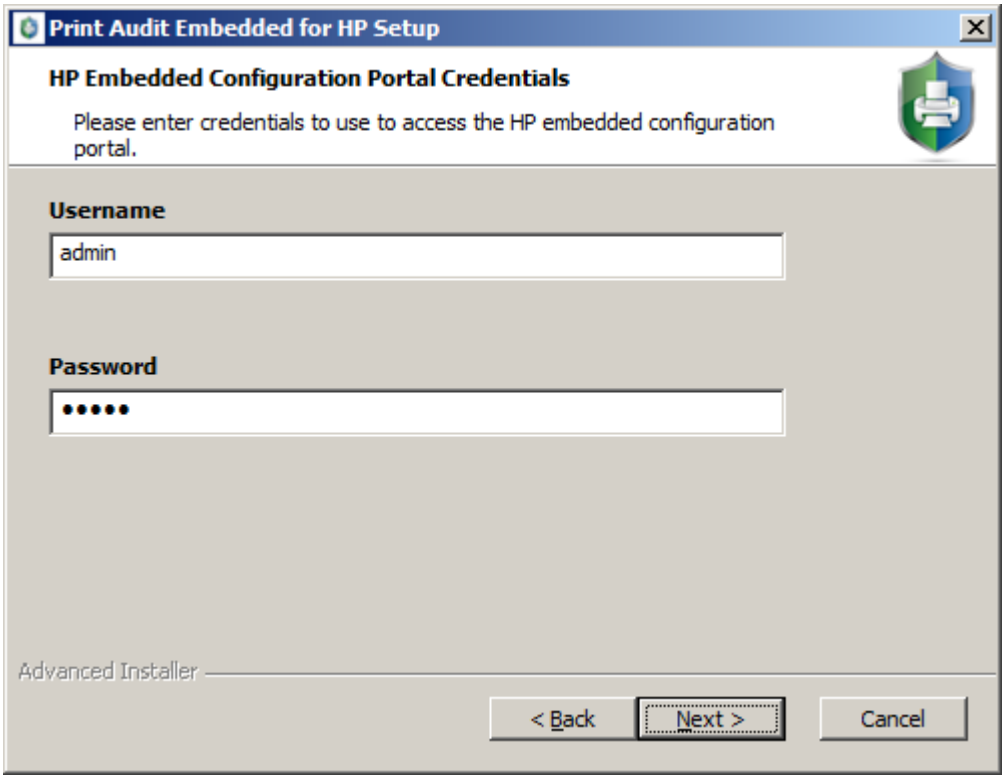
b. IP Address/Host Name - the IP Address or Host Name of the server running the Print Audit Secure Server.

c. Virtual Directory - the name of the virtual directory configured on the Print Audit Secure Server. The default is "pasecure".

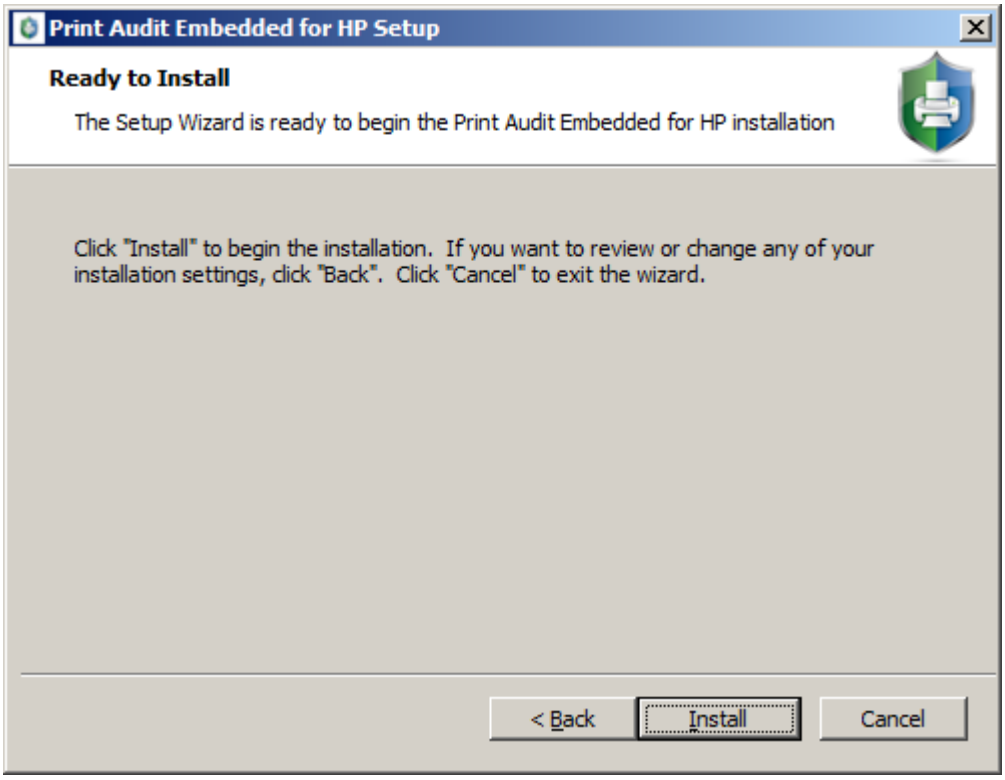
8. Enter the IP Address/Host Name where the installation package is being installed from and click Next when finished.



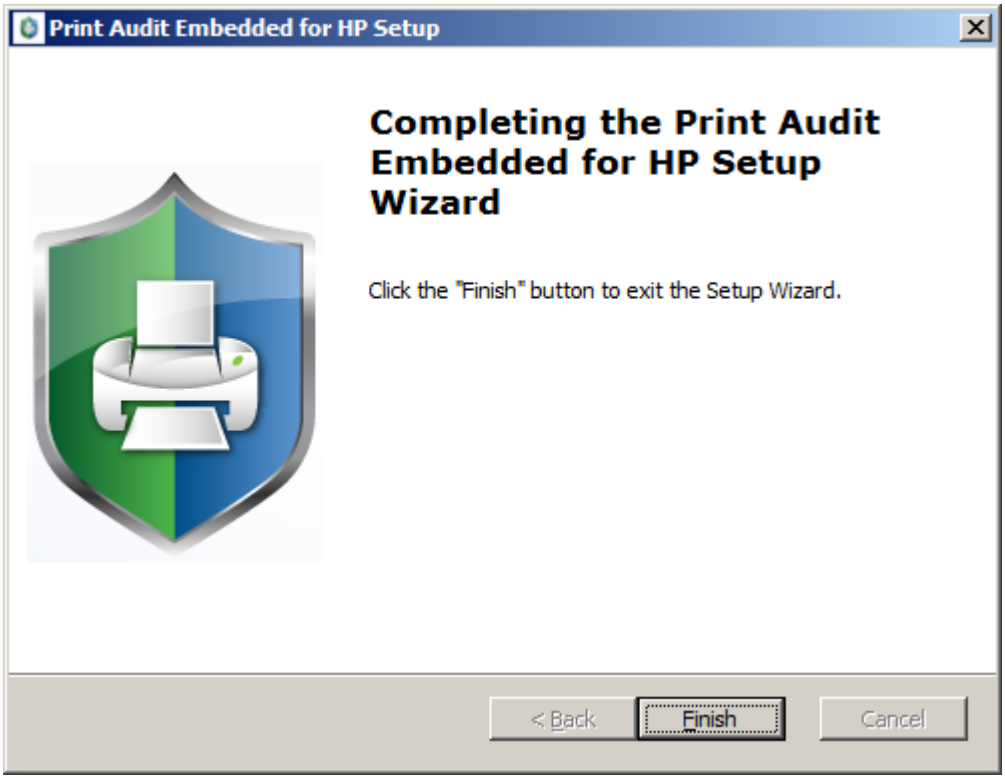
9. Enter the credentials used to access the HP Embedded configuration portal and click Next when finished.



10. Click Install to begin installing Print Audit Embedded for HP. The installation may take a few minutes to complete.



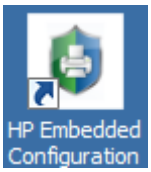
11. When the installation is complete, click Finish.



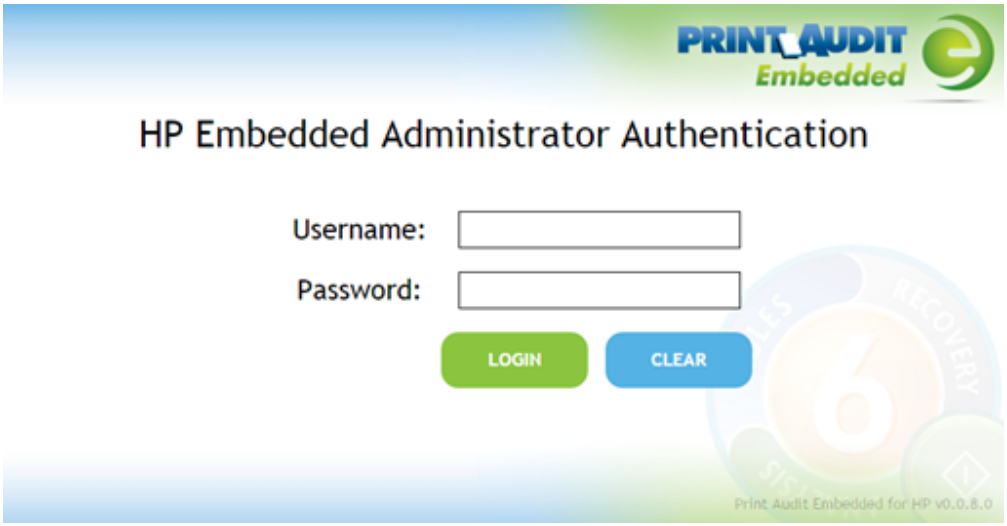
12. (Optional) Verify that IIS settings are correct. See the IIS Configuration/Setup for Print Audit Embedded for HP section in this document.

Deploying the Print Audit Embedded for HP application to MFPs

1. On the server desktop there should be a short cut named *HP Embedded Configuration.* Open it by double clicking on it. The short cut opens a web page with the following URL; *http://localhost/HP.Embedded.App/Config*



2. Enter the HP Embedded Configuration Portal credentials to authenticate and click "Login". The credentials are the same as those used to access the HP Embedded configuration portal .



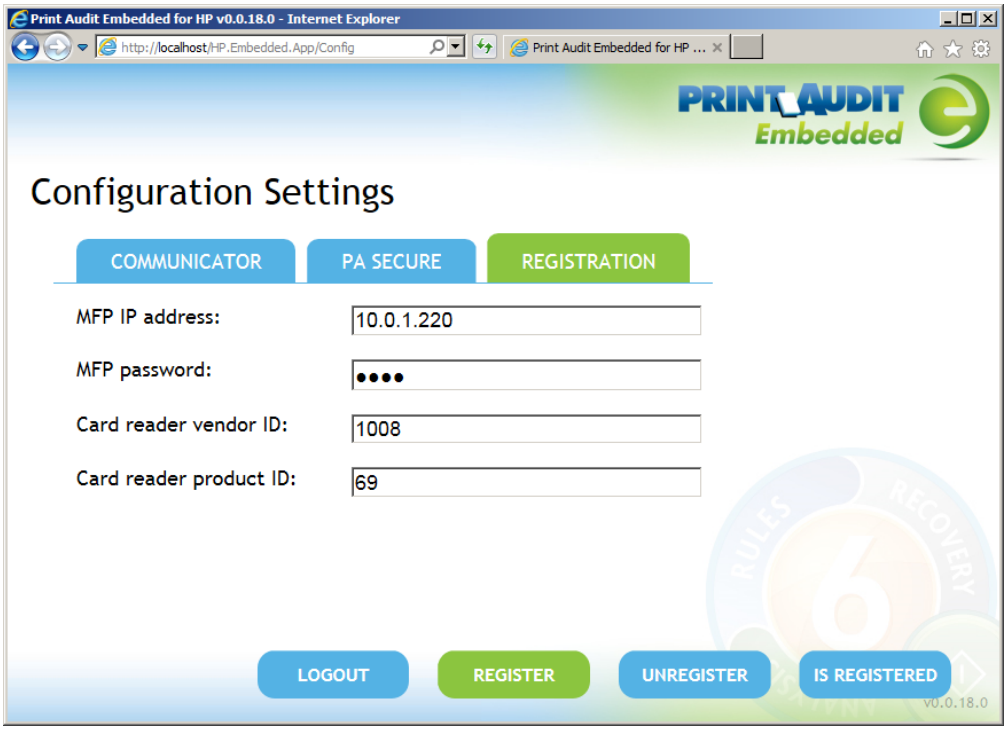
3. Once authenticated three tabs will appear:
    - Communicator
    - PA Secure
    - Registration

4. Communicator is where settings related to Print Audit 6 are set. If Copy, Scan and/or Fax tracking are to be used select 'Enable PA Communicator'. Configure the IP Address or Hostname and port for the server running the Database Communicator Service. Click Update to commit changes.

5. Click on the PA Secure Tab. *This* is where settings related to Print Audit Secure are set. If using the Print Audit Secure functionality select 'Enable PA Secure'. Enter the IP address or Hostname of the system hosting the Print Audit Secure Server. Click Update to commit changes.
   **Note: pasecure is the default virtual directory for a Print Audit Secure server

6. Click on the Registration Tab. Registration permits the administrator to perform different tasks regarding the embedded application. These are:
    - Register, deploys the application on to a device.
    - Unregister, removes the deployed application from a device.
    - Is Registered, checks the current status of the deployment of a device.
    - Set the Card Reader vendor and product ID (click for more details). The vendor and product ID are in decimal not hexadecimal format. Please consult the Card Reader manufacturer for these settings.

To register the application with the HP Device enter the IP address and the administrative password for the unit. Press the Register button.



Using the Print Audit Embedded for HP client

The Embedded for HP Client is very easy to use. First, it prompts you for the required information. What appears in the prompts will depend on how the Embedded Client was configured. After you enter the prompted information, the MFP is enabled for copying, scanning, fax, or printing a document server print job. When you are finished using the device, it is advised to return to the Embedded Client and indicate that you are finished, and end your logged in session. At this point, the information is tracked to the database, and the Embedded Client resets to be ready for the next user.

If you forget to return to the Embedded Client after finishing up, an Inactivity Timeout ensures that, after a period of inactivity, your logged in session ends, the information is tracked, and the panel interface is ready for the next user.

Detailed Panel Walkthrough

"None" Type of Authentication

First, press the Start button on the screen. The Embedded Client retrieves its configuration, and proceeds to prompt for the required information as discussed below.

At any time during the prompts, press the Cancel button to cancel all of your input and return to the start screen.

PIN or Card Reader Authentication

In many cases, the panel is configured to ask for authentication as the first prompt. The panel will prompt you to enter a PIN code, swipe your proximity card, or will allow either type of authentication .

Enter your PIN code using the numeric keypad, or press the Show Keyboard button to access a full alpha- numeric keyboard on the touch screen. Once you have entered your PIN code, press the OK button. You can also use the # key on the keypad for OK.

To use a proximity card, hold the card near the sensor. The light will turn green and the sensor will beep when your card has been read.

Custom Fields

If the panel is configured to prompt for custom fields, these are the next prompts. Select one of the presented options and then press the OK button. If there are more choices than will fit on one screen, use the Prev and Next buttons to page through the choices.

If the Custom Field is either the Searchable or Searchable Dropdown type, there will also be a Search button displayed. Press the Search button to bring up a keyboard, and enter in the text you wish to search for. Press OK to perform the search and hide the keyboard. Once you have searched, only options that match your search text will be shown, and you can page through them as usual. If you do not find the option you are looking for, you can perform another search.

Comments

If the panel is configured to allow the user to enter a comment, this will always be the last prompt. Enter a comment using the numeric keypad on the MFP, or press the Show Keyboard button to enter the Comment using a full alpha-numeric keyboard on the touch screen. When you have finished, press the OK button. The comment may be left blank.

Once you have finished entering all of the information, a screen with a large Done button appears. This screen also has instructions on how to return to the Embedded for HP Client. At this point (before pressing the Done button), use the MFP function keys to switch to Copy, Fax, Document Server, Scan, or Print mode as appropriate, and proceed to use the MFP normally.

2. Configuration - Embedded for HP

This Embedded for HP window in Print Audit 6 enables the configuration of all aspects of the Embedded for HP copier device. The different elements of the window are described below.

Pre-configuration checklist

If you are ready to begin configuring Print Audit 6 with Embedded for HP, you have:

- Installed the Print Audit Database Communicator, Database and Administration tools to a computer on the network that will be on and available at all times. The Print Audit Client should be installed on at least one workstation, to test printing and ensure that print jobs are being tracked correctly before continuing.
- Configured Print Audit 6 for PIN codes and validated fields to be integrated into Print Audit 6 Embedded.
- Installed the <LINK FOR HP DOWNLOAD> software on a computer that has Internet Information Services (IIS) and .Net installed, and is acting as a web server.
- Used this guide to configure Print Audit 6 Embedded on HP OXPd enabled devices.

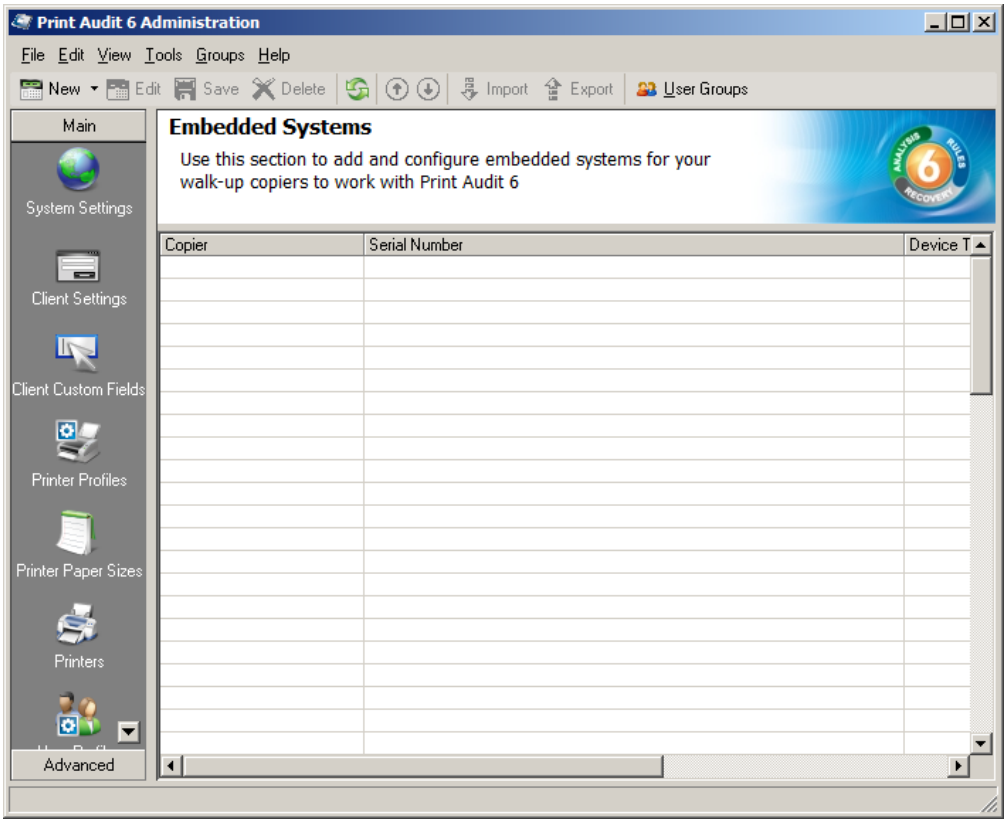
Overview

The Print Audit Administration tool provides the ability to configure Embedded for HP on all the MFDs in the environment using the Embedded Systems plug-in. Configure one copier for every physical HP MFD on which the Embedded Client will run.

Costs, authentication methods and custom fields may be configured for each device.

Adding, Editing and Deleting Copiers in Print Audit 6

Use the Embedded Systems section of the Administration tool to add, edit and delete Embedded for HP copiers. A copier in the Administration tool represents a physical copier in the network.



To add a new copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Click the New button on the toolbar.
4. Select Embedded for Hewlett-Packard from the dropdown list of embedded applications.
5. Press OK. The Add/Edit Embedded for HP window will appear.
6. At minimum, a copier name and the serial number of the copier must be provided. Please refer to the 'Embedded for HP Configuration Window' section below for more information filling out the Embedded for HP window.
7. Click the Save button. The Embedded for HP window closes and the copier appears in the Copiers list.

To edit a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Edit button on the toolbar. The Embedded for HP window appears.
5. Make any needed changes to the copier.
6. Click the Save button. The Embedded for HP window closes and the copier appears in the Copiers list.

To delete a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Delete button on the toolbar. A message appears to verify removal of the copier.
5. Click the Yes button to delete the copier. The list of copiers refreshes.

Configuring the HP MFP in Print Audit 6

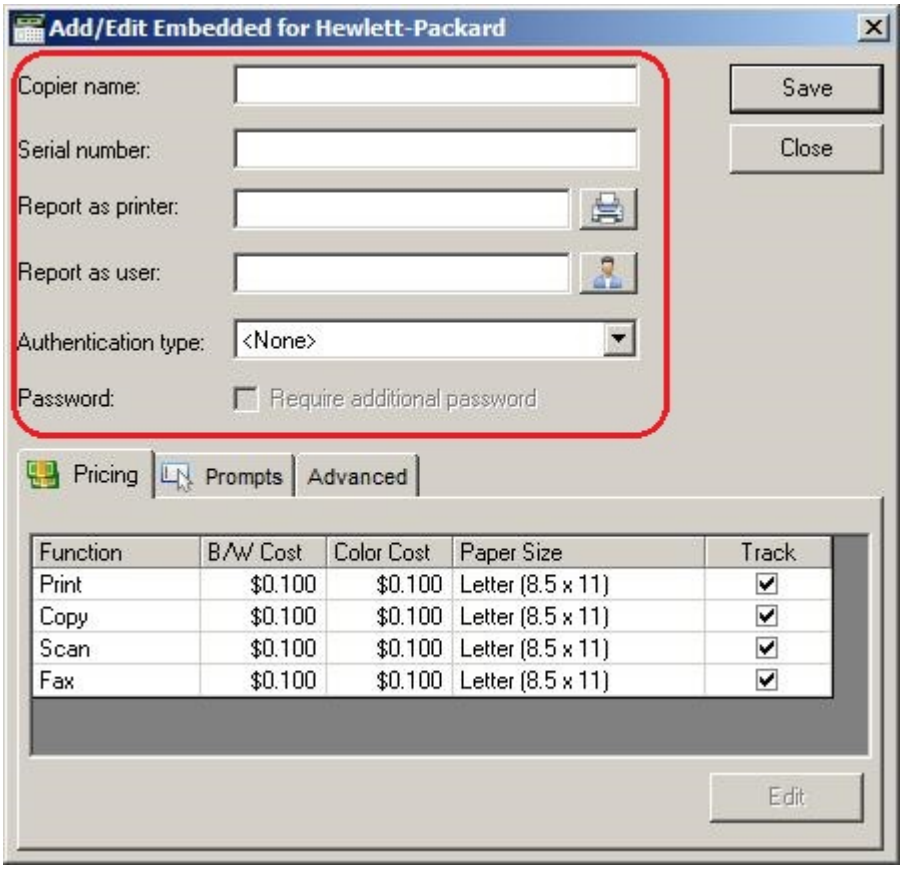
This Embedded for HP window in Print Audit 6 enables the configuration of all aspects of the Embedded for HP copier device. The different elements of the window are described below.

General

Copier name - The name to describe the copier. Enter a name that is descriptive enough to distinguish the copier from others. For example "Third Floor HP OfficeJet X585".

Serial number - The serial number of the HP MFD. NOTE: the serial number is case-sensitive and must match the serial number of the HP MFP that the Embedded Client is installed on

Report as printer - Use this to select an already existing Print Audit printer with which to associate the copier. For example, if there is an MFP in the office that users print to which is already in the Print Audit database, choose that MFP here for the copier so that all transactions are reported as the same printer. If a printer is not selected here, Print Audit will record transactions for this copier as the copier name.



Report as user - Use this to select an existing Print Audit user whom to associate all jobs from this copier. Use this functionality to still have individual user authentication, but for reporting purposes report all jobs to a single user.

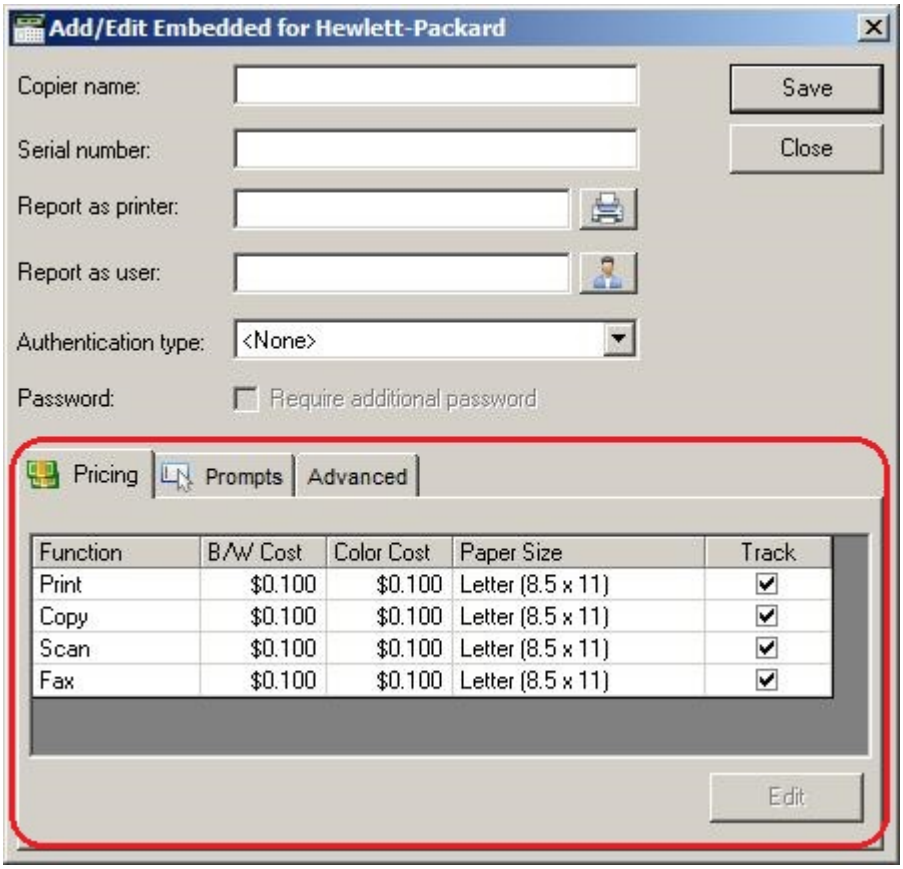
Authentication type - Select how the user will authenticate to the copier before they can do transactions. The authentication type determines how a user identifies themselves to the copier before they can do a transaction. The following options are available:

- None - Users do not have to authenticate before using the copier. All transactions are recorded to the generic HP_Embedded user.
- PIN code - Users must enter their Print Audit PIN to access the copier.
- Card Reader - Users must use their proximity card or swipe card to access the copier
- Card Reader or PIN - Users must use their proximity / swipe card or enter their Print Audit PIN to access the copier.
- Active Directory - Print Audit Embedded for HP can authenticate directly against an Active Directory server. When this option is selected, at least one Active Domain must be entered in the AD Domain(s) field. Multiple domains can be used if they are separated by a comma (,). When this authentication method is used, users will have to select the domain from a dropdown on the Print Audit Embedded for HP application as well as entering their Username/Password.

Require additional password - Check this box to require the user to enter an additional (optional) password before they can authenticate using the Authentication type selected above.

Pricing tab

This tab contains the pricing for each function on the copier.

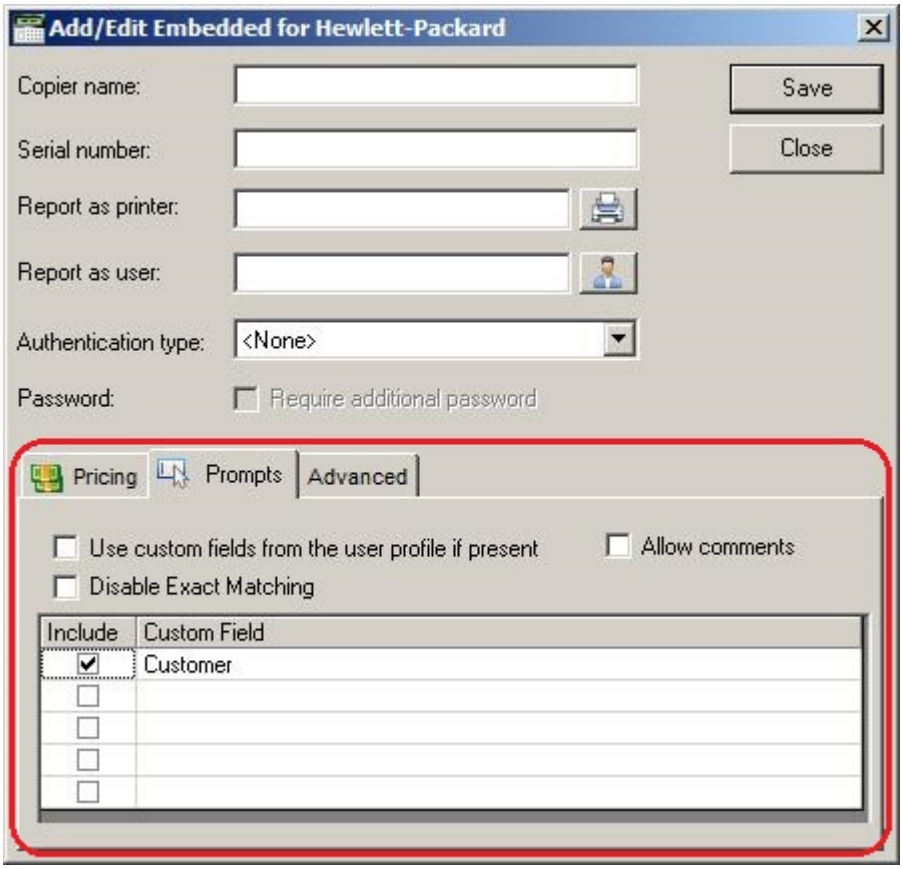


To edit the pricing for a particular function:

1. Clear the "Track" column for the function to disable the tracking of transactions of that type.
2. Select from the list the function that is to change and click the Edit button. The Configure Pricing and Paper Size Window appears.
3. Set the pricing as it makes sense for this copier in the organization.
4. Click the Done button. The Configure Pricing and Paper Size Window closes.

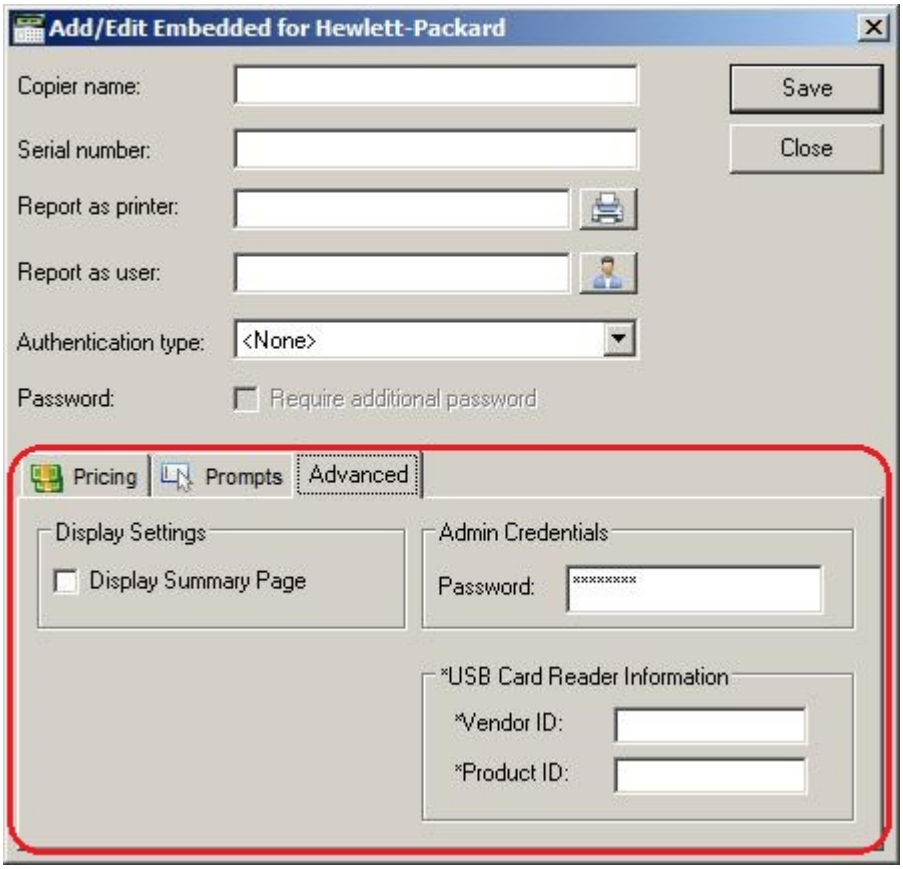
Prompts tab (only with Print Audit 6 Recovery)

This tab is only relevant when using Print Audit 6 Recovery for the charge-back of printing.



- For each Activity the user can be required to enter values for Custom Fields. Custom Fields are setup in the Custom Fields section of the Print Audit Administrator. On this tab, select from any one of the Custom Fields configured and define a custom prompt for each one. Note: The Client Custom Field(s) must be created first before they will appear under the Prompts tab.
- Use custom fields from the user profile - Check this box to override the default custom field choices with the custom fields set in a user's User Profile.
- Allow comments - Check this box if the user can enter general comments about the job.
- Disable Exact Match - Check this box if the user can enter the custom field directly in the field and proceeds to the next step without selecting from the list.
- Custom fields - The custom fields list contains all custom fields that have been defined. To use a custom field for the activity, check the Include checkbox.

Advanced tab



This tab is used for setting the summary page display as well as modifying the USB card reader information.

- Display Summary Page - check this box if you would like to view the summary page of all selected prompt / comment values.
- Admin Credentials - enter the login credentials for the MFP admin.
- - Vendor and Product IDs are numbers used to identify USB devices to computers and other hosts. Print Audit Embedded for HP requires the Vendor and Product specific to the USB card reader being used with the HP MFP so that the HP MFP can initialize the card reader. Please contact the manufacturer of the USB card reader for these values. Print Audit Embedded for HP requires these values to be in a "decimal" format. If they are provided in a hexadecimal format, you can use a hexadecimal to decimal converter such as Windows Calculator (in Programmer view) to perform the conversion.
    - Vendor ID - the Vendor ID of the USB Card reader in decimal format.
    - Product ID - the Product ID of the USB Card reader in decimal format.

3. Using HP Embedded with Print Audit 6

The Embedded for HP Client is very easy to use. It will first prompt for required identification or billing information, before enabling the device for copy, scan, fax, or print functionality. Once the desired function is complete, return to the panel and complete the session, otherwise the MFP will timeout the session. When the session ends, the copy, scan, fax, or print transaction is sent to the Print Audit 6 database, and the Embedded Client resets to be ready for the next user.

The standard set of steps to using Embedded for HP to track job information is as follows:

1. **Start the Transaction** - Press the Start button on the screen. The Embedded Client retrieves its configuration and proceeds to prompt for the required information. The Cancel button can be used at any time to return to the Start screen.

1. **Authenticate** - If configured to ask for a PIN Code, the Embedded Client displays a login screen. To login:
    a. Press the PIN Code button. An input form displays.
    b. Enter a PIN Code using the HP keyboard or the touch screen.
    c. Press the OK button to accept the input.
    d. Press the OK button on the Login screen to validate the PIN Code.
2. **Enter Custom Field Information** - If configured to ask for Custom Field information, the Embedded Client will prompt for one or more values from the user. To enter values for a searchable field:
    a. Press the button on the touch screen that corresponds to the Custom Field Name.
    b. Enter a full or partial code on the screen and click OK.
    c. If only one match is found for the field, the Embedded Client asks for the next Custom Field value if any is configured.
    d. If Print Audit finds more than one match, a list of values will display. Use the touch screen to navigate through the values.
    e. When the desired value is found, press the button corresponding to the value. It appears highlighted.
    f. Press the OK button to accept the value.
    g. Press the OK button again to move to the next screen.
3. **To enter values for a non-searchable field**:
    a. Press the button that corresponds to the desired value. It appears highlighted.
    b. Use the arrows on the touch screen to navigate through the choices.
    c. Press the OK button to accept the value. The Embedded Client will request the next Custom Field value if any is configured.

4. **Enter any Comments** - If configured, the Embedded Client will request any Comments for the job. Press OK if to proceed without entering comments. To enter comments:
    a. Press the Comments button on the touch screen. An input form appears.
    b. Use the input form to enter comments.
    c. Press the OK button to close the input form.
    d. Press the OK button on the Comments screen to accept the comments.
5. **Verify Selections** - After all information has been input, a summary screen appears showing the current balance if any, along with the custom values selected. Press the OK button to accept the selections and begin the job.
6. **Complete the Job** - After the job is completed, press the "" (Logout)" button on the HP MFP keypad. This completes the transaction, and transmits the job information to the Print Audit database. If the "" (Logout)" button is not used to end the session, the HP MFP will eventually timeout the session, return to the Start screen and transmit the job information to the Print Audit database.

4. Using Embedded for HP with Print Audit Secure

The Print Audit Secure Embedded for HP Client is very easy to use. It will first prompt for required information. The prompts which appear are dependent on how the Secure Embedded Client is configured. Once the prompted information is provided, the device will release the secure job(s). Then the Secure Embedded Client resets to be ready for the next user. If the session is not manually finished, the HP MFP will timeout.

Following are the standard set of steps to using Secure Embedded for HP to release a print job.

1. Authenticate

1. **PIN Code authentication** - If configured to request a PIN Code, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Pin Code Field
    b. Enter a PIN Code using the HP keyboard or the touch screen.
    c. Press the Login button to accept the input.
2. **Authenticate with a Username** - If configured to ask for a Username, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Username Field
    b. Enter a Username
    c. Click on the Password Field

d. Enter a Password

e. Press the Login button to accept the input.

3. **Authenticate with a swipe card** - If configured to ask for a swipe card, the Secure Embedded Client displays a login screen. To login:

   a. Swipe a card in a card reader attached to the MFP.

2. Release Print Jobs

1. To release all the compatible print jobs, click the Release All button.
2. To release only certain jobs, press the checkbox next to the jobs to be released.
3. Click the Release button. The selected job(s) will now print.

3. Delete Print Jobs

To delete print jobs, press the checkbox next to the jobs to be remove and press the Cancel button. A confirmation dialog will appear. Press OK to delete the job or Cancel to return to the Jobs List.

3. Refresh Job List

To force the MFP to reload the secured jobs list, press the Refresh button.

4. Complete the Job

When finished releasing print jobs, press the Logout button on the HP MFP screen. This will notify Print Audit Secure that the transaction is complete. If this step is not completed, the HP MFP will eventually reset back to the Start screen.

5. Troubleshooting - Embedded for HP

Please refer to this section if issues are encountered with the operation of Embedded for HP. If a resolution is not found in this section, please contact Print Audit technical support.

On the installation of the Print Audit Embedded for HP setup, error "Users is not a valid user or group" occurs.

When trying to run the Print Audit Embedded for HP setup, an error occurs "An error has occurred while applying security settings. Users is not a valid user or group." This could be a problem with the package or a problem connecting to a domain controller on the network. Check your network connecting and click retry or cancel to end install". This error occurs when installing to a non-English language version of the Windows operating system. The installer looks for a group or user called "Users" and generates the above error message. The solution is to create a new Local Users and Group user called "Users" and retry the installation.

Where can I find logging information?
The embedded application writes detailed information to the Windows event log during deployment and in run time using three different logging levels.

- Information
- Warning
- Error

The log can be found by invoking *eventvwr* from the Windows command prompt. The *Print Audit* log can be found under *Applications and Services Logs -> Print Audit.*

The application does not register successfully on the device.
Please check that the firmware on the device is not older than December 2014 and support the OXPd v1.7.1 SDK. Do also check that you are using the correct password for the device.

The application registers fine but it never shows up on the device's screen
Might be a firewall issue. Please make sure the following ports are open in both directions on the server where the embedded application has been installed.

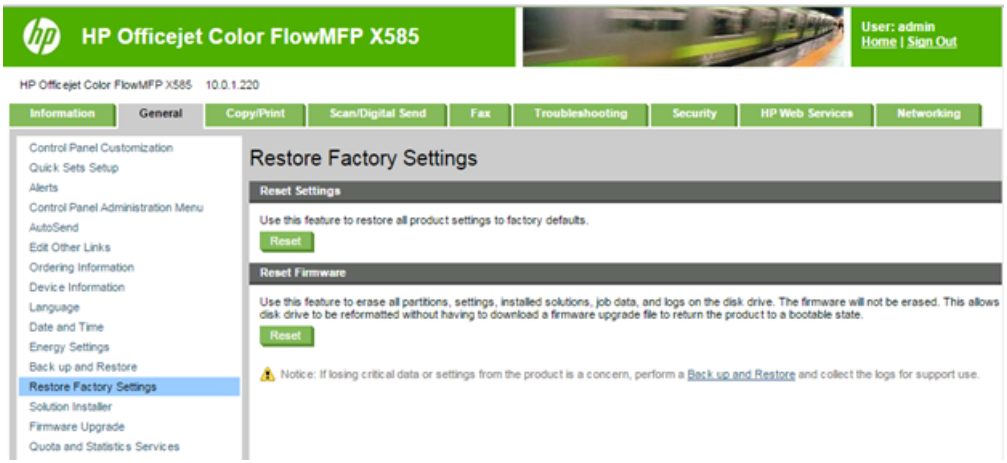
- 80
- 443
- 7627

Also make sure Microsoft .NET Framework v4.0 is installed on the server and that it has Windows Communication Foundation enabled.

When connect the USB card reader an error message is shown on the device.
All USB card readers must be registered on the device before being used. The application needs to know the *Vendor ID* and the *Product ID* of the specific card reader to function correctly. This information is entered when registering (deploying) the application through the *HP Embedded Configuration Portal.*

I have all prerequisites installed but the application just won't register (deploy) on to the device.
Sometimes it's needed to bring the device back to a known state. It could be that other applications have been running before on the device or somebody has changed important settings on the device. A *Factory Reset* will address these issues.

Open a web browser and surf to the MFP web page, sign in as *admin (*please note that a password must have been set for a factory reset is able to take place). Select the *General* tab then click on *Restore Factory Settings* on the left hand side of the screen. Press the *Reset* button below *Reset Firmware.* The process will eventually reboot the device. After the device has been rebooted you will need to reconfigure the network settings on the device and also set the password of the device.



I have registered the application on to the device but the authentication screen does not show.

Press the yellow circle arrow in the upper left hand corner of the MFP screen to refresh the screen. Many times this forces the application to lock down the device.

6. IIS Configuration/Setup for Print Audit Embedded for HP

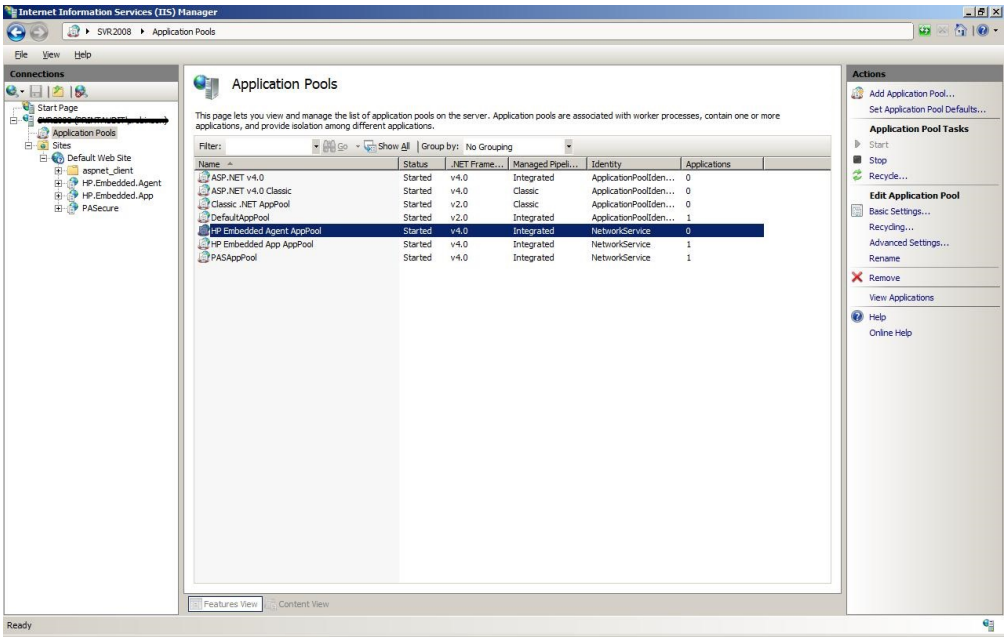
Please Note: The Print Audit Embedded for HP Setup Wizard is designed to configure settings in IIS when it is run. However, depending the environment, it may be necessary to verify or modify those settings. The examples presented in this guide are based on the default installation options. Please contact your System Administrator for additional details should changes to these defaults be required in your environment.

Verifying Application Pools

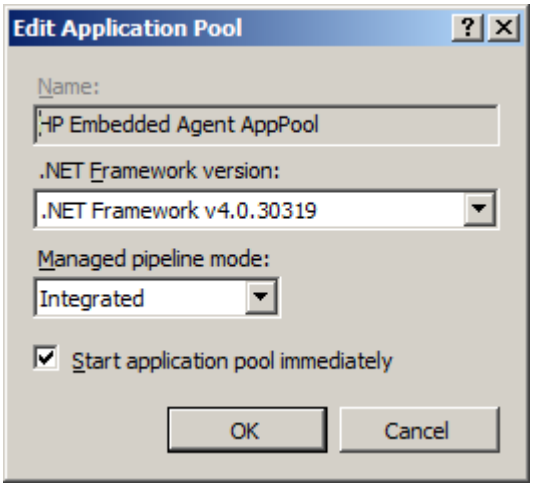
Application Pools in IIS allow different ASP.NET applications running on the web server to be isolated from each other. Errors in one application pool will not affect other applications running in other application pools. Print Audit Embedded for HP installs two separate application pools - HP Embedded Agent AppPool and HP Embedded App AppPool - both running under .NET Framework v4.0.30319.

To verify that the Application Pools have installed and configured correctly:

1. Open the Internet Information Services (IIS)Manager.



2. Under the IIS server name, "Application Pools".
3. Double click on the Application Name.



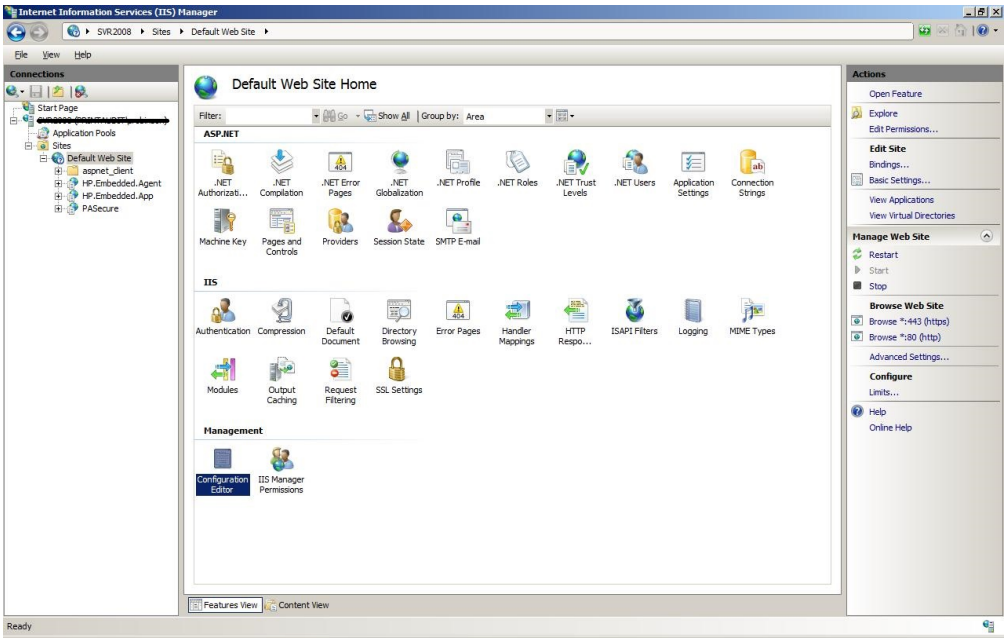
4. Use the dropdown ".NET Framework version" to select the appropriate version.

Verifying Application Pools used by Print Audit Embedded for HP sites

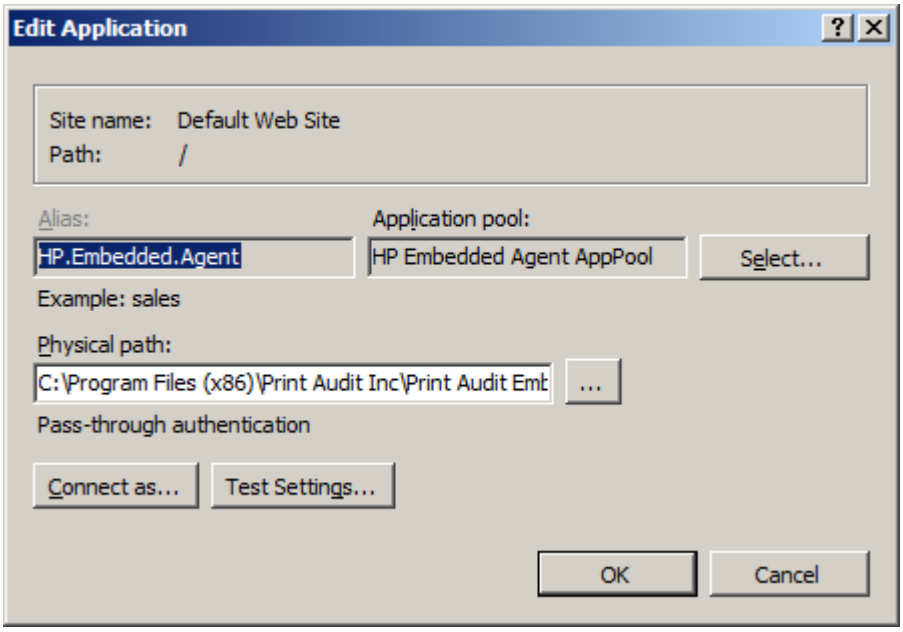
The Print Audit Embedded for HP creates two web sites under "Default Web Site" by default - HP.Embedded.Agent and HP.Embedded.App

To verify the Application pool used by a site:

1. Open the Internet Information Services (IIS) Manager.



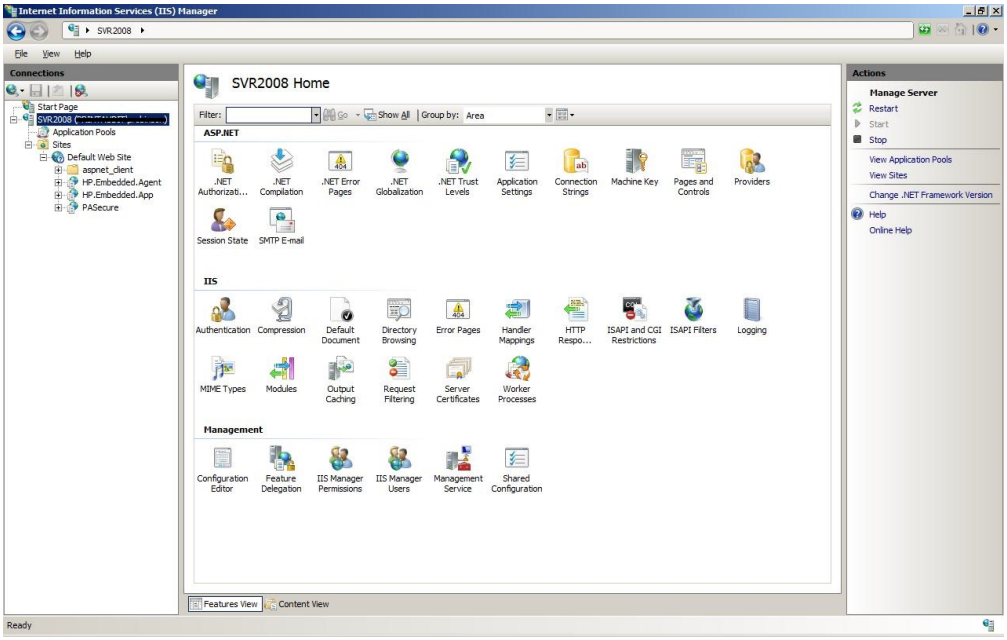
2. Locate the web site under "Sites" and highlight it. By default, the Print Audit Embedded for HP sties are under "Default Web Site".
3. Under "Action" (located on the right hand side of the IIS Manager), click on "Basic Settings..."



Verifying ASP.NET Restriction

The Print Audit Embedded for requires .NET Framework version 4 which may need to be enabled to work with IIS.

1. Open the Internet Information Services (IIS) Manager.
2. Click on the icon "ISAPI and CGI Restrictions"



3. Highlight the .NET versions that are set to "Not Allowed" and click on the "Allow" link under " Actions".

Embedded for Konica Minolta Documentation

Print Audit Embedded installs directly onto supported Konica Minolta OpenAPI-enabled multifunction peripherals, allowing users to control and recover all printing, copying, faxing and scanning costs. Review the documentation below for help installing and configuring Print Audit Embedded. You can also use the Knowledge Base to find more information.

Browse Documents:

Collapse allExpand all Collapse all

Browse Other Product Documentation:

Print Audit 6 Infinite Device Management Print Audit Secure Rapid Assessment Key Embedded for Sharp

Embedded for Kyocera Mita Embedded for Lexmark Embedded for Xerox Embedded for HP

Copy Audit Touch Copy Audit Numeric

Embedded for Konica Minolta Install and Setup

Print Audit Embedded for Konica Minolta is used alongside Print Audit 6 to provide authenticated access to Konica Minolta MFPs, for the purpose of securing device functionality, and tracking usage. Users can be required to authenticate at the MFP by login, PIN, or card swipe identification before they may access MFP functions.

When additionally used in conjunction with Print Audit Secure, users will also be able to select and release secure print documents directly from the MFP panel.
This guide provides instructions to install and configure Embedded for Konica Minolta with Print Audit 6.

When used with Print Audit 6, Embedded for Konica Minolta will track:

- walk-up copying
- scanning
- faxing
- printing from the document server

When Print Audit Secure is added, Embedded for Konica Minolta can additionally provide:

- Secure release of all printing
- Follow Me printing

Components

Embedded for Konica Minolta consists of two main components:

1. Print Audit 6 - Embedded for Konica Minolta Configuration:

Embedded for Konica Minolta is configured using the Embedded Systems plug-in for the Print Audit 6 Administration tool. Support for Embedded for Konica Minolta exists in Print Audit 6.11 or newer.

2. Embedded Client:

This software is installed on a Windows web enabled server while the embedded application runs on the MFP's embedded web browser. The Embedded Client provides a user interface directly on the panel of the Konica Minolta MFP to enable the tracking of copies, scans or faxes, or the printing of documents stored in the MFP's Document Server.

In addition to tracking the number of pages in a copy, scan, fax, or print job, the Embedded Client tracks additional information about the job. For example, the Embedded Client can request a PIN Code from the user to identify and track who is creating the photocopy. Or, it can request a Client Code to identify which customer or cost center should be billed for a fax transmission.

Print Audit 6

Print Audit 6 is a client application that tracks all printing directly from the desktop where the print job was issued. Every job, along with its attributes, are collected and stored in the Print Audit database, where it is available for reporting on printing volume and trends.

Print Audit 6 is available in 3 different modules, Analysis, Rules, and Recovery, which respectively, enable Analysis Reporting from the collected print data, the ability to create printing rules for rules-based printing, and the ability to allocate the cost of print jobs to a user, customer, or cost center.

When used with Embedded for Konica Minolta, Print Audit 6 can also track copy, scan, and fax jobs , and jobs that are printed from the document server.

Print Audit Secure

Print Audit Secure allows for print jobs to be held on the server until an authenticated user releases them from the MFP panel, or from a Print Audit Secure release station. When

a printer is managed by Print Audit Secure, incoming print jobs are prevented from being automatically output, by holding them in a secure queue on the server. When used with Embedded for Konica Minolta, users will authenticate at the MFP, view their held jobs on the MFP panel, select one or more jobs and release or delete them directly from the MFP front panel.

Authentication Devices

Print Audit Embedded for Konica Minolta supports Authentication Devices, such as swipe card or proximity card readers, within an Embedded for Konica Minolta environment. When an authentication device is configured in an environment with Embedded for Konica Minolta, users must authenticate at an authentication device before they are allowed to access the supported Konica Minolta MFP controlled by the device.

Please note: Card reader configuration and installation should only be performed by a qualified Konica Minolta copier technician.

Supported Card Readers

Please contact your Konica Minolta dealer for a list of supported card readers on your Konica Minolta MFP.

Licensing

To enable the Print Audit Embedded for Konica Minolta the following is required:

1. **One Print Audit Embedded for Konica Minolta license per controlled Konica Minolta MFP** - Print Audit Embedded for Konica Minolta is licensed on a per-MFP basis. To install Embedded for Konica Minolta on 15 MFPs, licenses must be purchased for each of the 15 MFPs. MFP licenses can be purchased as part of any Print Audit license, and are additional to the Print Audit 6 client licenses needed to track print jobs originating from Microsoft Windows and Apple Macintosh workstations. In the event that there are insufficient licenses, Print Audit will stop tracking some or all of the MFPs—MFPs will continue to function as normal, but no information will be tracked.
2. **Konica Minolta MFPs** - Print Audit Embedded for Konica Minolta is only supported on OpenAPI v4.
3. **Print Audit 6.11 or higher** - Print Audit Embedded for Konica Minolta requires Print Audit 6 to configure the MFPs. Consult the Print Audit 6 Installation Guide for more information.

Optional

1. **Print Audit Secure 1.3.x or higher** - Consult the Print Audit Secure Installation instructions for more information
2. **One Authentication Device per Konica Minolta MFP** - Print Audit Embedded for Konica Minolta supports HID proximity and contactless smart cards for authentication. Users can enter validation data by presenting the card at the card reader. If any authentication devices are to be used in the environment, one authentication device is required per MFP. *Please note that card reader installation should only be done by a qualified Konica Minolta copier technician as per Konica Minolta's documentation and best practices.*

1. Installation - Embedded for Konica Minolta

This section only addresses the installation requirements and configuration of Print Audit 6 for use with Embedded for Konica Minolta. For complete instructions on installing and configuring Print Audit 6, please refer to the Print Audit 6 Installation information found online. Refer to that documentation to perform the following steps to install Print Audit 6 in conjunction with Print Audit Embedded for Konica Minolta.

System Requirements

- **Windows Server 2008 R2 or newer** - requires Internet Information Services 7 or better.
- **MS-SQL Server 2005 Express or better -** running embedded applications on with an Access database is not recommended.
- **Print Audit 6.11.0 or newer**

- Download the latest version from h ttp://www.printaudit.com/software-updates.asp .

- **Microsoft .NET Framework v4.0**.
- **Internet Information Services (IIS)**.
- **Windows Communication Foundation**.
- **HTTP Activation enabled.**

Device Requirements

- **The devices needs to have the I-Option LK101 upgrade kit installed.**
- **Support OpenAPI v4.**
- **Must have a hard drive.**
- **Web browser enabled.**
- **OpenAPI enabled.**
- **SSL enabled.**
- **Allow unauthenticated print outs**

Optional

- Print Audit Secure 1.3.x is supported with Embedded for Konica Minolta.

Before you Install

- Print Audit Embedded for Konica Minolta will run on Konica Minolta devices with the above devices requirements met.

Steps to Install

1. (Optional) If using a swipe/proximity card reader for authentication, it is recommended that the reader be installed and configured first by a qualified Konica Minolta copier technician.
2. Obtain a Print Audit Embedded License for each MFP you need to install on.
3. Install and configure Print Audit 6 with the appropriate licensing.
4. Download the Konica Minolta Embedded Application from the Print Audit web site.
5. Configure the Konica Minolta device using the Web Interface.
6. Add the Konica Minolta device to the Print Audit Administrator.
7. Run the Konica Minolta Embedded Application package.

8. Register the Application.
9. Configure Print Audit 6 for use with Embedded for Konica.
10. Verify operation and tracking of the MFP.

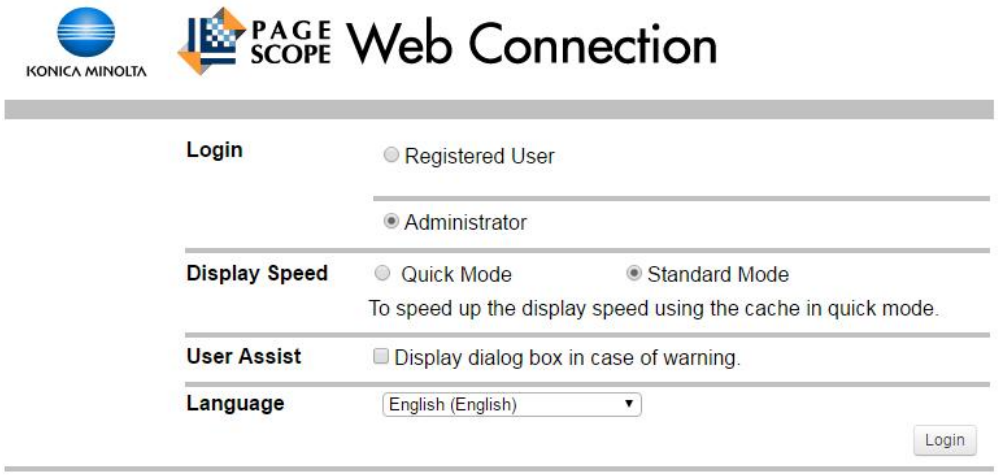
Installation Walkthrough

Before you begin the installation, check to make sure that both IIS and .Net have been installed as per the System Requirements.

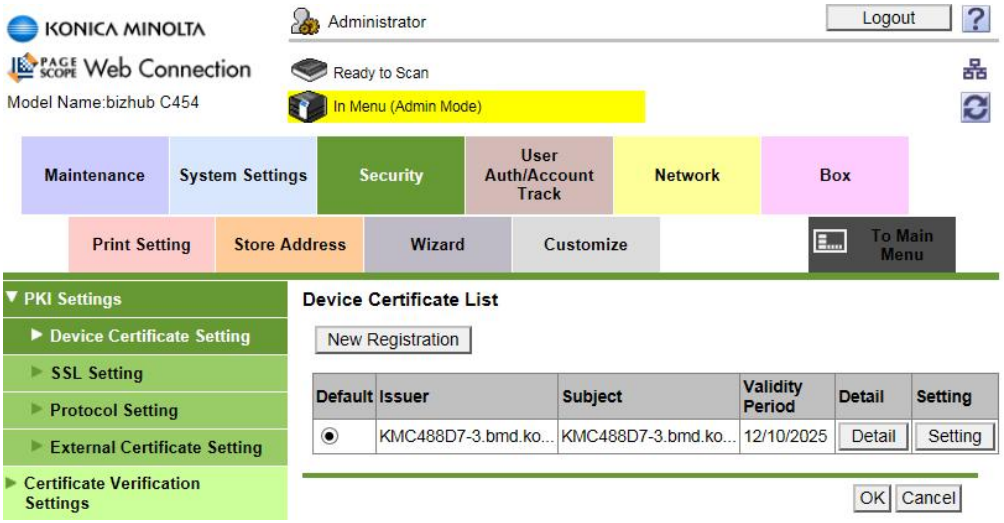
Configuring the Konica Minolta device using the Web Interface*

***Please not that the Konica Minolta web interface images may not match all MFP models.**

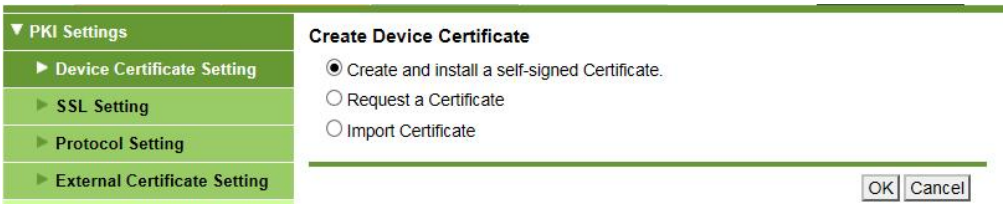
1. Log on as administrator on the device's web interface using the device's IP address using a web browser.



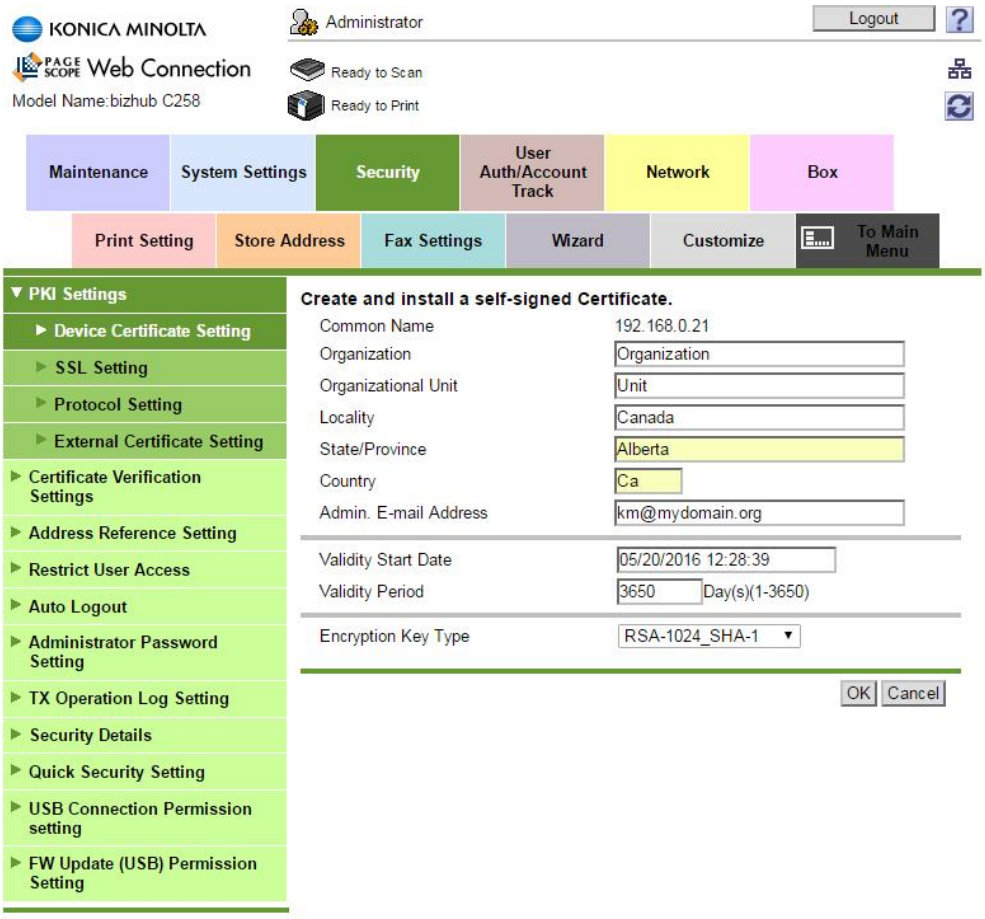
2. Select Security --> PKI Settings.



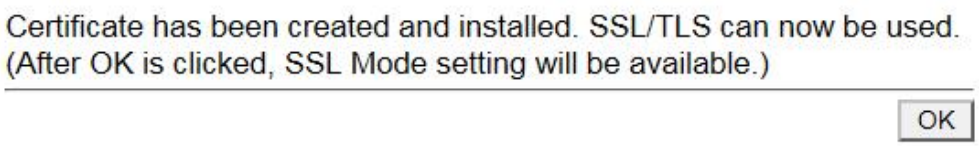
3. Create a new certificate by clicking New Registration -> Create and register a self-signed certificate.



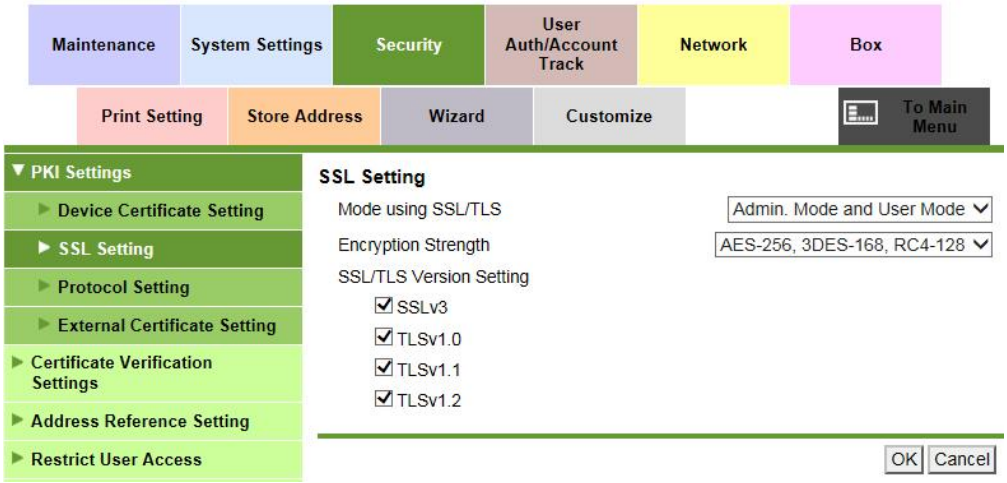
4. Fill in the fields with the appropriate information. Set the Validity Period 3650 Days (10 years) . Click OK



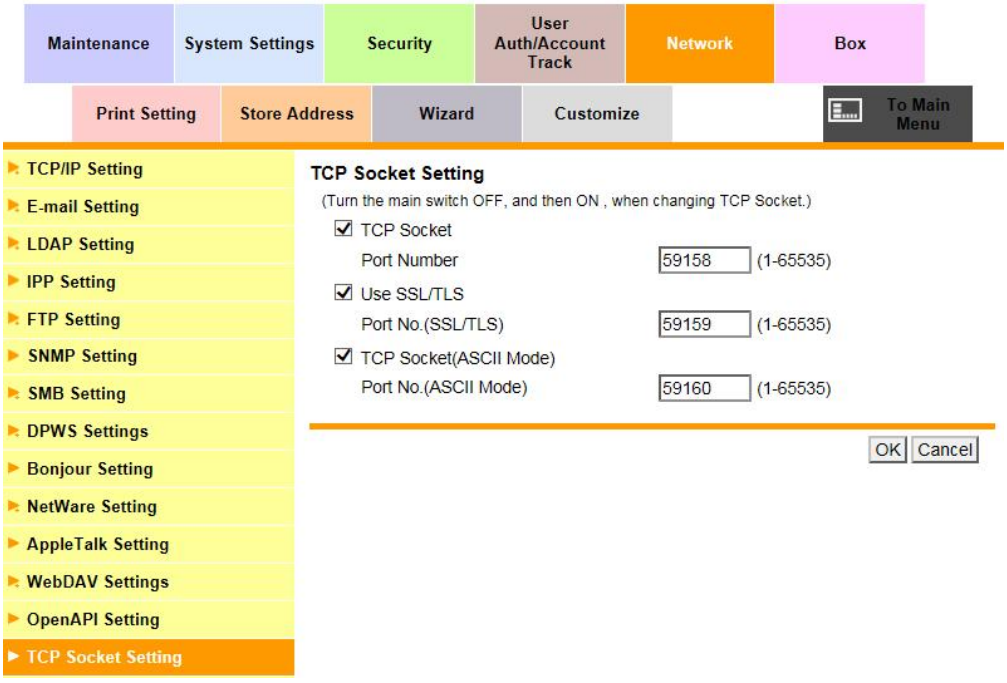
5. Click OK again.



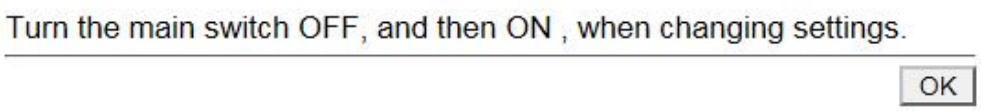
6. Log into the device web interface as administrator again. In the “Security” section display the “PKI Settings” subsection and from the menu on the left, choose “SSL Setting”. Change “ Mode using SSL/TLS” to “Admin Mode” or “Admin Mode and User Mode” (on some machines : just “enable”). Your web browser will re-logon to the web server under “https” mode.



7. Under Network -> TCP Socket Setting tick all checkboxes.



8. Press OK and then reboot the device when prompted to do so.

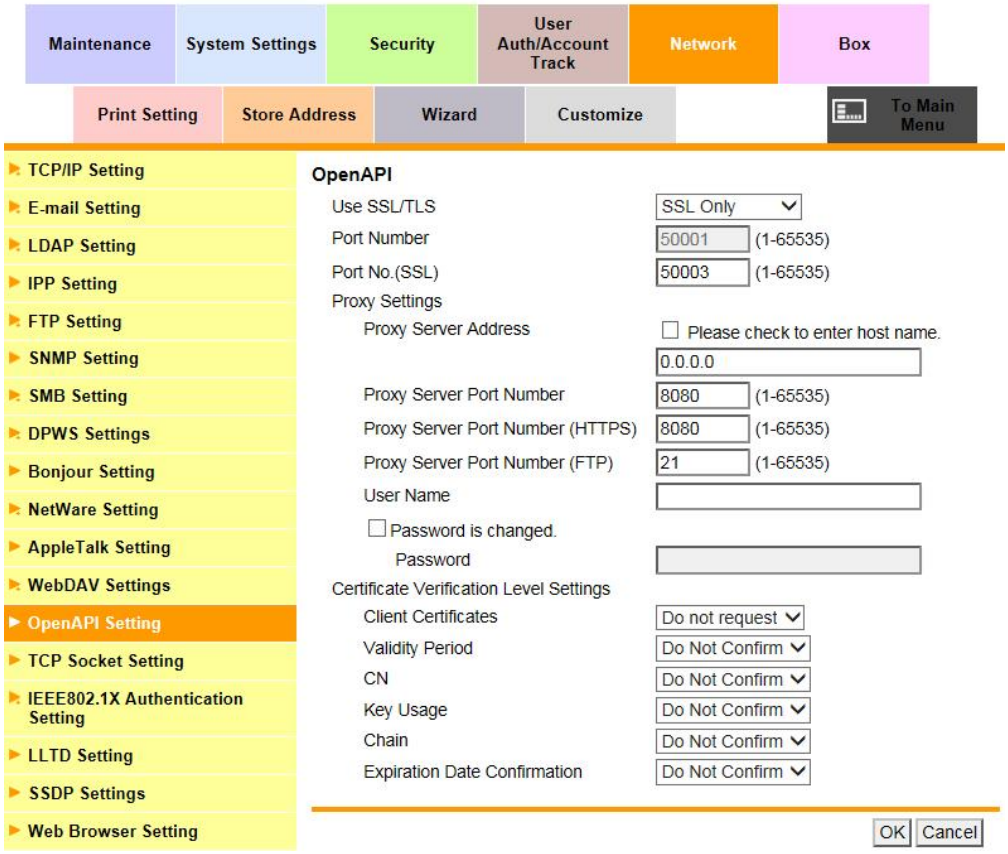


9. Log back into the administrator web interface then select Network -> OpenAPI Setting and make the following changes:

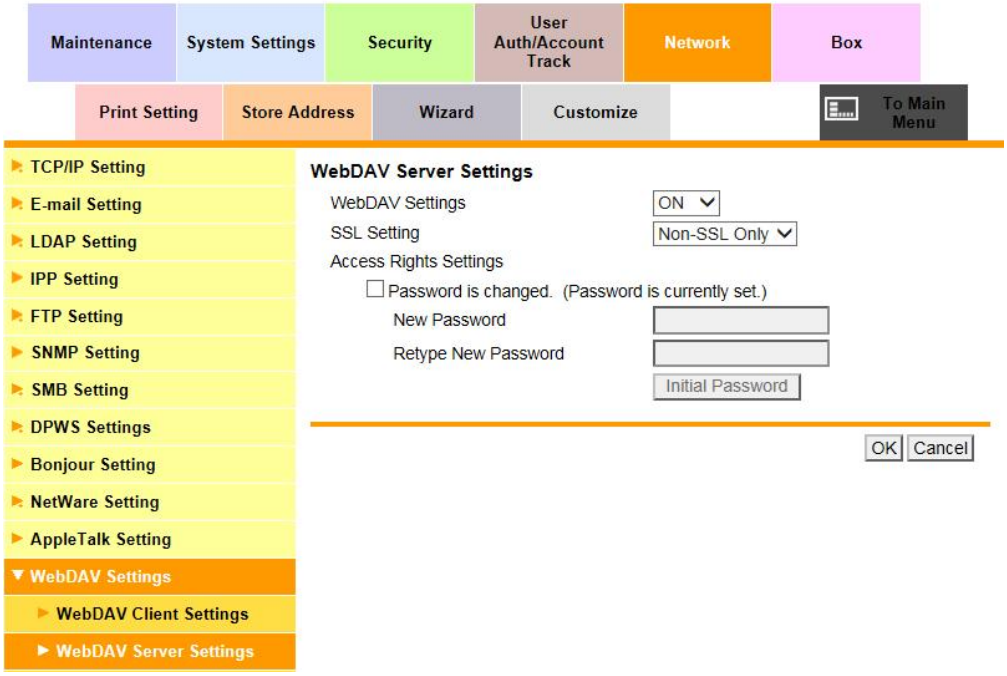
a. Set Use SSL/TLS to SSL Only.

b. Set Port No. (SSL) to 50003.

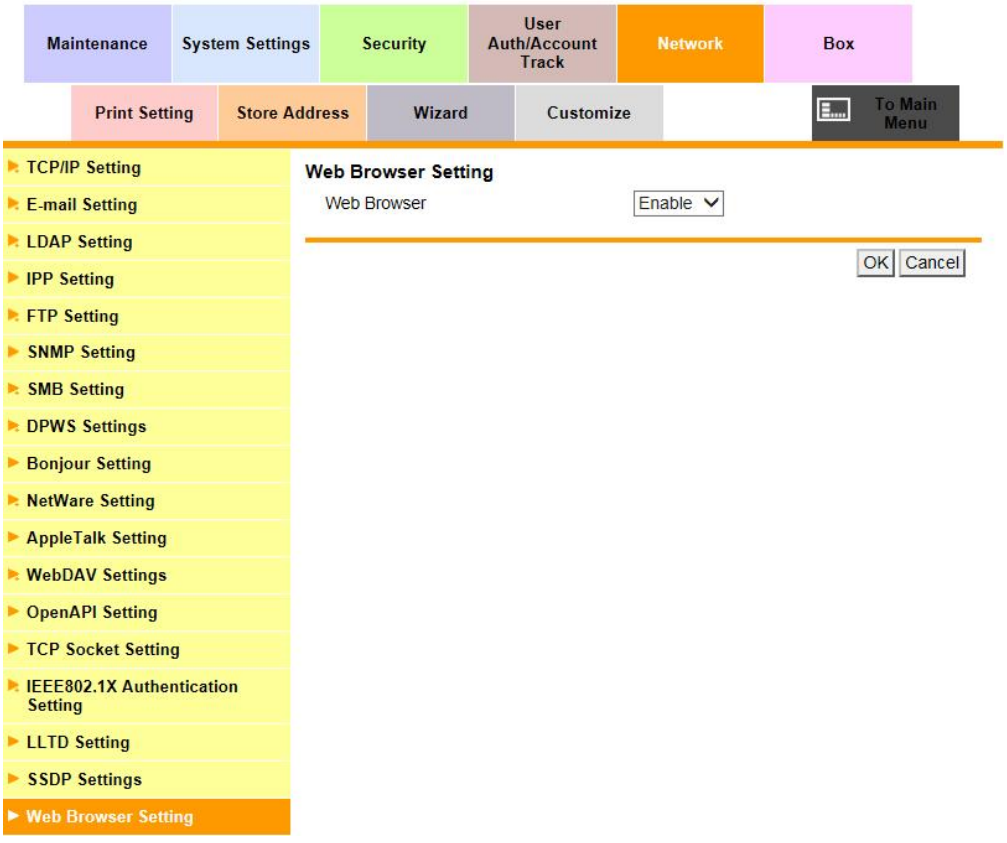
c. Set all Certificate Verification Level Settings to Do Not Confirm and the Client Certificates to Do Not Request.



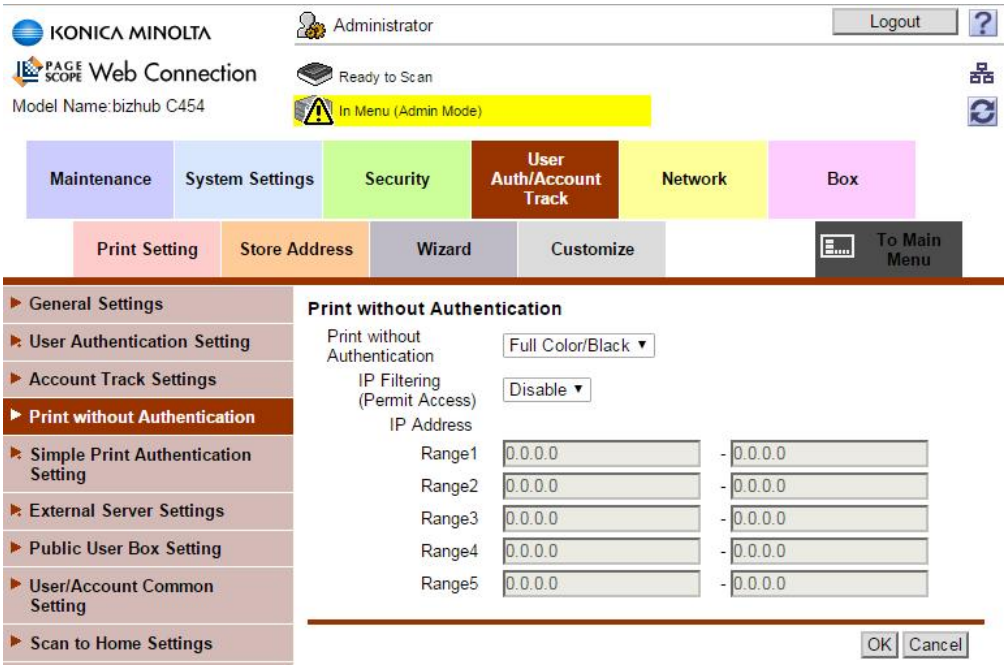
10. Select Network -> WebDAV Settings -> WebDAV Server Settings. Make sure WebDAV Settings is set to ON.



11. Enabled the web browser on the device through Network -> Web Browser Setting. Set Web Browser to Enable and press OK.



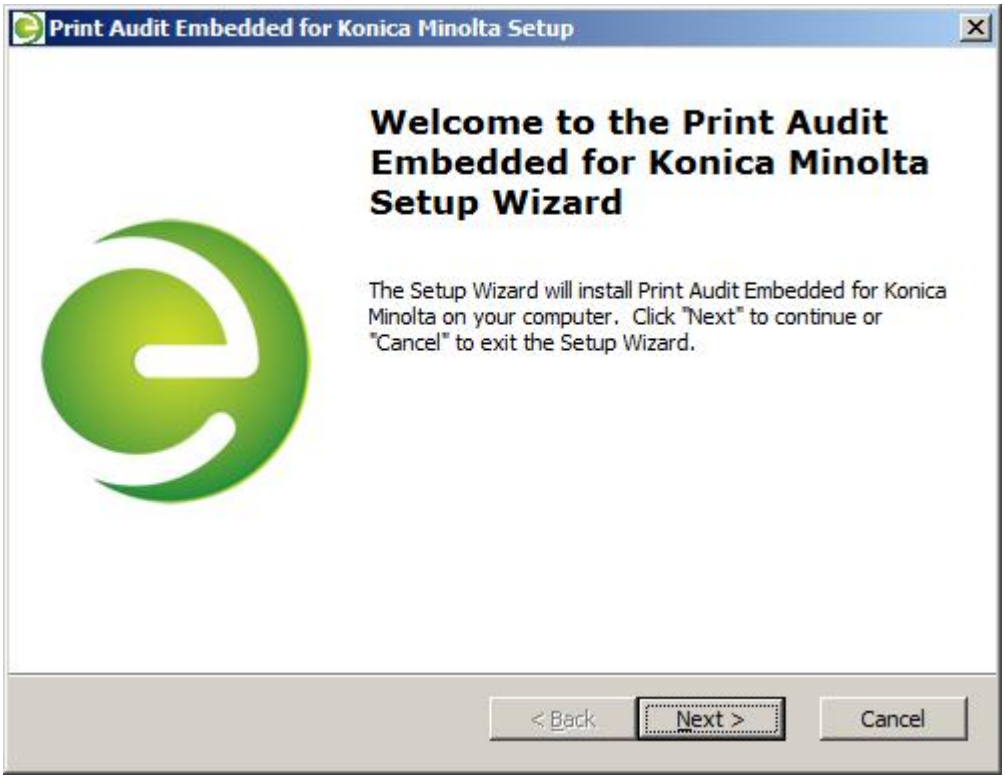
Browse to User Auth/Account Track ->Print without Authentication and set Print without Authentication to Full Color/Black and press OK.



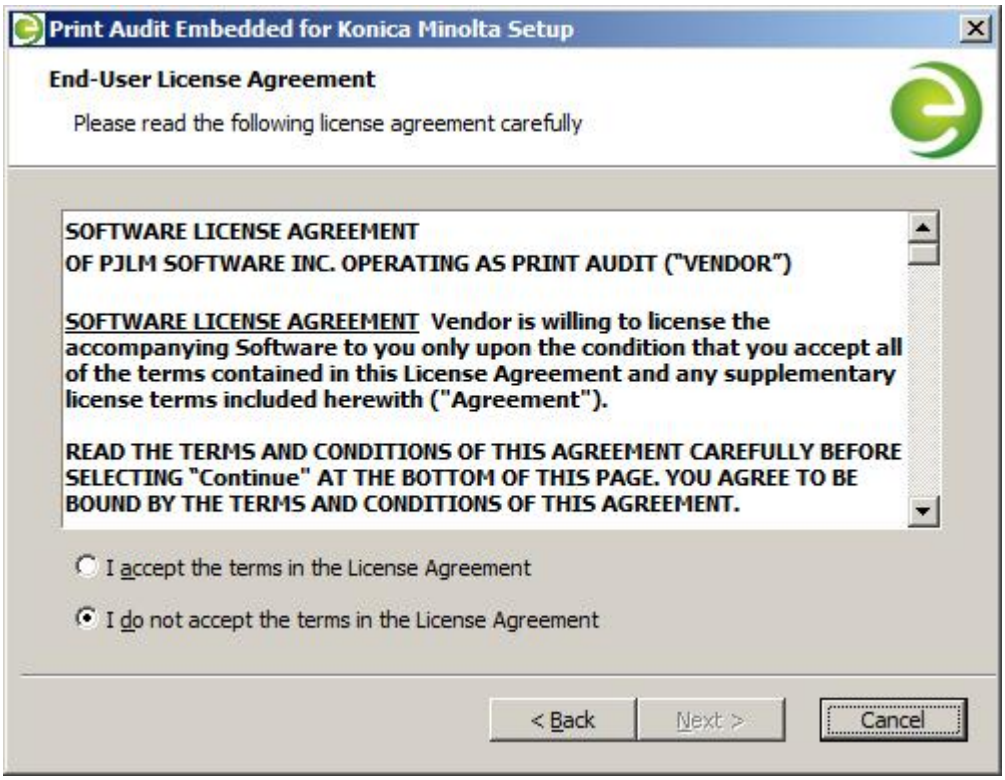
Installing the Print Audit Embedded for Konica Minolta installation package on the server.

The installation package has a wizard like user interface that will guide you through the installation process.

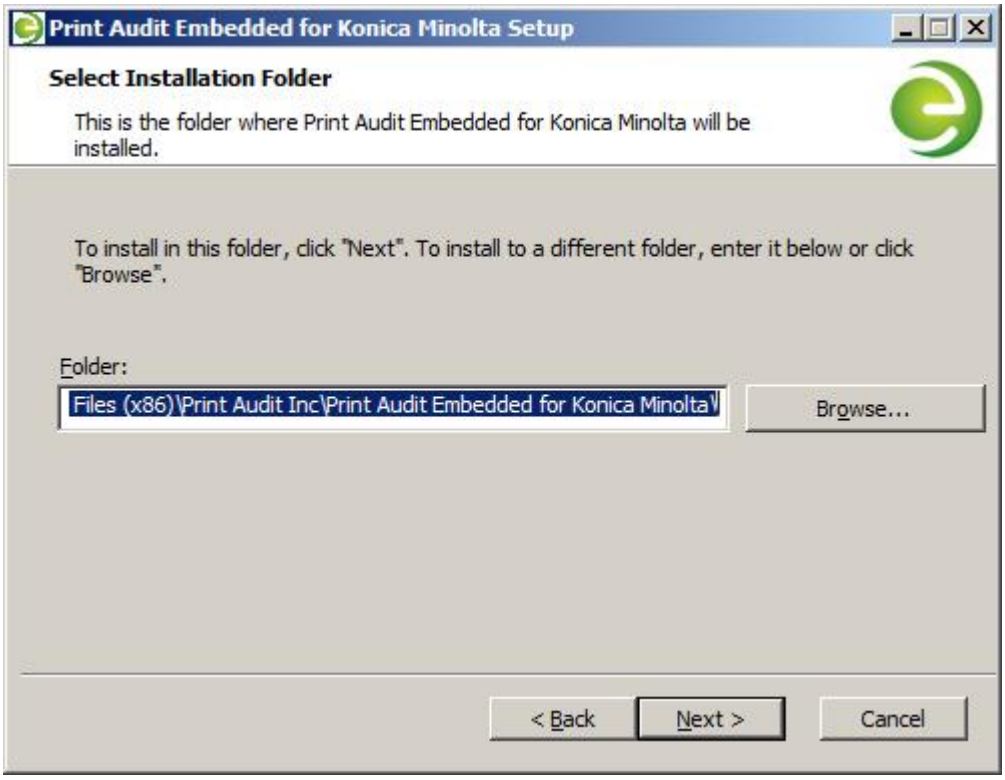
1. Double click on the Print Audit Embedded for Konica Minolta setup to begin the installation.
2. On the "Welcome to the Print Audit Embedded for Konica Minolta Setup Wizard", click Next.



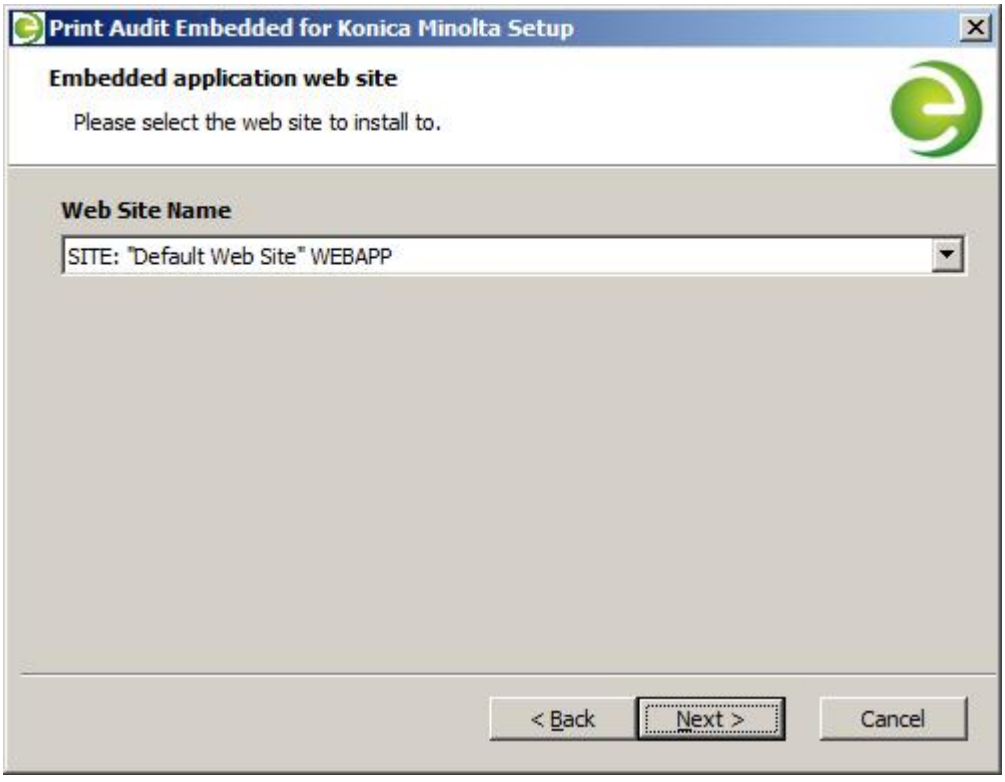
3. Read the End User License Agreement and select the checkbox if you accept. Click Next.



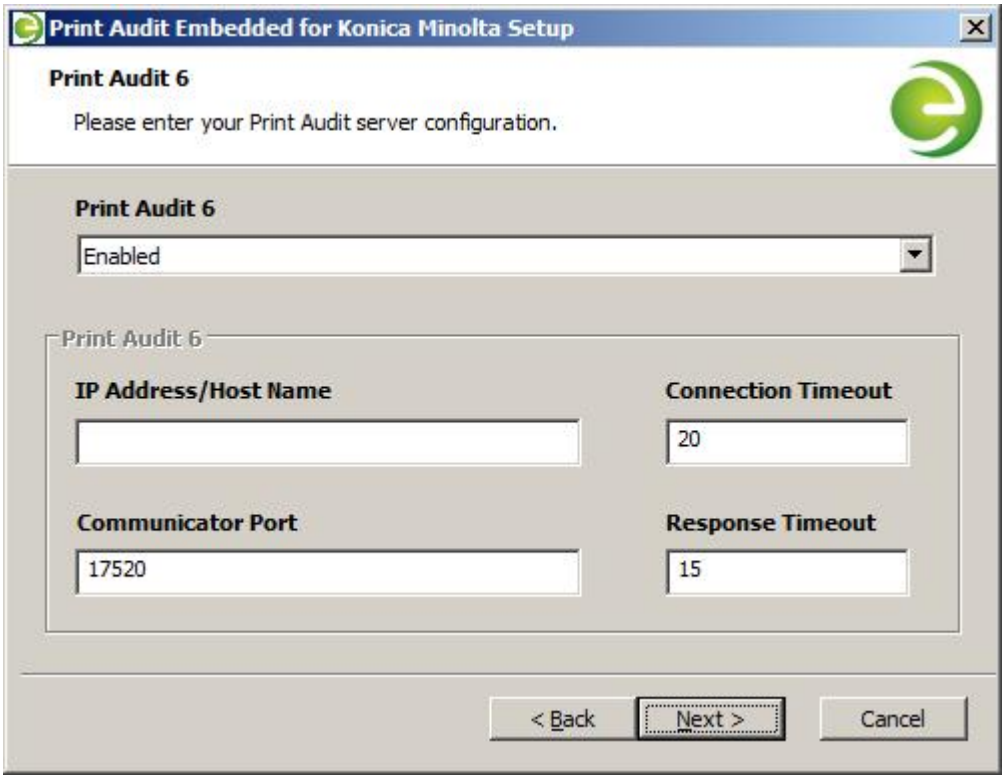
4. Select the install location. A default location will be available to you. Click Next when finished.



5. Select the Website name where the Embedded for Konica Minolta web service will be created. It is recommended to use the Default Web Site. Click Next.



6. Enter the Print Audit 6 configuration details. Click Next when finished.



a. From the dropdown box, choose Enabled or Disabled to enable/disable the Print Audit Embedded for Konica Minolta application for use with Print Audit 6.

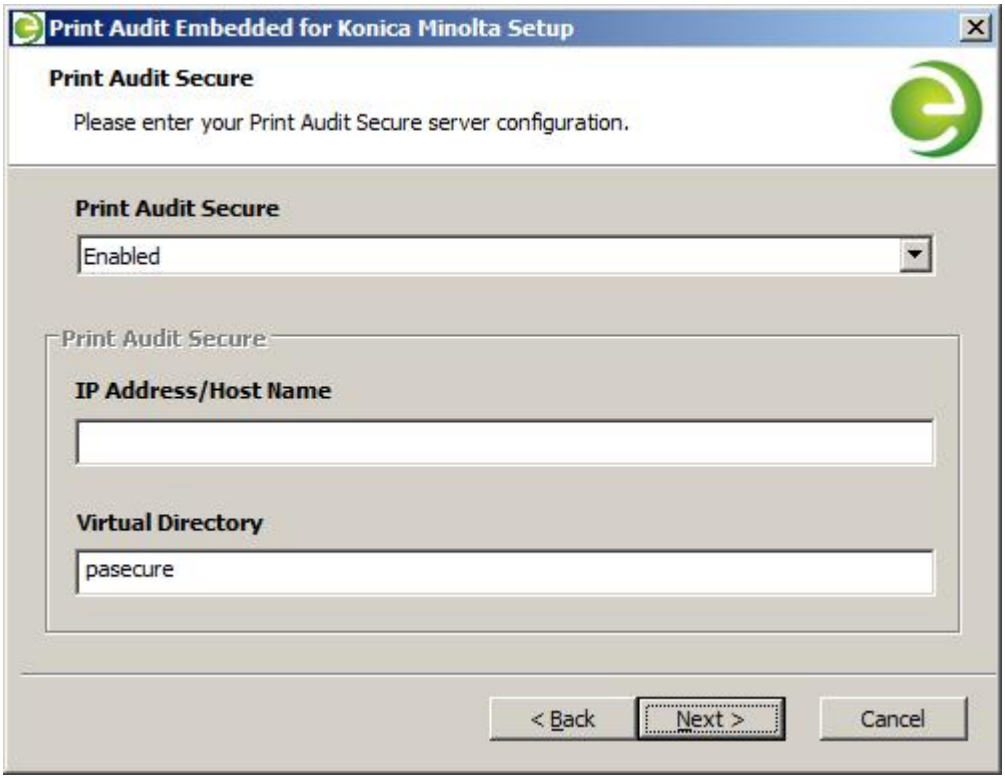
b. IP address/Host Name - the IP Address or Host Name of the server running the Print Audit 6 Database Communicator.

c. Communicator port - the port number the Database Communicator is set to listen on. The default is 17520.

d. Connection Timeout - the time in seconds that the Print Audit Embedded for Konica Minolta application will wait before a connection to the Database Communicator fails. The default is 20 seconds.

e. Response Timeout - the time in seconds that the Print Audit Embedded for Konica Minolta application will wait before a response from the Database Communicator before failing. The default is 15 seconds.

7. Enter the Print Audit Secure Server details. Click Next when finished.

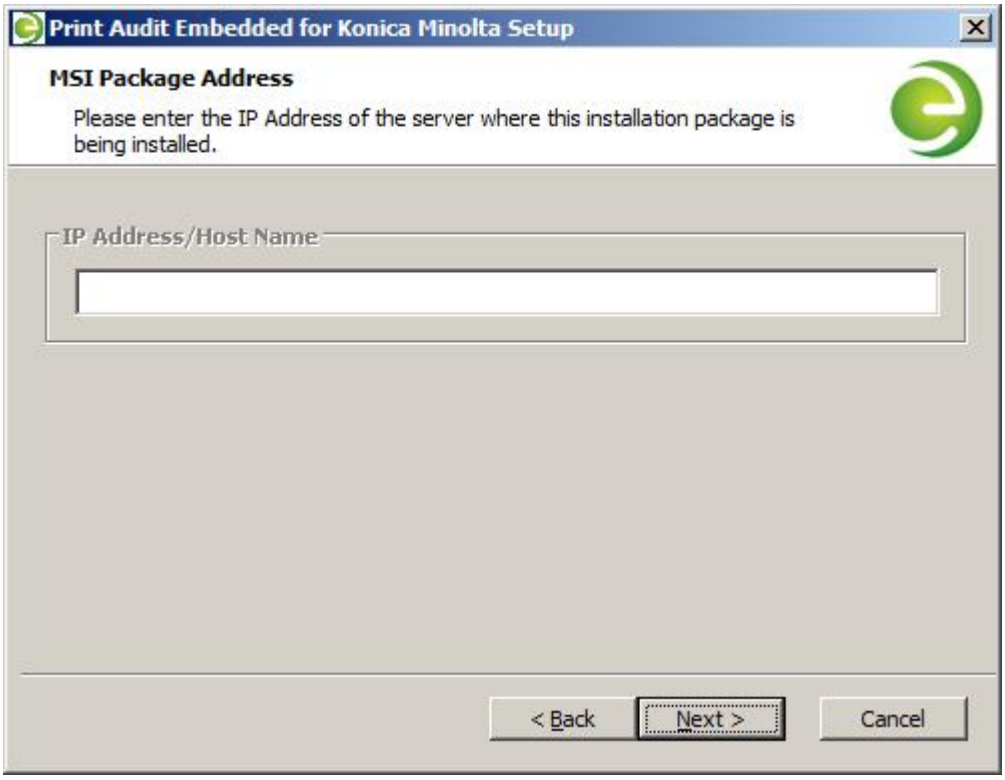


a. From the dropdown box, choose Enable or Disabled to enable/disable the Print Audit Embedded for Konica Minolta application for use with Print Audit Secure.

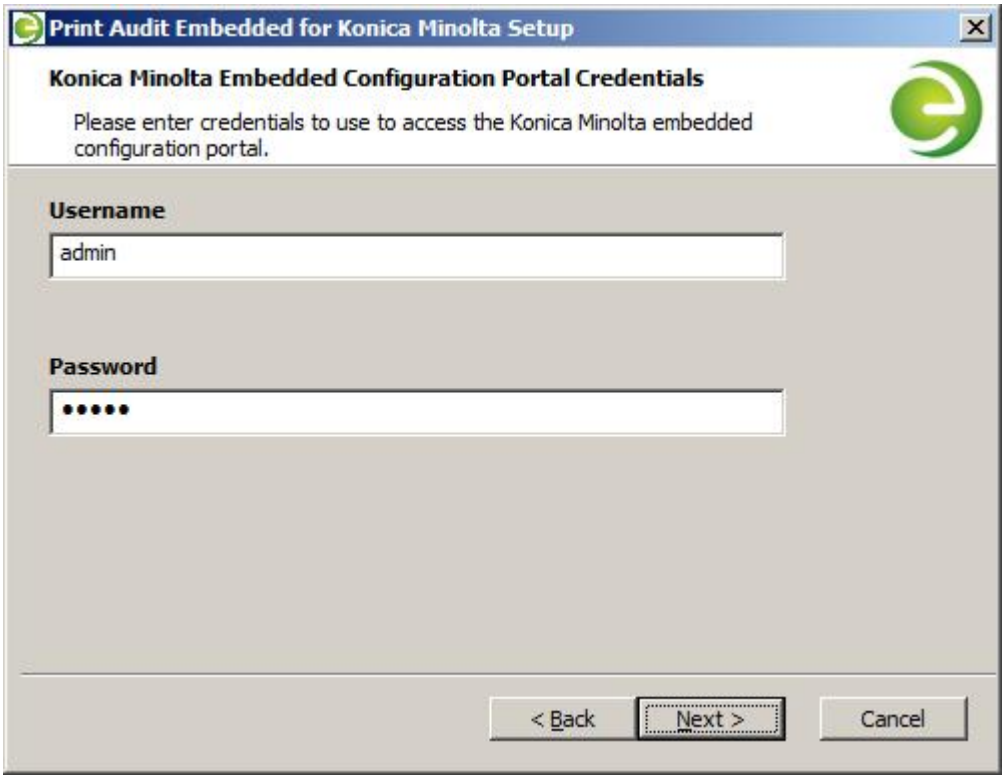
b. IP Address/Host Name - the IP Address or Host Name of the server running the Print Audit Secure Server.

c. Virtual Directory - the name of the virtual directory configured on the Print Audit Secure Server. The default is "pasecure".

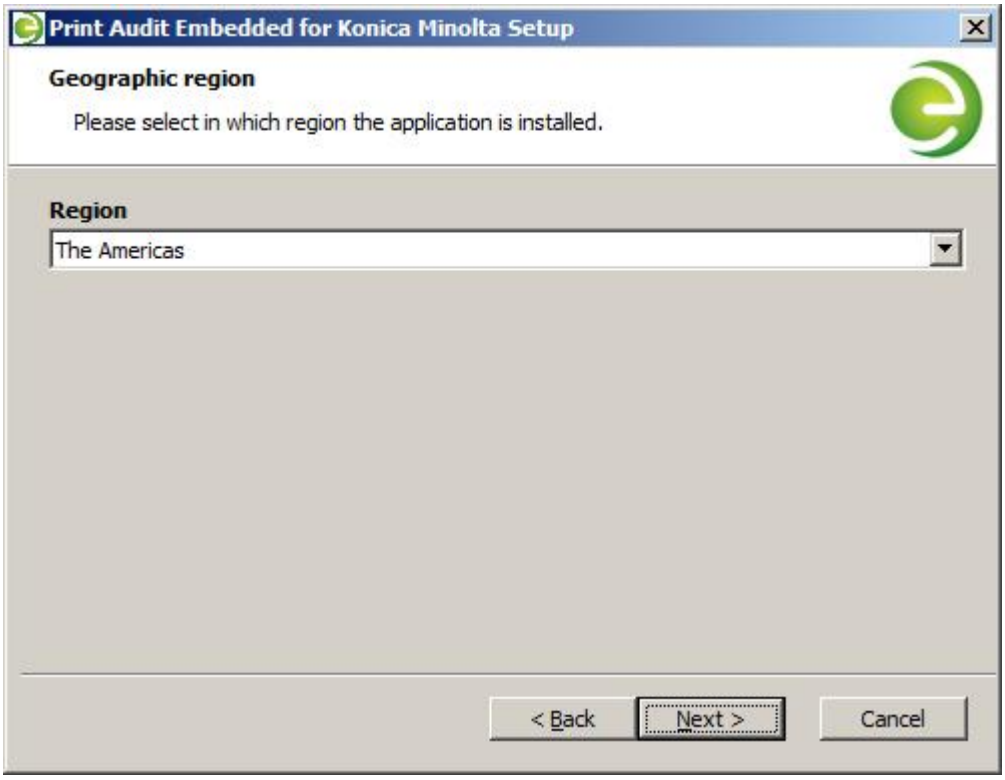
8. Enter the IP Address/Host Name where the installation package is being installed from and click Next when finished.



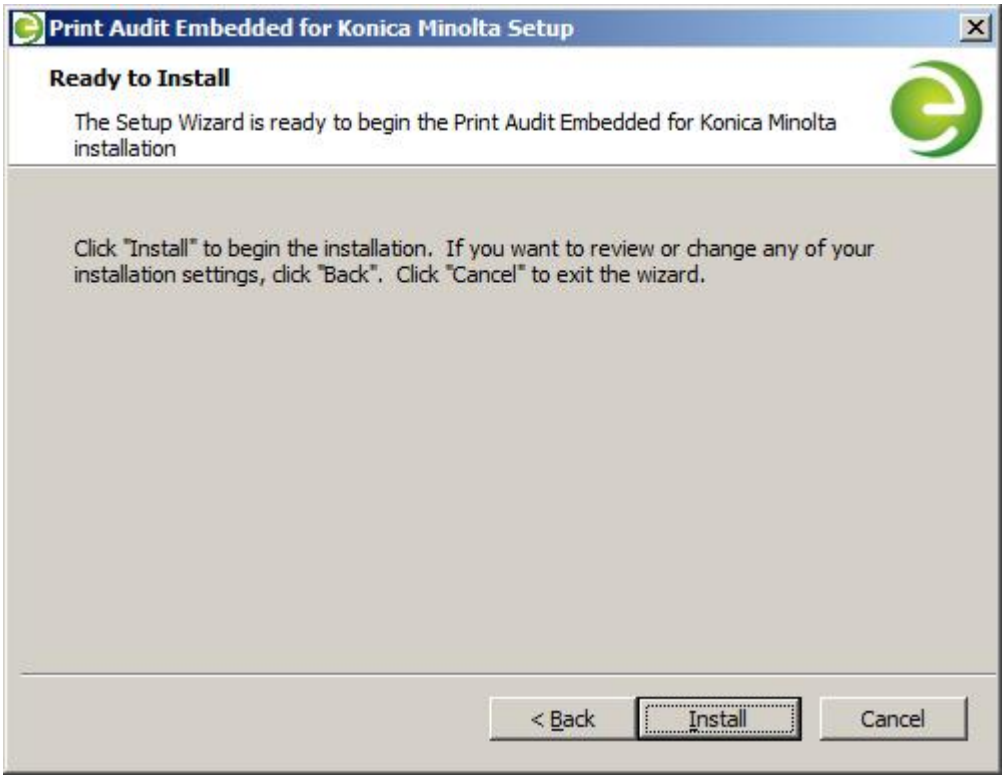
9. Enter the credentials used to access the Print Audit Embedded for Konica Minolta configuration portal and click Next when finished.



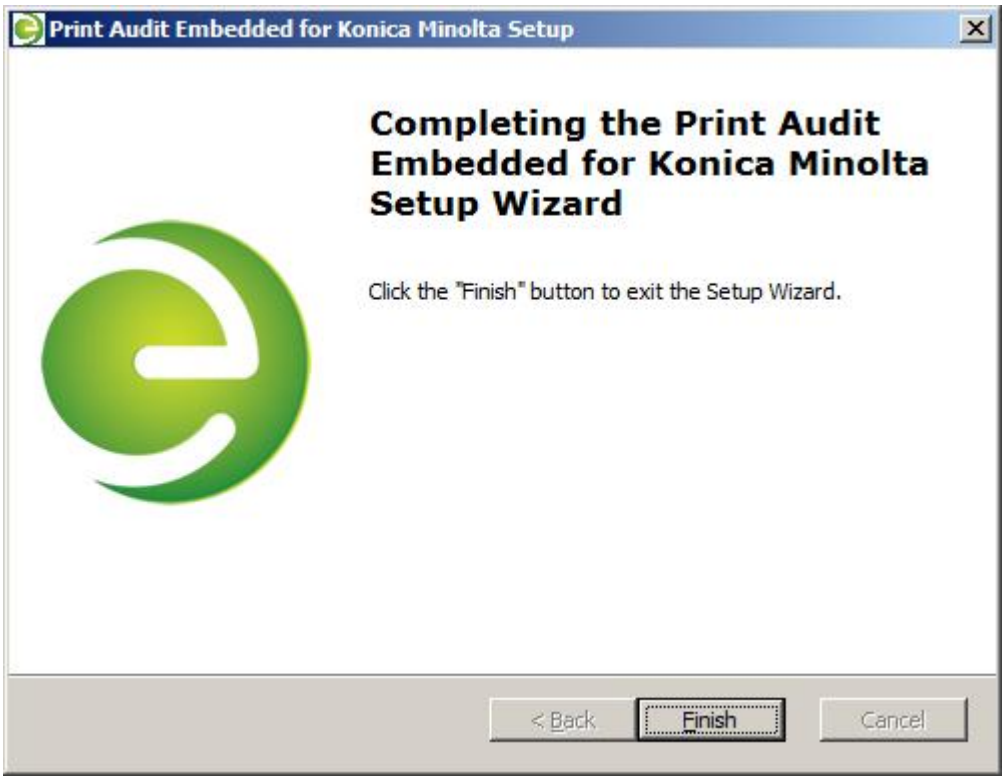
10. Select the appropriate Geographic region and click Next.



11. Click Install to begin installing Print Audit Embedded for Konica Minolta. The installation may take a few minutes to complete.



12. When the installation is complete, click Finish.

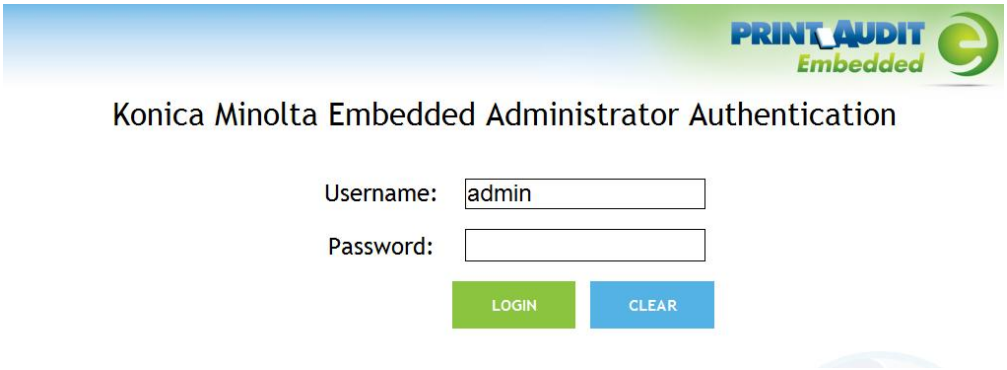


13. (Optionally) verify that IIS settings are correct. See the IIS Configuration/Setup for Print Audit Embedded for Konica Minolta section in this document.

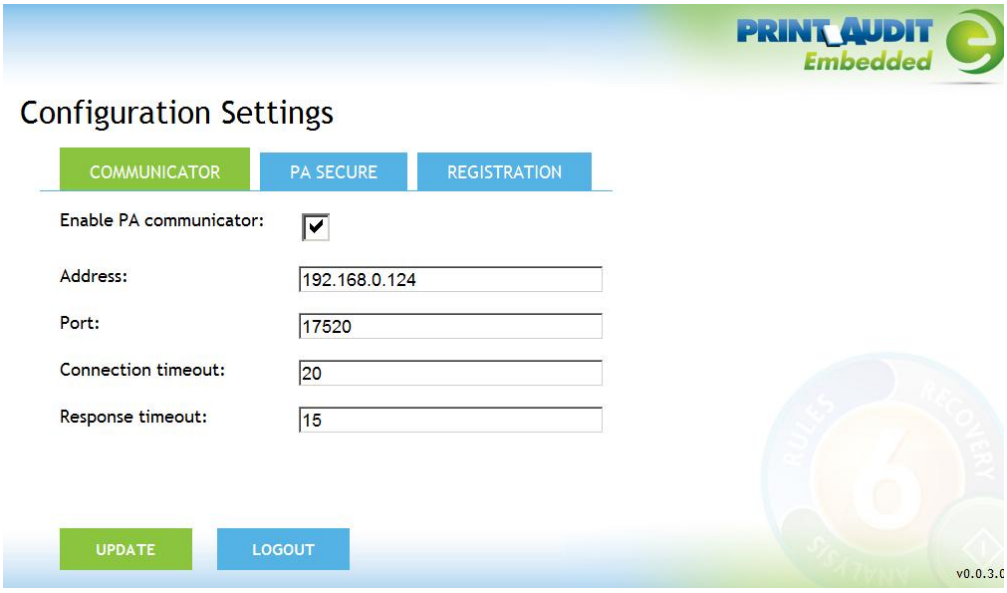
Deploying the Print Audit Embedded for Konica Minolta application to MFPs.

1. On the server desktop there should be a short cut named Konica Minotla *Embedded Configuration.* Open it by double clicking on it. The short cut opens a web page with the following URL; http://localhost/KM.Embedded.App/Config

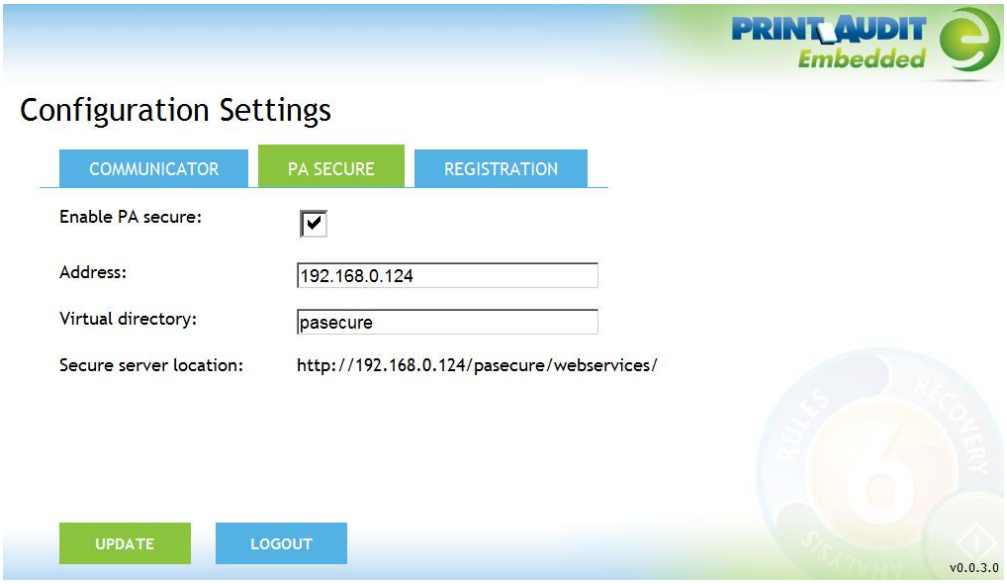
2. Enter the Konica Minolta Embedded Configuration Portal credentials to authenticate and click "Login". The credentials are the same as those used to access the Konica Embedded configuration portal.



3. Once authenticated three tabs will appear:
    - Communicator
    - PA Secure
    - Registration
4. Communicator is where settings related to Print Audit 6 are set. If Copy, Scan and/or Fax tracking are to be used select 'Enable PA Communicator'. Configure the IP Address or Hostname and port for the server running the Database Communicator Service. Click Update to commit changes.

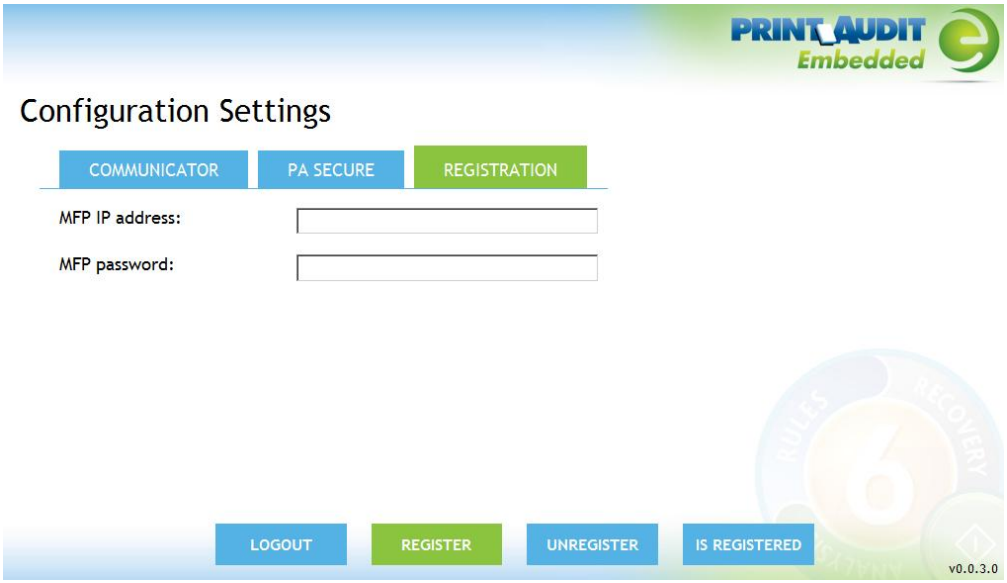


5. Click on the PA Secure Tab. *This* is where settings related to Print Audit Secure are set. If using the Print Audit Secure functionality select 'Enable PA Secure'. Enter the IP address or Hostname of the system hosting the Print Audit Secure Server. Click Update to commit changes.
   **Note: pasecure is the default virtual directory for a Print Audit Secure server.

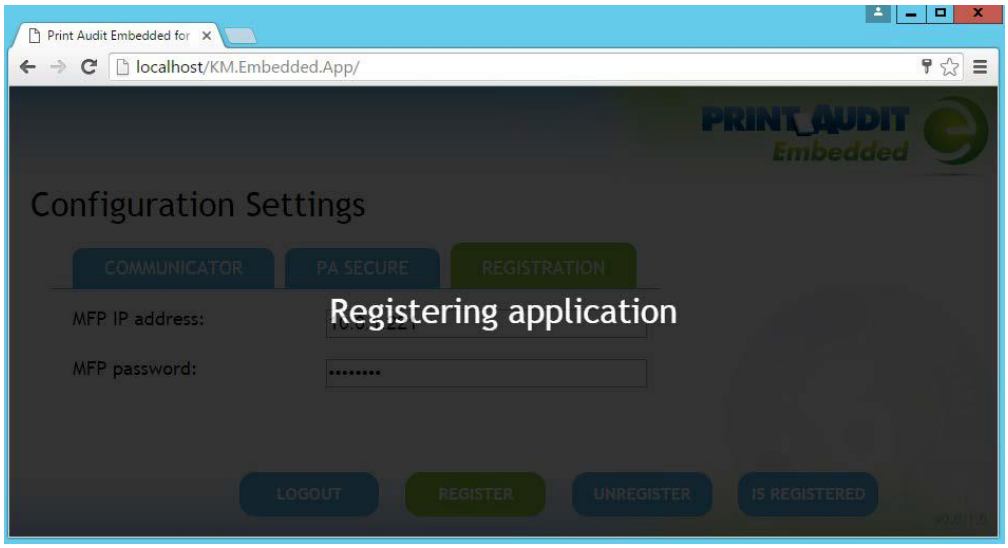


6. Click on the Registration Tab. Registration permits the administrator to perform different tasks regarding the embedded application. These are:
   - Register, deploys the application on to a device.
   - Unregister, removes the deployed application from a device.
   - Is Registered, checks the current status of the deployment of a device.

To register the application with the Konica Minolta device, enter the IP address and the administrative password for the unit. Press the Register button.



- The Registration may take some time to complete.



2. Configuration - Embedded for Konica Minolta

This Embedded for Konica Minolta window in Print Audit 6 enables the configuration of all aspects of the Embedded for Konica Minolta copier device. The different elements of the window are described below.

Pre-configuration checklist

If you are ready to begin configuring Print Audit 6 with Embedded for Konica Minolta, you have:

- Installed the Print Audit Database Communicator, Database and Administration tools to a computer on the network that will be on and available at all times. The Print Audit Client should be installed on at least one workstation, to test printing and ensure that print jobs are being tracked correctly before continuing.
- Configured Print Audit 6 for PIN codes and validated fields to be integrated into Print Audit 6 Embedded. (Optional)
- Installed the <LINK FOR Konica Minolta DOWNLOAD> software on a computer that has Internet Information Services (IIS) and .Net installed, and is acting as a web server.
- Used this guide to configure Print Audit 6 Embedded on Konica Minolta Open API enabled devices.

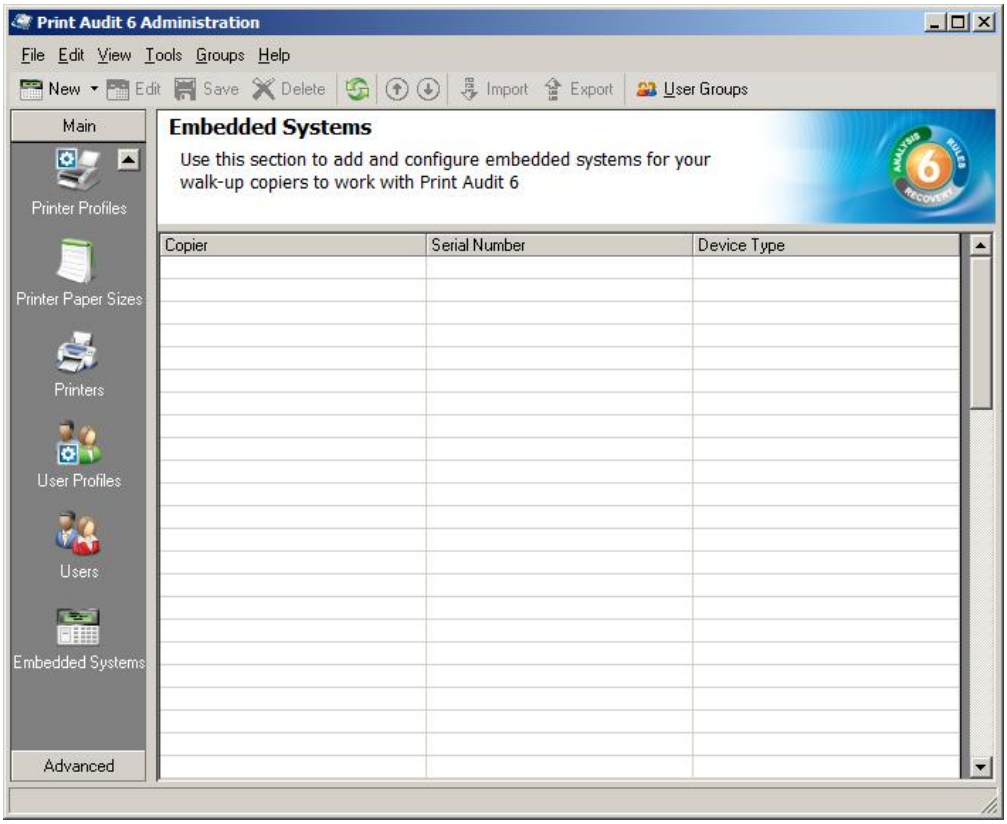
Overview

The Print Audit Administration tool provides the ability to configure Embedded for Konica Minolta on all the MFDs in the environment using the Embedded Systems plug-in. Configure one copier for every physical Konica Minolta MFD on which the Embedded Client will run.

Costs, authentication methods and custom fields may be configured for each device.

Adding, Editing and Deleting Copiers in Print Audit 6

Use the Embedded Systems section of the Administration tool to add, edit and delete Embedded for Konica Minolta copiers. A copier in the Administration tool represents a physical copier in the network.



To add a new copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Click the New button on the toolbar.
4. Select Embedded for Konica Minolta from the dropdown list of embedded applications.
5. Press OK. The Add/Edit Embedded for Konica Minolta window will appear.
6. At minimum, a copier name and the serial number of the copier must be provided. Please refer to the 'Embedded for Konica Minolta Configuration Window' section below for more information filling out the Embedded for Konica Minolta window.

7. Click the Save button. The Embedded for Konica Minolta window closes and the copier appears in the Copiers list.

To edit a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Edit button on the toolbar. The Embedded for Konica Minolta window appears.
5. Make any needed changes to the copier.
6. Click the Save button. The Embedded for Konica Minolta window closes and the copier appears in the Copiers list.

To delete a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Delete button on the toolbar. A message appears to verify removal of the copier.
5. Click the Yes button to delete the copier. The list of copiers refreshes.

Configuring the Konica Minolta MFP in Print Audit 6

This Embedded for Konica Minolta window in Print Audit 6 enables the configuration of all aspects of the Embedded for Konica Minolta copier device. The different elements of the window are described below.

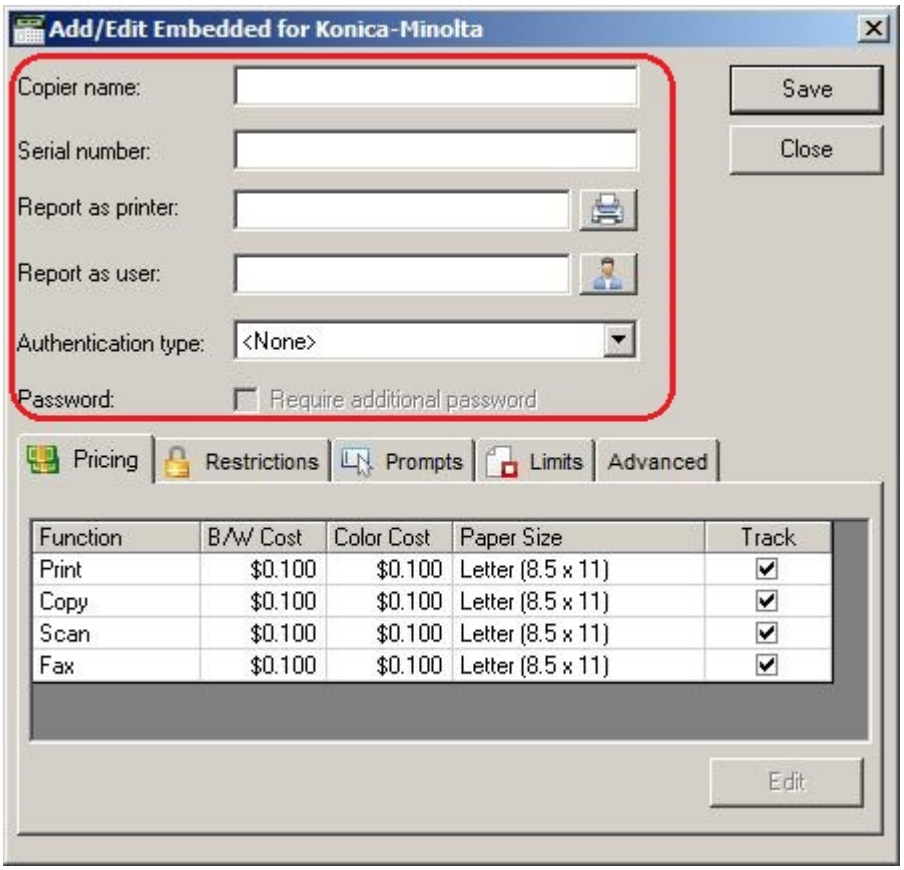
General

Copier name - The name to describe the copier. Enter a name that is descriptive enough to distinguish the copier from others. For example "Third Floor Konica Minolta".

Serial number - The serial number of the Konica Minolta MFD. NOTE: the serial number is case-sensitive and must match the serial number of the Konica Minolta MFP that the Embedded Client is installed on. To obtain the serial number, you will need to log in to the Konica Minolta

device. Typically, the serial number may be found under Device Status. The serial number may be referred to as the Engine Serial Number. For assistance on obtaining the serial number, please refer to your Konica Minolta documentation as the location of the serial number may vary from model to model.

Report as printer - Use this to select an already existing Print Audit printer with which to associate the copier. For example, if there is an MFP in the office that users print to which is already in the Print Audit database, choose that MFP here for the copier so that all transactions are reported as the same printer. If a printer is not selected here, Print Audit will record transactions for this copier as the copier name.



Report as user - Use this to select an existing Print Audit user whom to associate all jobs from this copier. Use this functionality to still have individual user authentication, but for reporting purposes report all jobs to a single user.

Authentication type - Select how the user will authenticate to the copier before they can do transactions. The authentication type determines how a user identifies themselves to the copier before they can do a transaction. The following options are available:

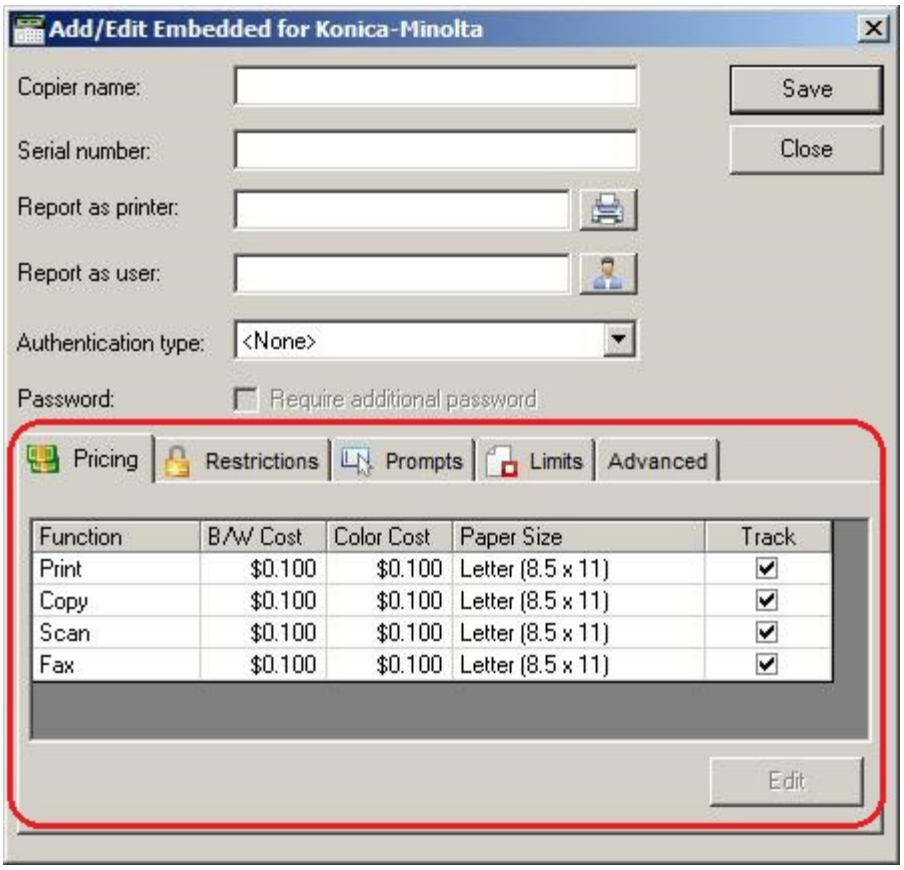
- None - Users do not have to authenticate before using the copier. All transactions are recorded to the generic Konica Minolta_Embedded user.
- PIN code - Users must enter their Print Audit PIN to access the copier.

- Card Reader - Users must use their proximity card or swipe card to access the copier
- Card Reader or PIN - Users must use their proximity / swipe card or enter their Print Audit PIN to access the copier.
- Active Directory - Print Audit Embedded for Konica Minolta can authenticate directly against an Active Directory server. When this option is selected, at least one Active Domain must be entered in the AD Domain(s) field. Multiple domains can be used if they are separated by a comma (,). When this authentication method is used, users will have to select the domain from a dropdown on the Print Audit Embedded for Konica Minolta application as well as entering their Username/Password.

Require additional password - Check this box to require the user to enter an additional (optional) password before they can authenticate using the Authentication type selected above.

Pricing tab

This tab contains the pricing for each function on the copier.



To edit the pricing for a particular function:

1. Clear the "Track" column for the function to disable the tracking of transactions of that type.
2. Select from the list the function that is to change and click the Edit button. The Configure Pricing and Paper Size Window appears.

3. Set the pricing as it makes sense for this copier in the organization.
4. Click the Done button. The Configure Pricing and Paper Size Window closes.

Prompts tab (only with Print Audit 6 Recovery)

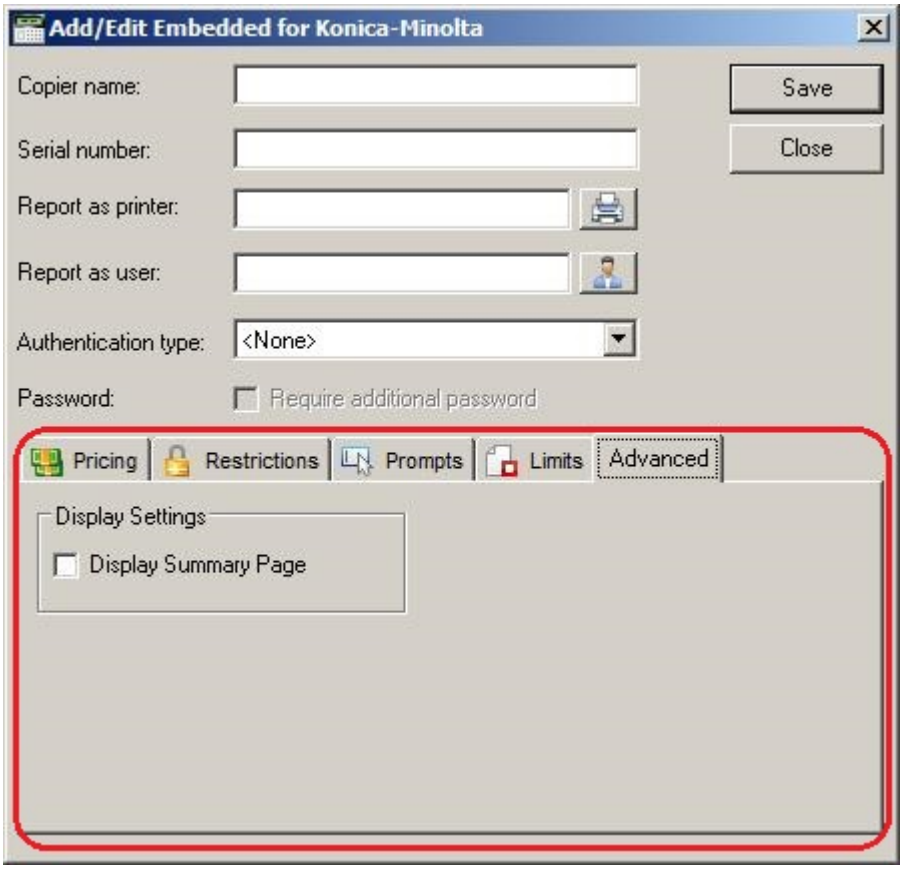
This tab is only relevant when using Print Audit 6 Recovery for the charge-back of printing.

- For each Activity the user can be required to enter values for Custom Fields. Custom Fields are setup in the Custom Fields section of the Print Audit Administrator. On this tab, select from any one of the Custom Fields configured and define a custom prompt for each one. Note: The Client Custom Field(s) must be created first before they will appear under the Prompts tab.
- Use custom fields from the user profile - Check this box to override the default custom field choices with the custom fields set in a user's User Profile.
- Allow comments - Check this box if the user can enter general comments about the job.
- Disable Exact Match - Check this box if the user can enter the custom field directly in the field and proceeds to the next step without selecting from the list.
- Custom fields - The custom fields list contains all custom fields that have been defined. To use a custom field for the activity, check the Include checkbox.

Advanced tab

This tab is used for setting the summary page display.

Check this box if you would like to view the summary page of all selected prompt / comment values.



3. Using Embedded for Konica Minolta with Print Audit 6

The Embedded for Konica Minolta Client is very easy to use. It will first prompt for required identification or billing information, before enabling the device for copy, scan, fax, or print functionality. Once the desired function is complete, return to the panel and complete the session, otherwise the MFP will timeout the session. When the session ends, the copy, scan, fax, or print transaction is sent to the Print Audit 6 database, and the Embedded Client resets to be ready for the next user.

The standard set of steps to using Embedded for Konica Minolta to track job information is as follows:

1. **Start the Transaction** - Press the Start button on the screen. The Embedded Client retrieves its configuration and proceeds to prompt for the required information. The Cancel button can be used at any time to return to the Start screen.

1. **Authenticate** - If configured to ask for a PIN Code, the Embedded Client displays a login screen. To login:

    a. Press the PIN Code button. An input form displays.

    b. Enter a PIN Code using the Konica Minolta keyboard or the touch screen.

c. Press the OK button to accept the input.

d. Press the OK button on the Login screen to validate the PIN Code.

2. **Enter Custom Field Information** - If configured to ask for Custom Field information, the Embedded Client will prompt for one or more values from the user. To enter values for a searchable field:

   a. Press the button on the touch screen that corresponds to the Custom Field Name.

   b. Enter a full or partial code on the screen and click OK.

   c. If only one match is found for the field, the Embedded Client asks for the next Custom Field value if any is configured.

   d. If Print Audit finds more than one match, a list of values will display. Use the touch screen to navigate through the values.

   e. When the desired value is found, press the button corresponding to the value. It appears highlighted.

   f. Press the OK button to accept the value.

   g. Press the OK button again to move to the next screen.

3. **To enter values for a non-searchable field**:

   a. Press the button that corresponds to the desired value. It appears highlighted.

   b. Use the arrows on the touch screen to navigate through the choices.

   c. Press the OK button to accept the value. The Embedded Client will request the next Custom Field value if any is configured.

4. **Enter any Comments** - If configured, the Embedded Client will request any Comments for the job. Press OK if to proceed without entering comments. To enter comments:

   a. Press the Comments button on the touch screen. An input form appears.

   b. Use the input form to enter comments.

   c. Press the OK button to close the input form.

   d. Press the OK button on the Comments screen to accept the comments.

5. **Verify Selections** - After all information has been input, a summary screen appears showing the current balance if any, along with the custom values selected. Press the OK button to accept the selections and begin the job.

6. **Complete the Job** - After the job is completed, press the "" (Logout)" button on the Konica Minolta MFP keypad. This completes the transaction, and transmits the job information to the Print Audit database. If the "" (Logout)" button is not used to end the session, the Konica Minolta MFP will eventually timeout the session, return to the Start screen and transmit the job information to the Print Audit database.

4. Using Embedded for Konica Minolta with Print Audit Secure

The Print Audit Secure Embedded for Konica Minolta Client is very easy to use. It will first prompt for required information. The prompts which appear are dependent on how the Secure Embedded Client is configured. Once the prompted information is provided, the device will release the secure job(s). Then the Secure Embedded Client resets to be ready for the next user. If the session is not manually finished, the Konica Minolta MFP will timeout.

Following are the standard set of steps to using Secure Embedded for Konica Minolta to release a print job.

1. Authenticate

1. **PIN Code authentication** - If configured to request a PIN Code, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Pin Code Field
    b. Enter a PIN Code using the Konica Minolta keyboard or the touch screen.
    c. Press the Login button to accept the input.
2. **Authenticate with a Username** - If configured to ask for a Username, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Username Field
    b. Enter a Username
    c. Click on the Password Field
    d. Enter a Password
    e. Press the Login button to accept the input.
3. **Authenticate with a swipe card** - If configured to ask for a swipe card, the Secure Embedded Client displays a login screen. To login:
    a. Swipe a card in a card reader attached to the MFP.

2. Release Print Jobs

1. To release all the compatible print jobs, click the Release All button.
2. To release only certain jobs, press the checkbox next to the jobs to be released.
3. Click the Release button. The selected job(s) will now print.

3. Delete Print Jobs

To delete print jobs, press the checkbox next to the jobs to be remove and press the Cancel button. A confirmation dialog will appear. Press OK to delete the job or Cancel to return to the Jobs List.

3. Refresh Job List

To force the MFP to reload the secured jobs list, press the Refresh button.

4. Complete the Job

When finished releasing print jobs, press the Logout button on the Konica Minolta MFP screen. This will notify Print Audit Secure that the transaction is complete. If this step is not completed, the Konica Minolta MFP will eventually reset back to the Start screen.

5. Troubleshooting Print Audit Embedded for Konica Minolta

Please refer to this section if issues are encountered with the operation of Embedded for Konica Minolta. If a resolution is not found in this section, please contact Print Audit technical support.

Where can I find logging information?
The embedded application writes detailed information to the Windows event log during deployment and in run time using three different logging levels.

- Information
- Warning
- Error

The log can be found by invoking *eventvwr* from the Windows command prompt. The *Print Audit* log can be found under *Applications and Services Logs -> Print Audit.*

When the Konica Minolta device comes out of sleep/energy saving mode, the first card swipe does not unlock the MFP.

This is a known issue with some Konica Minolta MFP's. Check with your Konica Minolta dealer to see if a newer firmware version exists that addresses this issue.

6. IIS Configuration/Setup for Print Audit Embedded for Konica Minolta

Please Note: The Print Audit Embedded for Konica Minolta Setup Wizard is designed to configure settings in IIS when it is run. However, depending the environment, it may be necessary to verify or modify those settings. The examples presented in this guide are based on the default installation options. Please contact your System Administrator for additional details should changes to these defaults be required in your environment.

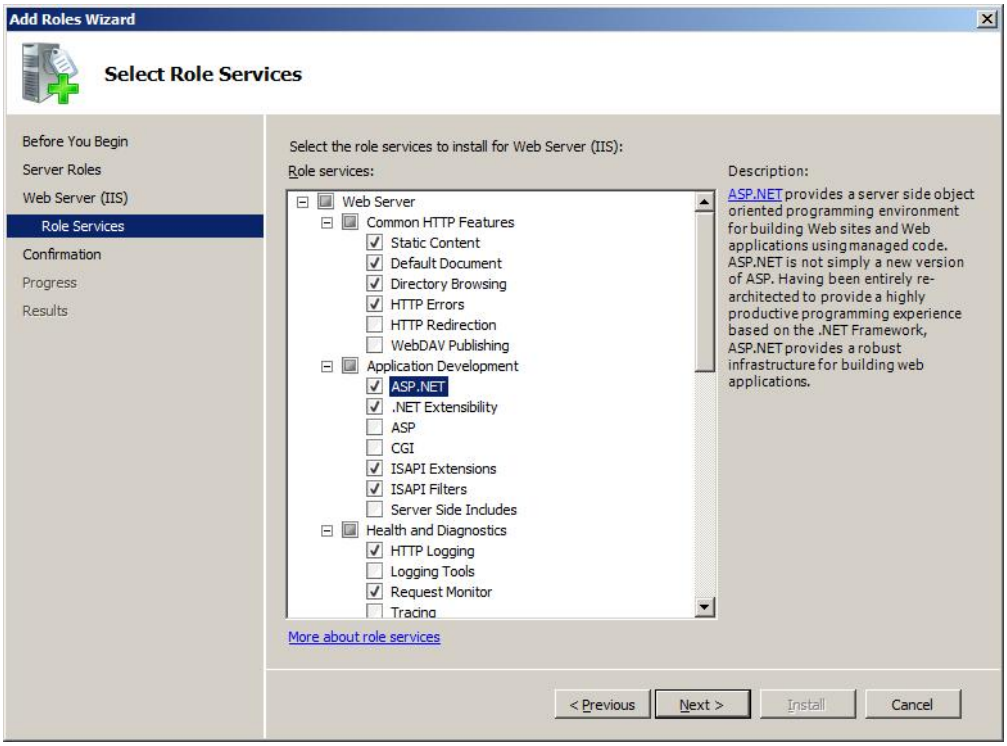
Installing IIS Components for Print Audit Embedded for Konica Minolta

Depending on the version of IIS and Windows operating system, the installation of the components may vary.

Server 2008/IIS 7

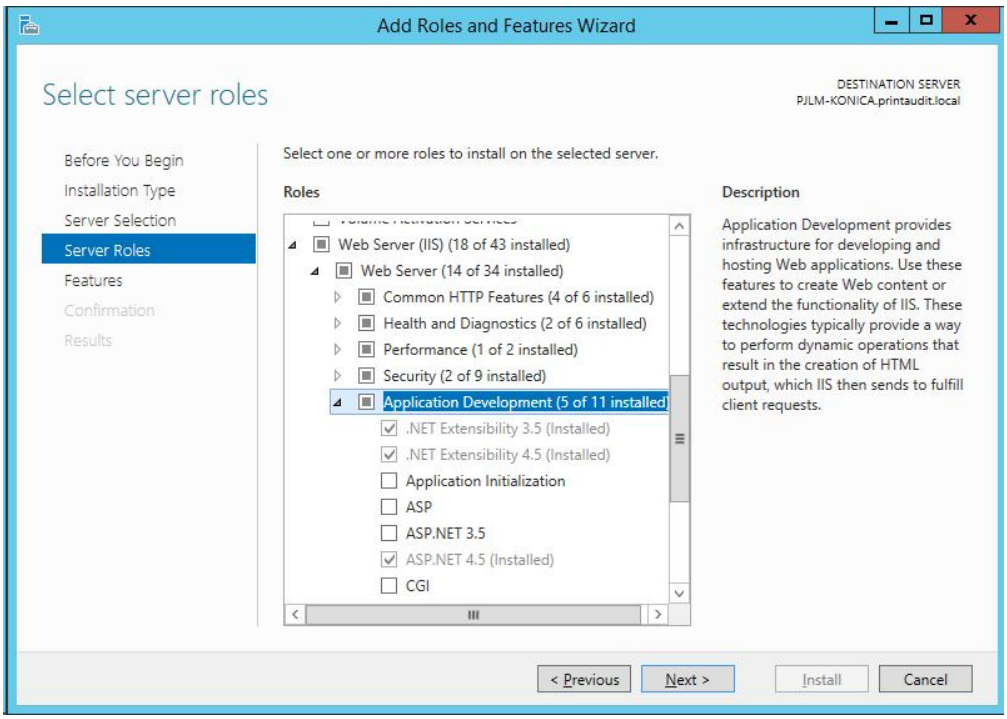
.NET Framework 4 is not a recognized Feature in Server 2008 and cannot be added through the Features Wizard. It requires that .NET Framework 4 be downloaded from Microsoft and installed separately.

The following IIS components should be selected when adding/modifying IIS through the Roles Wizard.



Windows 2012/IIS8 and up

The following IIS components should be selected when adding/modifying IIS through the Roles Wizard:



The following Features should be added/modified through the Features Wizard:

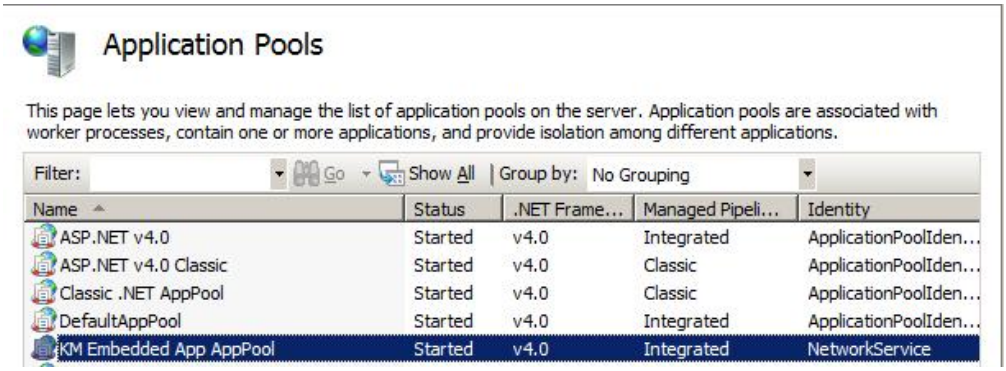
Verifying Application Pools

Application Pools in IIS allow different ASP.NET applications running on the web server to be isolated from each other. Errors in one application pool will not affect other applications running in other application pools. Print Audit Embedded for Konica Minolta installs a single application pool:

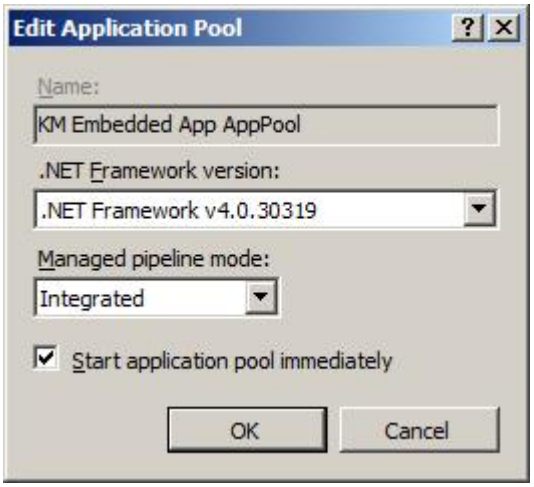
- KM Embedded App AppPool - runs under .NET Framework v4.0.30319

To verify the .NET Framework version for the application pool:

1. Open the Internet Information Services (IIS) Manager.
2. Under the IIS server name, select "Application Pools"



3. Double click on the Application Pool Name.



4. Use the dropdown ".NET Framework version" to select the appropriate version if it is not already set.

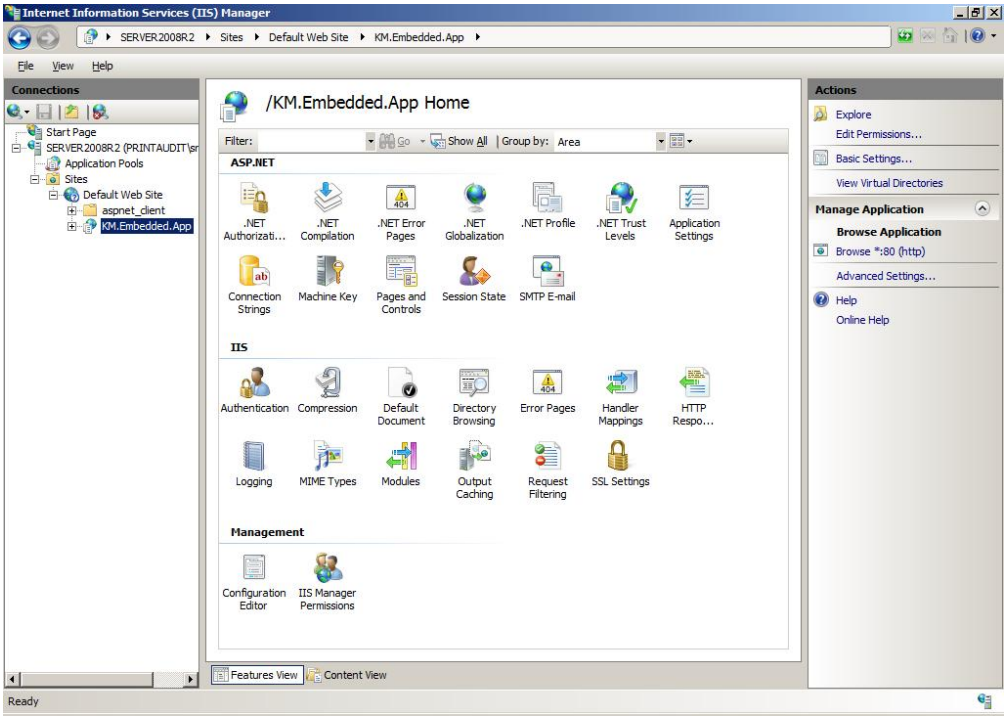
Verifying Application Pools used by Print Audit Embedded for Konica Minolta sites

The Print Audit Embedded for Konica Minolta creates one web sites under "Default Web Site" by default:

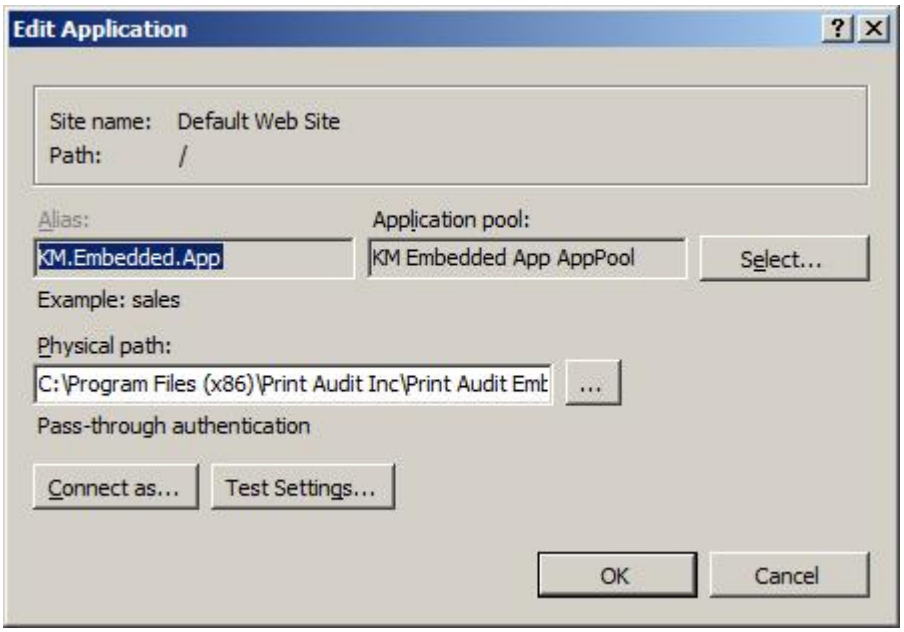
- KM.Embedded.App - KM Embedded App AppPool uses the application pool.

To verify the Application pool used by a site:

1. Open the Internet Information Services (IIS) Manager.



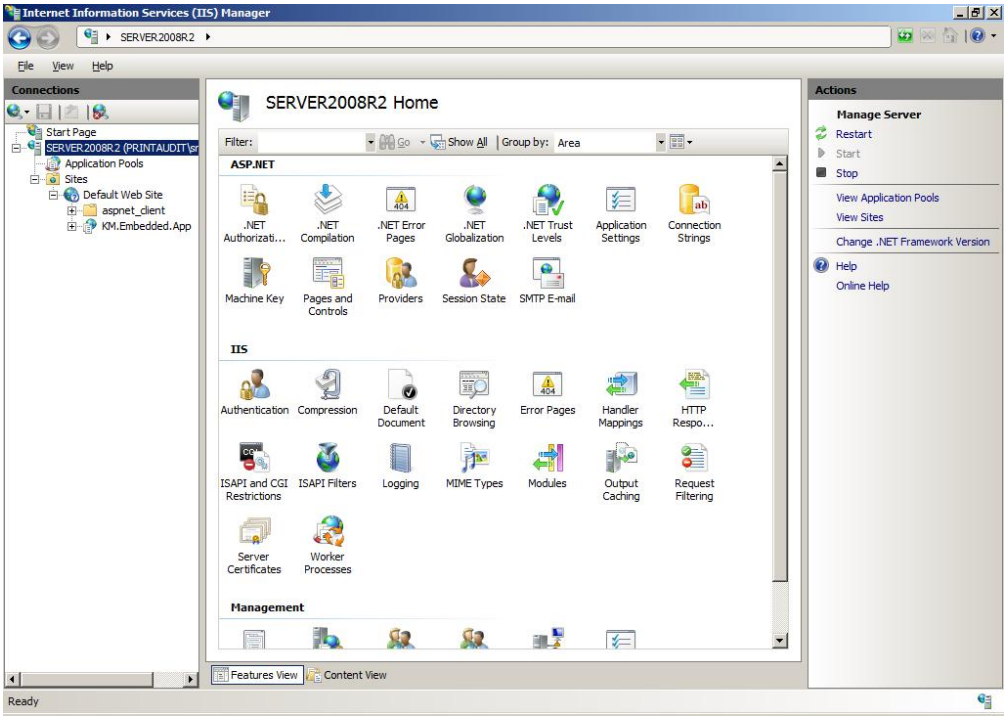
2. Locate the web site under "Sites" and highlight it. By default, the Print Audit Embedded for Konica Minolta sites are under "Default Web Site".
3. Under "Actions" (located on the right hand side of the IIS Manager), click on "Basic Settings... "



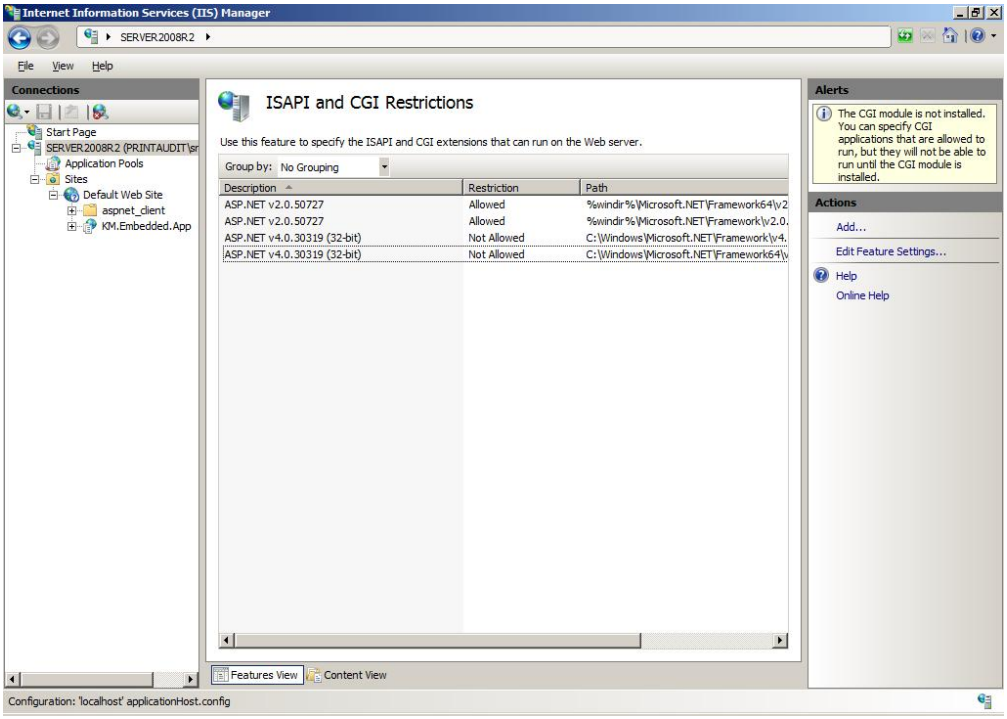
Verifying ASP.NET Restriction

The Print Audit Embedded for Konica Minolta requires .NET Framework and version 4.

1. Open the Internet Information Services (IIS) Manager.



2. Click on the icon "ISAPI and CGI Restrictions"



3. Highlight the .NET 4 versions that are set to "Not Allowed" and click on the "Allow" link under "Actions".

Embedded for Kyocera Documentation

Print Audit® Embedded installs directly onto supported Kyocera multifunction peripherals, allowing users to control and recover all printing, copying, faxing and scanning costs. Review the documentation below for help with installation or configuration of Print Audit Embedded. You can also use the Knowledge Base to find more information.

Browse Documents:

Browse Other Product Documentation:

Print Audit 6 Infinite Device Management Print Audit Secure Rapid Assessment Key Embedded for Sharp

Embedded for Kyocera Mita Embedded for Lexmark Embedded for Xerox Embedded for HP

Copy Audit Touch Copy Audit Numeric

Embedded for Kyocera Installation and Setup Guide

Print Audit Embedded for Kyocera is used alongside Print Audit 6 to provide authenticated access to Kyocera MFPs, for the purpose of securing device functionality, and tracking usage. Users must authenticate at the MFP by login, PIN, or card swipe identification before they may access MFP functions.

When additionally used in conjunction with Print Audit Secure, users will also be able to select and release secure print documents directly from the MFP panel.
This guide provides instructions to install and configure Embedded for Kyocera with Print Audit 6.

When used with Print Audit 6, Embedded for Kyocera will track:

- walk-up copying
- scanning
- faxing
- printing from the document server

When Print Audit Secure is added, Embedded for Kyocera can additionally provide:

- Secure release of all printing
- Follow Me printing

Components

Embedded for Kyocera consists of two main components:

1. Print Audit 6 - Embedded for Kyocera Configuration:

Embedded for Kyocera is configured using the Embedded Systems plug-in for the Print Audit 6 Administration tool. Support for Embedded for Kyocera exists in Print Audit 6.8.0 or newer.

2. Embedded Client:

This software runs on the MFP. The Embedded Client provides a user interface directly on the panel of the Kyocera MFP to enable the tracking of copies, scans or faxes, or the printing of documents stored in the MFP's Document Server.

In addition to tracking the number of pages in a copy, scan, fax, or print job, the Embedded Client tracks additional information about the job. For example, the Embedded Client can request a PIN Code from the user to identify and track who is creating the photocopy. Or, it can request a Client Code to identify which customer or cost center should be billed for a fax transmission.

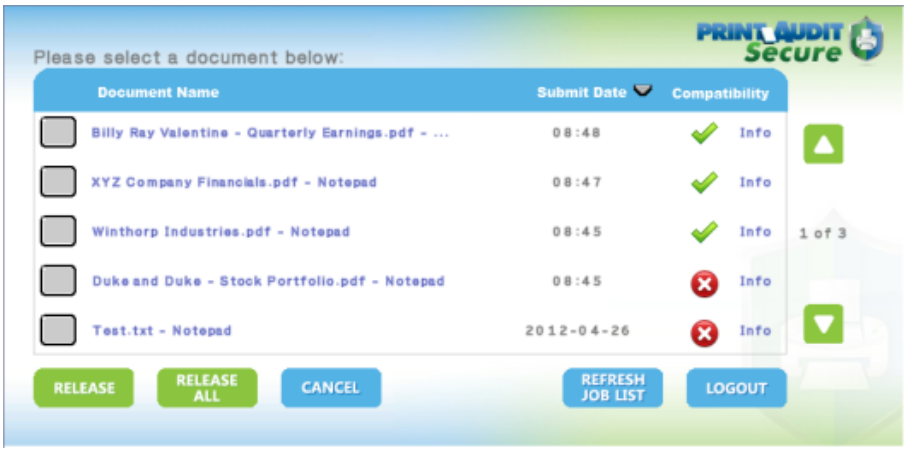
Print Audit 6

Print Audit 6 is a client application that tracks all printing directly from the desktop where the print job was issued. Every job, along with its attributes, are collected and stored in the Print Audit database, where it is available for reporting on printing volume and trends.

Print Audit 6 is available in 3 different modules, Analysis, Rules, and Recovery, which respectively, enable Analysis Reporting from the collected print data, the ability to create printing rules for rules-based printing, and the ability to allocate the cost of print jobs to a user, customer, or cost center.

When used with Embedded for Kyocera, Print Audit 6 can also track copy, scan, and fax jobs, and jobs that are printed from the document server.

Print Audit Secure



Print Audit Secure on Sharp OSA-enabled device

Print Audit Secure allows for print jobs to be held on the server until an authenticated user releases them from the MFP panel, or from a Print Audit Secure release station. When a printer is managed by Print Audit Secure, incoming print jobs are prevented from being automatically output, by holding them in a secure queue on the server. When used with Embedded for Kyocera, users will authenticate at the MFP, view their held jobs on the MFP panel, select one or more jobs and release or delete them directly from the MFP front panel.

Authentication Devices

Print Audit Embedded for Kyocera supports Authentication Devices, such as swipe card or proximity card readers, within an Embedded for Kyocera environment. When an Authentication Device is configured in an environment with Embedded for Kyocera, users must authenticate at an Authentication Device before they are allowed to access the supported Kyocera MFP controlled by the device.

Licensing

To enable the Print Audit Embedded for Kyocera the following is required:

1. **One Print Audit Embedded for Kyocera license per controlled Kyocera MFP** - Print Audit Embedded for Kyocera is licensed on a per-MFP basis. To install Embedded for Kyocera on 15 MFPs, licenses must be purchased for each of the 15 MFPs. MFP licenses can be purchased as part of any Print Audit license, and are additional to the Print Audit 6 client

licenses needed to track print jobs originating from Microsoft Windows and Apple Macintosh workstations. In the event that there are insufficient licenses, Print Audit will stop tracking some or all of the MFPs—MFPs will continue to function as normal, but no information will be tracked.

2. **Kyocera MFPs** - Print Audit Embedded for Kyocera is only supported on Kyocera HyPAS MFPs which support the HyPAS API version 2.0
3. **Print Audit 6.8.0 or higher** - Print Audit Embedded for Kyocera requires Print Audit 6 to configure the MFPs. Consult the Print Audit 6 Installation Guide for more information.

Optional

1. a. **Print Audit Secure 1.1 or higher** - Consult the Print Audit Secure Installation instructions for more information
   b. **One Authentication Device per Kyocera MFP** - Print Audit Embedded for Kyocera supports HID proximity and contactless smart cards for authentication. Users can enter validation data by presenting the card at the card reader. If any authentication devices are to be used in the environment, one authentication device is required per MFP. NOTE: The Kyocera Card Authentication Kit is required for use with most card readers. Please contact your Kyocera dealer for additional information on obtaining and installing the Card Authentication Kit.

Limitations

Print Audit Embedded would ideally function identically across all makes and models. However, due to differences among the proprietary platforms, it is sometimes not possible to implement all features and functionality of the product. The following are a list of known limitations, when using Print Audit Embedded for Kyocera Mita.

1. **Interrupt Button limitations:** The Interrupt Button does not provide information to Print Audit Embedded. Therefore, if a user logs into the device via Print Audit Embedded, and a second user hits the interrupt button to initiate interruption of the current job, all job activity will be attributed attribute to the currently logged in user.
2. **Ability to Return to Print Audit Embedded:** Once a user has logged in and Print Audit Embedded unlocks the device, allowing a user to choose a task on the panel, there is no method to return to the Print Audit Embedded application. Therefore, it is not possible for a user to attribute jobs to more than one custom field per logged on session, as is possible with other versions of Print Audit Embedded.
3. **Limitations with Account Limits:** There is no method available to display account limit messages to the user when the limits are reached. User-based configuration of limits is not possible. Print Audit Embedded controls page-type limits at the embedded configuration level .

4. **Cost Allowances:** There is no method to preventing a user from exceeding their account limit, if there was available credit in their account when they logged in. If they exceed their limit, they could go beyond their minimum balance. However, if the user attempts to login with no available balance, they will be denied from using the device.
5. **Swipe Card Registration:** Currently, this feature is not available under Hypas 2.0 due to limitations.

1. Installation - Embedded for Kyocera

System Requirements

- **Windows 2000 or newer**
- **MS-SQL Server 2005 Express or better -** running embedded applications on with an Access database is not recommended.

Before you Install

- Print Audit Embedded for Kyocera will run on Kyocera HYPAS MFPs which support the HyPAS API version 2.0.
- The target MFPs must be completely started before the installation can proceed.

Steps to install

1. Obtain a Print Audit Embedded License for each MFP you need to install on.
2. Install and configure Print Audit 6 with the appropriate licensing.
3. Deploy the Print Audit Embedded for Kyocera to the device using NetViewer or from flash drive as per below.
4. Download the Kyocera Embedded Application from the Print Audit web site.
5. Download and install the Kyocera NetViewer if deploying from NetViewer – instructions below .
6. Create the record for the MFP in the Print Audit Administrator Embedded section.
7. Install the Embedded Application using NetViewer and configure.
8. Verify operation and tracking of the MFP.

Deploying the Print Audit Embedded for Kyocera application Installation to MFP

There are two methods of deploying the Print Audit Kyocera Embedded Client to a Kyocera device:

1. Deployment via the Kyocera NetViewer application.
2. Deployment via a flash drive (USB port).

Deployment via Kyocera Net Viewer

1. Download the latest version of Kyocera NetViewer from the Kyocera website. Be sure you save the file to a location you can find it in later.
2. You will need to download the latest version of Kyocera NetViewer from the Kyocera website and save it to a location where you can find it later.
    a. http://www.printaudit.com/software-updates.asp
3. Run the NetViewer5xx.exe file:
    a. Choose where to extract the files to
    b. Choose the option to run Setup when the files are extracted
    c. Follow the prompts to complete the NetViewer installation for Device management
4. Run the NetViewer application
    a. If this is the first time it is run, choose the location for your Workspace
    b. Add Devices Wizard
        - Select Express or Custom to begin search for devices on the network
            i. Express will use the default IP range available to the workstation
            ii. Custom will allow you to configure specific IP address(s) and other settings to discover devices
    c. When device discovery has completed, you will be taken to the General view and your device(s) will be shown
    d. Right click on the Kyocera device you wish to install to
    e. Select 'Communication Settings'
    f. In the 'Login' section, enter the user name and password of an Kyocera device-level administrator user and set 'Authenticate mode switch' to 'Use local authentication'
    g. Select 'OK' to close Communication Settings window
    h. Right click on the Kyocera device again and select "Advanced"
    i. Select "Manage Applications"
    j. Select "Install application"
    k. Check the box for "Activate application after installation" and click "Next"
    l. Use the Browse button to go to the location where the Kyocera Embedded Application was saved.
    m. Select the "PAE_Kyocera_Embedded_x.x.x.pkg" file and click Open.
    n. Click "Next" and a confirmation window will be shown that lists the information about the package you are installing and the device it is being installed to.

o. Click "Finish" and you will be taken to a screen that displays the installation window and the application will be installed – you should see a "Success" notice when it completes

p. Click on "Close" and you will be taken back to the main NetViewer window.

q. Repeat as necessary for all of the other MFPs where you need to install the application

Deployment via Flash Drive

Please note that the USB Flash Drive containing the Print Audit Embedded for Kyocera application package must be formatted to FAT32 prior to copying the package to it.. Other file system formats will not be recognized by the MFP.

1. Insert the USB Flash Drive containing the Print Audit Kyocera Embedded application to be installed into the USB Port (A1)
2. If prompted "Removable Memory was recognized. Displaying files. Are you sure?", press [No]
3. Press the System Menu key on the Operation Panel or the System Menu icon on the Kyocera's LCD console
4. Navigate to the [Application] key and press it.
5. When the user authentication screen appears, enter the administrator username and password for the Kyocera.
6. Press [Add]
7. Select the Print Audit Embedded for Kyocera application and press [Install]
8. When the confirmation screen appears, press [Yes]
9. Press [Close] to return to application list
10. Select the Print Audit Embedded for Kyocera application in the application list
11. Press [Activate]
12. Confirm activation, press [Yes]
13. Once the activation is complete, the Print Audit Embedded for Kyocera START screen will appear within a few seconds

Configuring the Kyocera Embedded Application

The Kyocera Embedded application can be configured through the Kyocera Operation Panel or through the Print Audit Administrator.

To access the the Kyocera configuration from the Operation Panel on a machine with the Embedded for Kyocera package installed:

1. Press the "Gear" icon in the upper right hand corner below the Print Audit logo.
2. When the user authentication screen appears, enter the administrator user name and password for the Kyocera. This will take you to the Kyocera Embedded configuration pages

To add a new Kyocera Embedded Application device from the Print Audit Administrator:

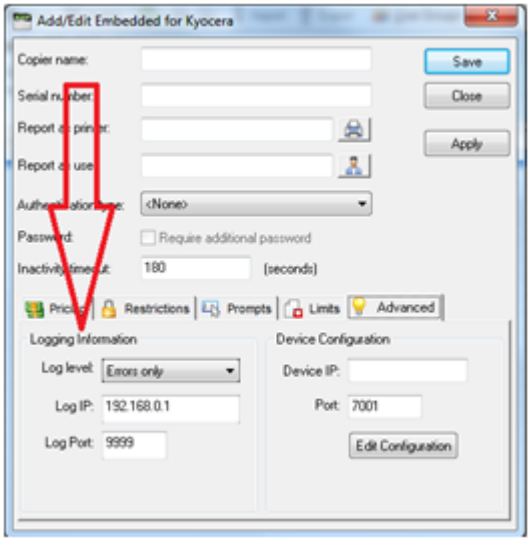
1. Open the Print Audit Administrator
2. Click on the icon "Embedded Systems" on the left
3. Double click on a blank line, or click on New in the top left of the window.
4. Select “Embedded for Kyocera” from the drop-down list and click on OK.
5. Enter the “Copier name”, this is a text field for you to enter the name of your device.
6. Enter the “Serial number”, this must correspond to the device you are entering, the field is case sensitive.
7. Click on the Advanced tab

To configure the Kyocera Embedded Application from the Print Audit Administrator:

1. Open the Print Audit Administrator
2. Click on the icon "Embedded Systems" on the left
3. Double click on the Kyocera device you wish to configure or select it and click on Edit
4. Click on the Advanced tab:

Advanced Tab

Logging Information

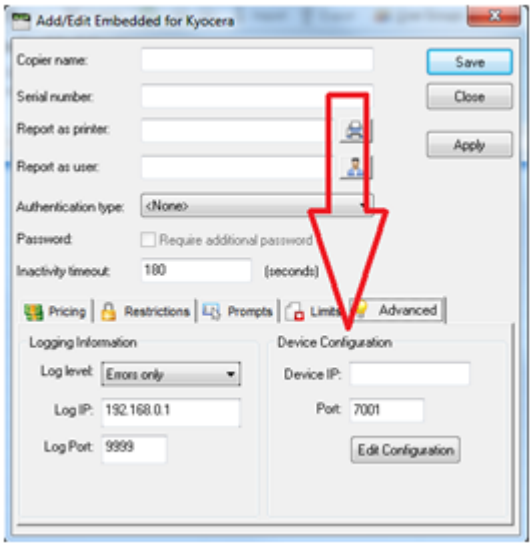


Log Level is an optional setting and only needs to be set when troubleshooting with the assistance of Print Audit Support.

1. Log Level - sets the logging level of the Kyocera Client for the device.
    a. Errors only
    b. Simple
    c. Full
    d. No Logging

1. Log IP - IP Address of the logging
2. Log Port - Port of the logging

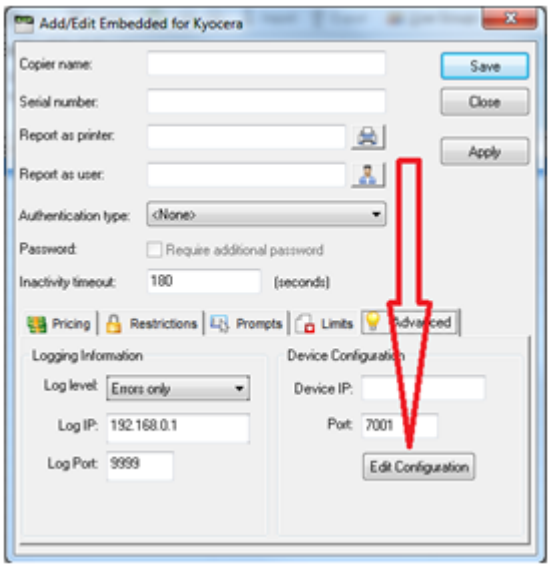
Device Configuration



These fields are required; you must enter the correct IP address and Port.

1. Device IP - the IP address or Hostname of the device that the Print Audit Kyocera Client has been installed on
2. Port - the port used to communicate with the Kyocera device. This setting defaults to port " 7001"

Edit Configuration



IMPORTANT: You must click on this button to enter the Edit Device Configuration window. Inside this window you will find the Apply to Device button, you must click on this to submit any changes to the embedded installation.

Communicator Settings

This tab enables the settings that allow the Kyocera device to communicate with Print Audit Administrator.

1. Enable PA Communicator - enable the Kyocera to work with Print Audit 6 (Copy/Scan/Fax tracking) on the Kyocera device
2. Address - the IP address of the computer running the Print Audit Database Communicator
3. Port - port that the Print Audit Database Communicator is listening on. This setting defaults to 17520
4. Timeout - the Inactivity Timeout the Kyocera will wait before returning to the Print Audit screen. This setting is in milliseconds and defaults to 5000 (5 seconds)

Display Settings

This tab controls the display settings for use with Print Audit 6. They have no effect if Print Audit 6 is not enabled.

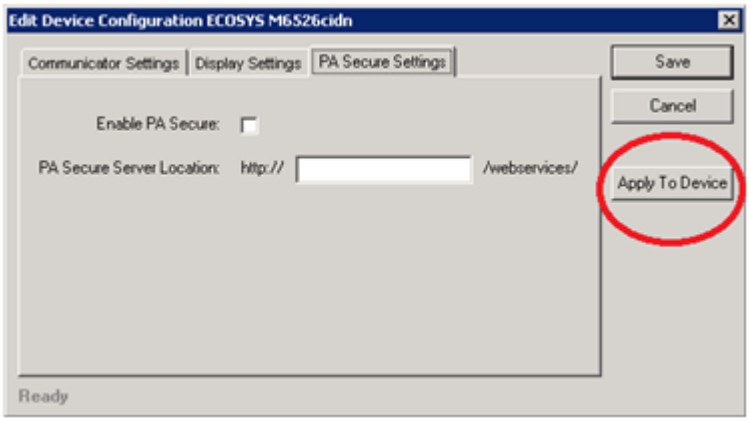
1. Display Summary Page - shows summary page that displaying the details of the job
2. Number of Grid Columns - adjusts the number of columns displayed on a custom field search . Valid entries are 1 or 2

PA Secure Settings

This tab enables the settings for the Print Audit Secure software. Enable these settings only if you are using the Print Audit Secure software on this device.

1. Enable PA Secure - enable the Kyocera to work with Print Audit Secure
2. PA Secure Server - the URL of the Print Audit Secure server web site

Apply to Device - send the configuration settings to the device



This button sends the configuration settings to the device
WARNING: You must click on this button to submit your changes to the device before clicking on Save.

Authentication Types

The authentication type determines how a user identifies themselves to the copier before they can do a transaction. The following options are available:

None - Users do not have to authenticate before using the copier. All transactions are recorded to a generic user.

PIN code - Users must enter their PIN code that has been set up in the Users section of the Print Audit Administrator.

Card reader - Users must use a proximity card to use the copier.

Card reader or PIN - Users can use a proximity card, or enter a PIN.

NOTE: Check the Require additional password box on the Embedded for Kyocera Window to require an additional password before users can authenticate.

Using the Embedded for Kyocera Client

The Embedded for Kyocera Client is very easy to use. First, it prompts you for the required information. What appears in the prompts will depend on how the Embedded Client was configured. After you enter the prompted information, the MFP is enabled for copying, scanning, fax, or printing a document server print job. When you are finished using the device, it is advised to return to the Embedded Client and indicate that you are finished, and end your logged in session. At this point, the information is tracked to the database, and the Embedded Client resets to be ready for the next user.

If you forget to return to the Embedded Client after finishing up, an Inactivity Timeout ensures that, after a period of inactivity, your logged in session ends, the information is tracked, and the panel interface is ready for the next user.

Detailed Panel Walkthrough

"None" Type of Authentication

First, press the Start button on the screen. The Embedded Client retrieves its configuration, and proceeds to prompt for the required information as discussed below.

At any time during the prompts, press the Cancel button to cancel all of your input and return to the start screen.

PIN or Card Reader Authentication

In many cases, the panel is configured to ask for authentication as the first prompt. The panel will prompt you to enter a PIN code, swipe your proximity card, or will allow either type of authentication .

Enter your PIN code using the numeric keypad, or press the Show Keyboard button to access a full alpha- numeric keyboard on the touch screen. Once you have entered your PIN code, press the OK button. You can also use the # key on the keypad for OK.

To use a proximity card, hold the card near the sensor. The light will turn green and the sensor will beep when your card has been read.

Custom Fields

If the panel is configured to prompt for custom fields, these are the next prompts. Select one of the presented options and then press the OK button. If there are more choices than will fit on one screen, use the Prev and Next buttons to page through the choices.

If the Custom Field is either the Searchable or Searchable Dropdown type, there will also be a Search button displayed. Press the Search button to bring up a keyboard, and enter in the text you wish to search for. Press OK to perform the search and hide the keyboard. Once you have searched, only options that match your search text will be shown, and you can page through them as usual. If you do not find the option you are looking for, you can perform another search.

Comments

If the panel is configured to allow the user to enter a comment, this will always be the last prompt. Enter a comment using the numeric keypad on the MFP, or press the Show Keyboard button to enter the Comment using a full alpha-numeric keyboard on the touch screen. When you have finished, press the OK button. The comment may be left blank.

Once you have finished entering all of the information, a screen with a large Done button appears. This screen also has instructions on how to return to the Embedded for Kyocera Client. At this point (before pressing the Done button), use the MFP function keys to switch to Copy, Fax, Document Server, Scan, or Print mode as appropriate, and proceed to use the MFP normally.

Declining Balances

If declining balances are enabled for the current user each copy/fax/scan operation will debit the account balance in real-time. Once the balance of the current user reaches zero all MFP copy/fax/scan functions will be locked until such time that the user logs in again with a positive balance.

When you have finished using the MFP, return to the Embedded for Kyocera, and press the Done button. At this point, all of the information is tracked to the database, and the panel interface resets to the first screen.

2. Configuration - Embedded for Kyocera

The following are instructions to configure Print Audit 6 with Embedded for Kyocera.

Pre-configuration checklist

If you are ready to begin configuring Print Audit 6 with Embedded for Kyocera, you have:

- Installed the Print Audit Database Communicator, Database and Administration tools to a computer on the network that will be on and available at all times. The Print Audit Client should be installed on at least one workstation, to test printing and ensure that print jobs are being tracked correctly before continuing.
- Configured Print Audit 6 for user quotas, PIN codes and validated fields to be be integrated into Print Audit 6 Embedded.
- Used this guide to configure Print Audit 6 Embedded on the Kyocera HyPAS devices.

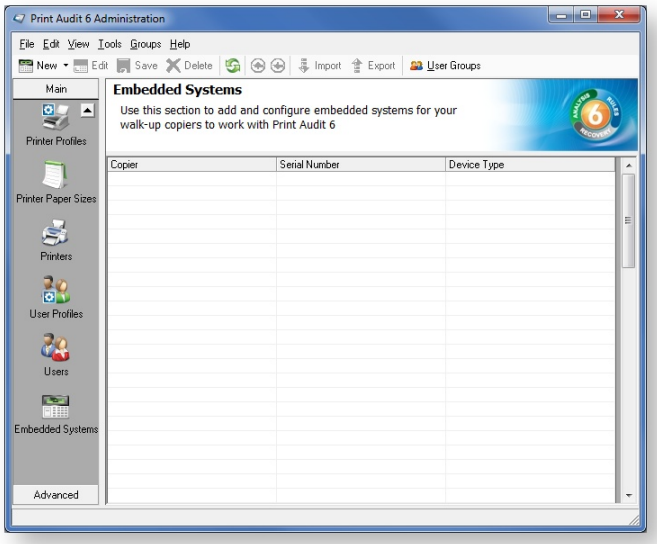
Overview

The Print Audit Administration tool provides the ability to configure Embedded for Kyocera on all the MFDs in the environment using the Embedded Systems plug-in. Configure one copier for every physical Kyocera MFD on which the Embedded Client will run.

Costs, restrictions, limits, authentication methods and custom fields may be configured for each device.

Adding, Editing and Deleting Copiers in Print Audit 6

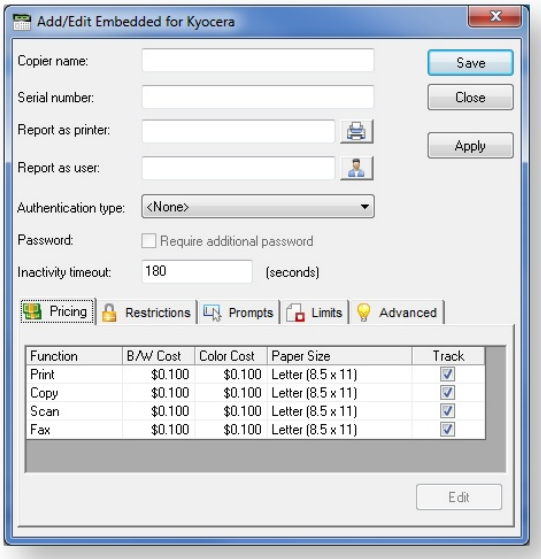
Use the Embedded Systems section of the Administration tool to add, edit and delete Embedded for Kyocera copiers. A copier in the Administration tool represents a physical copier in the network.



To add a new copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Click the New button on the toolbar.
4. Select Embedded for Kyocera from the dropdown list of devices
5. Press OK. The Add/Edit Embedded for Kyocera window will appear
6. At minimum, a copier name and the serial number of the copier must be provided. Please refer to the 'Embedded for Kyocera Configuration Window' section below for more information filling out the Embedded for Kyocera window.
7. Click the Save button. The Embedded for Kyocera window closes and the copier appears in the Copiers list.

To edit a copier:



1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Edit button on the toolbar. The Embedded for Kyocera window appears.
5. Make any needed changes to the copier.
6. Click the Save button. The Embedded for Kyocera window closes and the copier appears in the Copiers list.

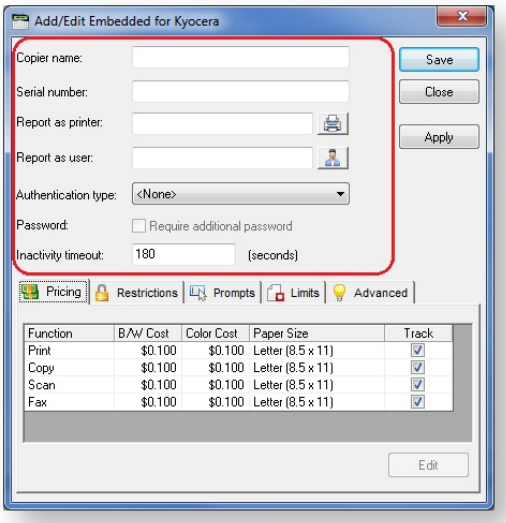
To delete a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Delete button on the toolbar. A message appears to verify removal of the copier.
5. Click the Yes button to delete the copier. The list of copiers refreshes.

Configuring the Kyocera MFP in Print Audit 6

This Embedded for Kyocera window in Print Audit 6 enables the configuration of all aspects of the Embedded for Kyocera copier device. The different elements of the window are described below.

General



Copier name - The name to describe the copier. Enter a name that is descriptive enough to distinguish the copier from others. For example "Third Floor Kyocera TA3050".

Serial number - The serial number of the Kyocera MFD. NOTE: the serial number is case-sensitive and must match the serial number of the Kyocera MFD that the Embedded Client is installed on.

Report as printer - Use this to select an already existing Print Audit printer with which to associate the copier. For example, if there is an MFD in the office that users print to which is already in the Print Audit database, choose that MFD here for the copier so that all transactions are reported as the same printer. If a printer is not selected here, Print Audit will record transactions for this copier as the copier name.

Report as user - Use this to select an existing Print Audit user whom to associate all jobs from this copier. Use this functionality to still have individual user authentication, but for reporting purposes report all jobs to a single user.

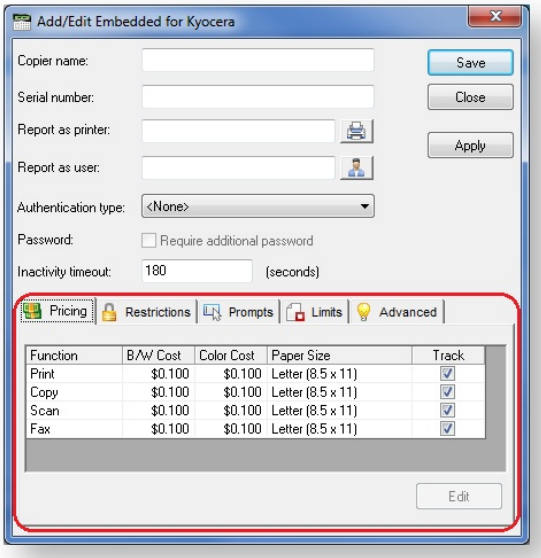
Authentication type - Select how the user will authenticate to the copier before they can do transactions. The authentication type determines how a user identifies themselves to the copier before they can do a transaction. The following options are available:

- None - Users do not have to authenticate before using the copier. All transactions are recorded to the generic Kyocera_Embedded user.
- PIN code - Users must enter their Print Audit PIN to access the copier.

- Card Reader - Users must use their proximity card or swipe card to access the copier
- Card Reader or PIN - Users must use their proximity / swipe card or enter their Print Audit PIN to access the copier.

Require additional password - Check this box to require the user to enter an additional (optional) password before they can authenticate using the Authentication type selected above.

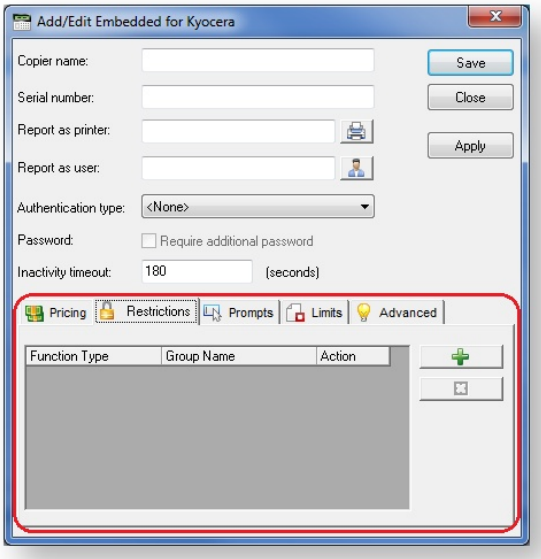
Pricing tab



This tab contains the pricing for each function on the copier.

To edit the pricing for a particular function:

1. Clear the "Track" column for the function to disable the tracking of transactions of that type.
2. Select from the list the function that is to change and click the Edit button. The Configure Pricing and Paper Size Window appears.
3. Set the pricing as it makes sense for this copier in the organization.
4. Click the Done button. The Configure Pricing and Paper Size Window closes.


Add/Edit Embedded for Kyocera
Copier name:
Serial number:
Report as printer:
Report as user:
Authentication type:
<None>
Password:
Require additional password
Inactivity timeout:
180
(seconds)
Save
Close
Apply
Pricing
Restrictions
Prompts
Limits
Advanced
Function Type
Group Name
Action

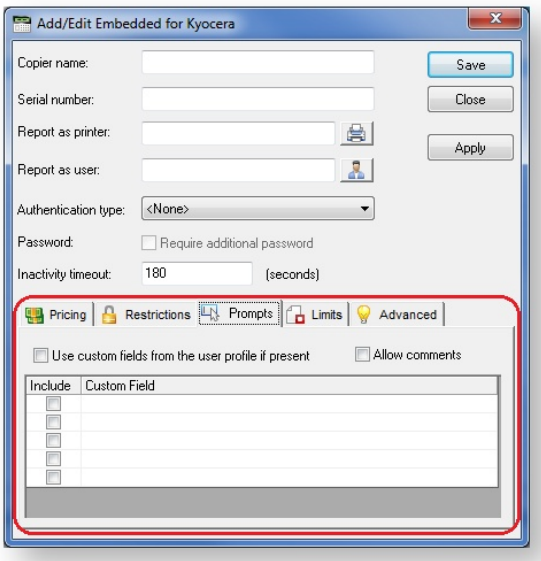
Restrictions tab (only with Print Audit 6 Rules)

Choose to restrict access to the copier based on which user group a user belongs to.

Add button - Click this button to add a new restriction. The Configure Restriction Group window appears.

Remove button - Click this button to remove a restriction.

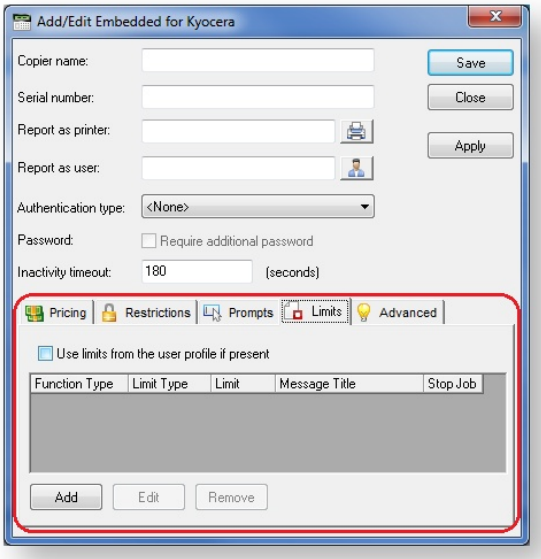
Prompts tab (only with Print Audit 6 Recovery)



This tab is only relevant when using Print Audit 6 Recovery for the charge-back of printing.

- For each Activity the user can be required to enter values for Custom Fields. Custom Fields are setup in the Custom Fields section of the Print Audit Administrator. On this tab, select from any one of the Custom Fields configured and define a custom prompt for each one.
- Use custom fields from the user profile - Check this box to override the default custom field choices with the custom fields set in a user's User Profile.
- Allow comments - Check this box if the user can enter general comments about the job.
- Custom fields - The custom fields list contains all custom fields that have been defined. To use a custom field for the activity, check the Include checkbox.

Limits tab (only with Print Audit 6 Rules)



This tab is only relevant when using Print Audit 6 Rules to enforce rules-based printing.

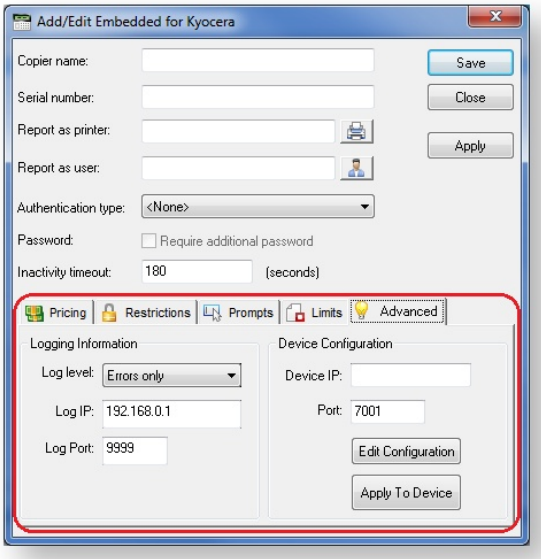
Use limits from the user profile - Check this to use limits defined in a user's profile instead of the limits defined here.

Add - Click this to add a new printing limit.

Edit - Click this to edit an existing limit.

Remove - Click this to remove an existing limit.

Advanced tab



Logging Information

Log Level - Use this drop down box to change amount of information the Embedded Client will log. Unless instructed to change this setting by technical support, leave this set to Errors Only.

Log IP - Enter the IP address where the logger application is located. The device will direct logging information to this address.

Log Port - Enter the port number the device will use to transmit logging information.

Device Configuration

Device IP- Enter the IP Address of the device being set up and configured.

Port - Enter the port number that will be used to receive the configuration information when it is pushed to the device. Must be set to 7001. Ensure the port is open and enabled if a firewall has been activated on computer.

Edit Configuration - Click this to edit the configuration information.

Apply To Device - Click this to send the configuration information to the IP address and port specified above.

Edit Configuration

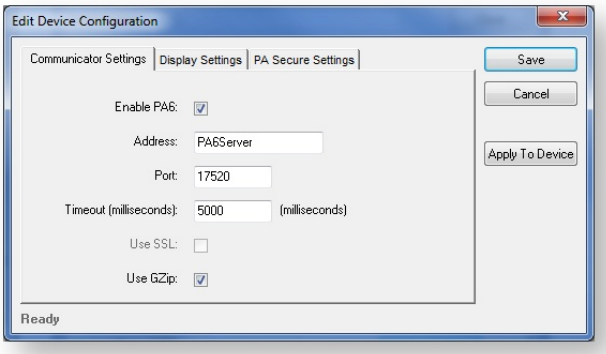
Use this feature to remotely configure a device for use with Print Audit 6 and Print Audit Secure.

Save - Click this to save data and return to Add/Edit Embedded for Kyocera window

Cancel - Click this to cancel any changes made and return to Add/Edit Embedded for Kyocera window

Apply To Device - Click this box to send configuration information to the device

Communicator Settings

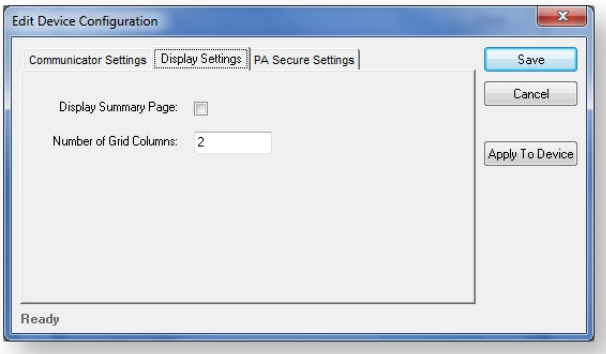


Enable PA6 - Check this box to enable device to use Print Audit 6

Address - Enter the hostname or IP address of the server hosting the Print Audit 6 Database Communicator

Port - Enter the port number used to send and receive data with the Database Communicator

Timeout - Enter the time, in milliseconds, to wait while communicating with the Database Communicator.

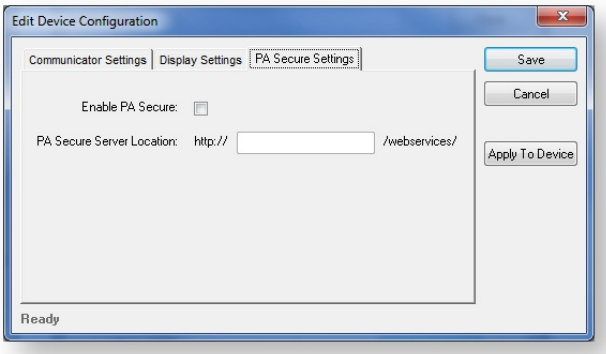


Display Settings

Display Summary Page - Check this box to enable Print Audit Embedded to display a summary of user selected custom fields and user balances (if features are enabled)

Number of Grid Columns - Enter the number of columns to use when displaying values in a table.

Print Audit Secure Settings



Enable PA Secure - Check this box to enable device to use Print Audit Secure

PA Secure Server Location - Enter the location of the Print Audit Secure server

Repeat the above steps for each Kyocera MFP on which Embedded for Kyocera will be used. The Troubleshooting section of this document should be consulted if there are issues running the panel.

3. Using Card Readers - Embedded for Kyocera

Embedded for Kyocera allows the use of proximity cards for user authentication. Please note there is some additional configuration required in order to support proximity cards. To configure the Kyocera Embedded to use Swipe Cards, the Authentication type must be set to "Card Reader" or " Card Reader or PIN Code" as indicated in the "Adding, Editing and Deleting Copiers in Print Audit 6 " section of previous Configuration module.

NOTE: The Kyocera Card Authentication Kit is required. This component is purchased separately from your Kyocera dealer to use . Please contact them for additional information on obtaining a License Key for the Card Authentication Kit and the installation procedure for your Kyocera device.

Configuring Card IDs in the Print Audit Administrator

Before proximity cards will be recognized as valid, they must be configured in the Print Audit Administrator.

- Launch the Print Audit Administrator.
- Click on the Users icon on the left hand side of the screen.
- Double-click on the user you want to assign a proximity card ID to.
- Enter their proximity card ID number into the PIN code field.
- If you did not enable Facility (FAC) codes when you provisioned the card readers, enter the card ID number only. In many cases this number is 5 digits or less, although it may be longer in some installations.
- If you enabled Facility (FAC) codes when you provisioned the card reader, enter in the Facility (FAC) code, followed by a -, and then the card ID number. For example, if the Facility (FAC) code is 176 and the ID number is 12345, you would enter 176-12345.
- If a user's ID number or the Facility (FAC) code starts with one or more zeroes, do not enter the leading zeroes when you are entering the numbers into the PIN Code field. For example, if a card ID number is 00793, enter 793.
- Click the Save button to save the user.
- You may also import a large number of IDs at once from a CSV file using the import functionality in the Administrator. See the help in the Administrator for more information on assigning PIN codes (card IDs) to users.

4. Using Embedded for Kyocera with Print Audit 6

The Embedded for Kyocera Client is very easy to use. It will first prompt for required identification or billing information, before enabling the device for copy, scan, fax, or print functionality. Once the desired function is complete, return to the panel and complete the session, otherwise the MFP will timeout the session. When the session ends, the copy, scan, fax, or print transaction is sent to the Print Audit 6 database, and the Embedded Client resets to be ready for the next user.

The standard set of steps to using Embedded for Kyocera to track job information is as follows:

1. **Start the Transaction** - Press the Start button on the screen. The Embedded Client retrieves its configuration and proceeds to prompt for the required information. The Cancel button can be used at any time to return to the Start screen.
2. **Authenticate** - If configured to ask for a PIN Code, the Embedded Client displays a login screen. To login:
    a. Press the PIN Code button. An input form displays.
    b. Enter a PIN Code using the Kyocera keyboard or the touch screen.
    c. Press the OK button to accept the input.
    d. Press the OK button on the Login screen to validate the PIN Code.
3. **Enter Custom Field Information** - If configured to ask for Custom Field information, the Embedded Client will prompt for on or more values from the user. To enter values for a searchable field:
    a. Press the button on the touch screen that corresponds to the Custom Field Name.
    b. Enter a full or partial code on the screen and click OK.
    c. If only one match is found for the field, the Embedded Client asks for the next Custom Field value if any is configured.
    d. If Print Audit finds more than one match, a list of values will display. Use the touch screen to navigate through the values.
    e. When the desired value is found, press the button corresponding to the value. It appears highlighted.
    f. Press the OK button to accept the value.
    g. Press the OK button again to move to the next screen.
4. **To enter values for a non-searchable field**:
    a. Press the button that corresponds to the desired value. It appears highlighted.
    b. Use the arrows on the touch screen to navigate through the choices.

c. Press the OK button to accept the value. The Embedded Client will request the next Custom Field value if any is configured.

5. **Enter any Comments** - If configured, the Embedded Client will request any Comments for the job. Press OK if to proceed without entering comments. To enter comments:
   a. Press the Comments button on the touch screen. An input form appears.
   b. Use the input form to enter comments.
   c. Press the OK button to close the input form.
   d. Press the OK button on the Comments screen to accept the comments.
6. **Verify Selections** - After all information has been input, a summary screen appears showing the current balance if any, along with the custom values selected. Press the OK button to accept the selections and begin the job.
7. **Complete the Job** - After the job is completed, press the "" (Logout)" button on the Kyocera MFP keypad. This completes the transaction, and transmits the job information to the Print Audit database. If the "" (Logout)" button is not used to end the session, the Kyocera MFP will eventually timeout the session, return to the Start screen and transmit the job information to the Print Audit database.

Note: Declining balances

If declining balances are enabled for the current user, each MFP operation (copy/fax/scan) will debit the account balance in real-time, however it is not possible to restrict that user from exceeding their account balance in real time.

If the user logs in with an active balance, they are authorized to use all device functions, even if the transactions exceed their minimum allowable balance. However, if a user logs in with an account at or below the minimum allowable balance, they will be restricted from performing any MFP functions until such a time that the user logs in again with a positive account balance.

5. Using Embedded for Kyocera with Print Audit Secure

The Print Audit Secure Embedded for Kyocera Client is very easy to use. It will first prompt for required information. The prompts which appear are dependent on how the Secure Embedded Client is configured. Once the prompted information is provided, the device will release the secure job(s). Then the Secure Embedded Client resets to be ready for the next user. If the session is not manually finished, the Kyocera MFP will timeout.

Following are the standard set of steps to using Secure Embedded for Kyocera to release a print job.

1. Authenticate

1. **PIN Code authentication** - If configured to request a PIN Code, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Pin Code Field
    b. Enter a PIN Code using the Kyocera keyboard or the touch screen.
    c. Press the Login button to accept the input.
2. **Authenticate with a Username** - If configured to ask for a Username, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Username Field
    b. Enter a Username
    c. Click on the Password Field
    d. Enter a Password
    e. Press the Login button to accept the input.
3. **Authenticate with a swipe card** - If configured to ask for a swipe card, the Secure Embedded Client displays a login screen. To login:
    a. Swipe a card in a card reader attached to the MFP.

2. Release Print Jobs

1. To release all the compatible print jobs, click the Release All button.
2. To release only certain jobs, press the checkbox next to the jobs to be released.
3. Click the Release button. The selected job(s) will now print.

3. Delete Print Jobs

To delete print jobs, press the checkbox next to the jobs to be remove and press the Cancel button. A confirmation dialog will appear. Press OK to delete the job or Cancel to return to the Jobs List.

4. Refresh Job List

To force the MFP to reload the secured jobs list, press the Refresh Jobs List button.

5. Complete the Job

When finished releasing print jobs, press the Logout button on the Kyocera MFP screen. This will notify Print Audit Secure that the transaction is complete. If this step is not completed, the Kyocera MFP will eventually reset back to the Start screen.

6. Troubleshooting - Embedded for Kyocera

Please refer to this section if issues are encountered with the operation of Embedded for Kyocera. If a resolution is not found in this section, please contact Print Audit technical support.

Embedded for Kyocera application goes straight to the Copy Screen after pressing the START button.

Possible causes of this issue are:

- The Embedded for Kyocera application has been installed but not properly configured
- The Embedded for Kyocera application is unable to connect to the Database Communicator component
- The Embedded for Kyocera license is not valid

1. The Embedded for Kyocera application has been installed but not properly configured. Please check the following:
    a. an entry exists in the Print Audit Administrator Embedded Systems for the Kyocera device
    b. the Serial Number for the Kyocera device has been entered incorrectly. The serial number must match the Kyocera device's and is case-sensitive
    c. the IP address or port entered for the Kyocera device are correct
    d. the Print Audit 6 and\or Print Audit Secure settings have been entered correctly and applied to the device successfully
2. The Embedded for Kyocera application is unable to connect to the Database Communicator component. Please check the following:
    a. the Database Communicator service is running
    b. the IP address and port of the Database Communicator those configured in the Embedded for Kyocera settings in the Print Audit Administrator
3. The Embedded for Kyocera license is not valid. Please check the following:
    a. there is one Kyocera Embedded (HyPAS) license for each device running Embedded for Kyocera present in the "Connectors and Addons" tab in the Print Audit Administrator licensing
    b. the Database Communicator service has been restarted since the Print Audit License Key was activated
    c. the Print Audit License Key includes the appropriate number of Embedded for Kyocera licenses

The card reader beeps and the LED light turns green but Embedded for Kyocera does not authenticate:

1. check to see that the Kyocera Card Authentication Kit has been successfully configured and licensed
2. check to see that the Kyocera device has been configured to use "Card Reader" or "Card Reader or PIN"

A Kyocera device that previous showed in Kyocera Net Viewer is no longer visible.

If you delete a device in the Kyocera Net Viewer device list, Net Viewer automatically adds it to the Excluded Devices list. In order to display the device again, go to Device --> Discovery – Show excluded devices. Click on "Include device" to re-add it to list of discovered devices.

The Kyocera device can't see the Embedded for Kyocera installation package or displays an error message.

The flash drive (thumb drive) must be formatted for "FAT32" for the Kyocera to recognize it. If the drive is not formatted as FAT32, the Kyocera may emit a warning beep or display an error "The removable memory is not formatted - Cannot recognize the removable memory".

The images and text are out of alignment when running Embedded for Kyocera on a small screen Kyocera device.

Issue: When running the Embedded for Kyocera on a small screen device, the images and text are out of alignment.

Solution: Make sure that you are running Print Audit Embedded for Kyocera 1.1.0 or better. Print Audit Embedded for Kyocera 1.0.0 supported large screen (8.5 in.) devices.

Embedded for Lexmark Documentation

Print Audit Embedded installs directly onto supported Lexmark multifunction peripherals, allowing users to control and recover all printing, copying, faxing and scanning costs. Review the documentation below for help installing and configuring Print Audit Embedded.

You can also use our Knowledge Base to find more information.

Browse Documents:

Browse Other Product Documentation:

Print Audit 6 Infinite Device Management Print Audit Secure Rapid Assessment Key Embedded for Sharp

Embedded for Kyocera Mita Embedded for Lexmark Embedded for Xerox Embedded for HP

Copy Audit Touch Copy Audit Numeric

Embedded for Lexmark-Install and Setup

Print Audit Embedded for Lexmark is used alongside Print Audit 6 to provide authenticated access to Lexmark MFPs, for the purpose of securing device functionality, and tracking usage. Users must authenticate at the MFP by login, PIN, or card swipe identification, before they may access MFP functions.

When additionally used in conjunction with Print Audit Secure, users will also be able to select and release secure print documents directly from the MFP panel.
This guide provides instructions to install and configure Embedded for Lexmark with Print Audit 6.

When used with Print Audit 6, Embedded for Lexmark will track:

- walk-up copying
- scanning
- faxing

When Print Audit Secure is added, Embedded for Lexmark can additionally provide:

- secure release of all printing
- Follow Me printing

Components

Embedded for Lexmark consists of two main components:

1. Print Audit 6 - Embedded for Lexmark Configuration:

Embedded for Lexmark is configured using the Embedded Systems plug-in for the Print Audit 6 Administration tool. Support for Embedded for Lexmark exists in Print Audit 6.9.0 or newer.

2. Embedded Client:

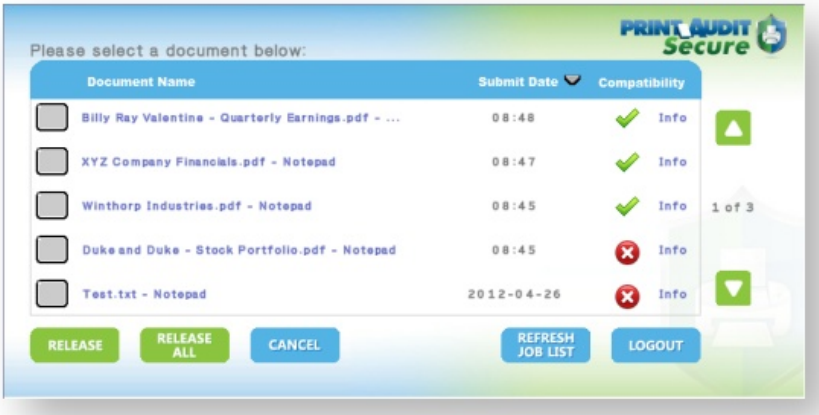
This software runs on the MFP. The Embedded Client provides a user interface directly on the panel of the Lexmark MFP to enable the tracking of copies, scans or faxes.

In addition to tracking the number of pages in a copy, scan, fax, or print job, the Embedded Client tracks additional information about the job. For example, the Embedded Client can request a PIN Code from the user to identify and track who is creating the photocopy. Or, it can request a Client Code to identify which customer or cost center should be billed for a fax transmission.

Print Audit 6

Print Audit 6 is a client application that tracks all printing directly from the desktop where the print job was issued. Every job, along with its attributes, are collected and stored in the Print Audit database, where it is available for reporting on printing volume and trends.
Print Audit 6 is available in 3 different modules, Analysis, Rules, and Recovery, which respectively, enable Analysis Reporting from the collected print data, the ability to create printing rules for rules-based printing, and the ability to allocate the cost of print jobs to a user, customer, or cost center.
When used with Embedded for Lexmark, Print Audit 6 can also track copy, scan, and fax jobs.

Print Audit Secure



Print Audit Secure on Sharp OSA-enabled device

Print Audit Secure allows for print jobs to be held on the server until an authenticated user releases them from the MFP panel, or from a Print Audit Secure release station. When a printer is managed by Print Audit Secure, incoming print jobs are prevented from being automatically output, by holding them in a secure queue on the server. When used with Embedded for Lexmark, users will authenticate at the MFP, view their held jobs on the MFP panel, select one or more jobs and release or delete them directly from the MFP front panel.

Authentication Devices

Print Audit Embedded for Lexmark supports Authentication Devices, such as swipe card or proximity card readers, within an Embedded for Lexmark environment. When an Authentication Device is configured in an environment with Embedded for Lexmark, users must authenticate at an Authentication Device before they are allowed to access the supported Lexmark MFP controlled by the device.

Licensing

To enable the Print Audit Embedded for Lexmark the following is required:

1. **One Print Audit Embedded for Lexmark license per controlled Lexmark MFP -** Print Audit, Embedded for Lexmark is licensed on a per-MFP basis. To install Embedded for Lexmark on 15 MFPs, licenses must be purchased for each of the 15 MFPs. MFP licenses can be purchased as part of any Print Audit license, and are additional to the Print Audit 6 client licenses needed to track print jobs originating from Microsoft Windows and Apple Macintosh workstations. In the event that there are insufficient licenses, Print Audit will stop tracking some or all of the MFPs—MFPs will continue to function as normal, but no information will be tracked.

2. **Print Audit 6.9.0 or higher -** Print Audit Embedded for Lexmark requires Print Audit 6 to configure the MFPs. Consult the Print Audit 6 Installation Guide for more information.

Optional

1. **Print Audit Secure 1.1 or higher -** Consult the Print Audit Secure Installation instructions for more information.
2. **One Authentication Device per Lexmark MFP-** Print Audit Embedded for Lexmark supports optional proximity and contactless smart cards for authentication via a USB Reader. Users can enter validation data by presenting the card at the card reader. If an authentication devices are to be used in the environment, one authentication device is required per MFP. Note: Please contact your Lexmark representative for additional assistance when setting up the card reader.

Limitations

Print Audit Embedded would ideally function identically across all makes and models. However, due to differences among the proprietary platforms, it is sometimes not possible to implement all features and functionality of the product. The following are a list of known limitations, when using Print Audit Embedded for Lexmark:

1. **Assigning Limits** - Assigning Limits in the Embedded for Lexmark plugin based on the Function type is not supported. However, limits from a User profile can be applied if the check box is selected.
2. **Cost Allowances:** There is no method to preventing a user from exceeding their account limit, if there was available credit in their account when they logged in. If they exceed their limit, they could go beyond their minimum balance. However, if the user attempts to login with no available balance, they will be denied from using the device.

1. Installation - Lexmark

This section only addresses the installation requirements and configuration of Print Audit 6 for use with Embedded for Lexmark. For complete instructions on installing and configuring Print Audit 6, please refer to the Print Audit 6 Installation information found online. Refer to that documentation to perform the following steps to install Print Audit 6 in conjunction with Print Audit Embedded for Lexmark.

Before you Install

System Requirements

- **Lexmark embedded Solutions Framework (eSF) 2.0, 3.0 or 4.0**
- **MS-SQL Server 2005 Express or better -** running embedded applications on with an Access database is not recommended.
- **Print Audit 6.9** or newer* - The Print Audit 6 Database Communicator, Database, and Administrative tools must be installed on a Windows 2000 or newer computer
- **Optional -** Print Audit Secure 1.1 or better is required to use the Print Audit Embedded for Lexmark with Secure Server options

The latest versions of the Print Audit 6 and Print Audit Secure software are available from the Print Audit website.

Pre-Installation Steps

1. Obtain a Print Audit Embedded for Lexmark license for each MFP you need to install on
2. Install and configure Print Audit 6 with the appropriate licensing
3. Download the Print Audit Embedded for Lexmark from the Print Audit web site
4. Create the record for the MFP in the Print Audit Administrator Embedded section

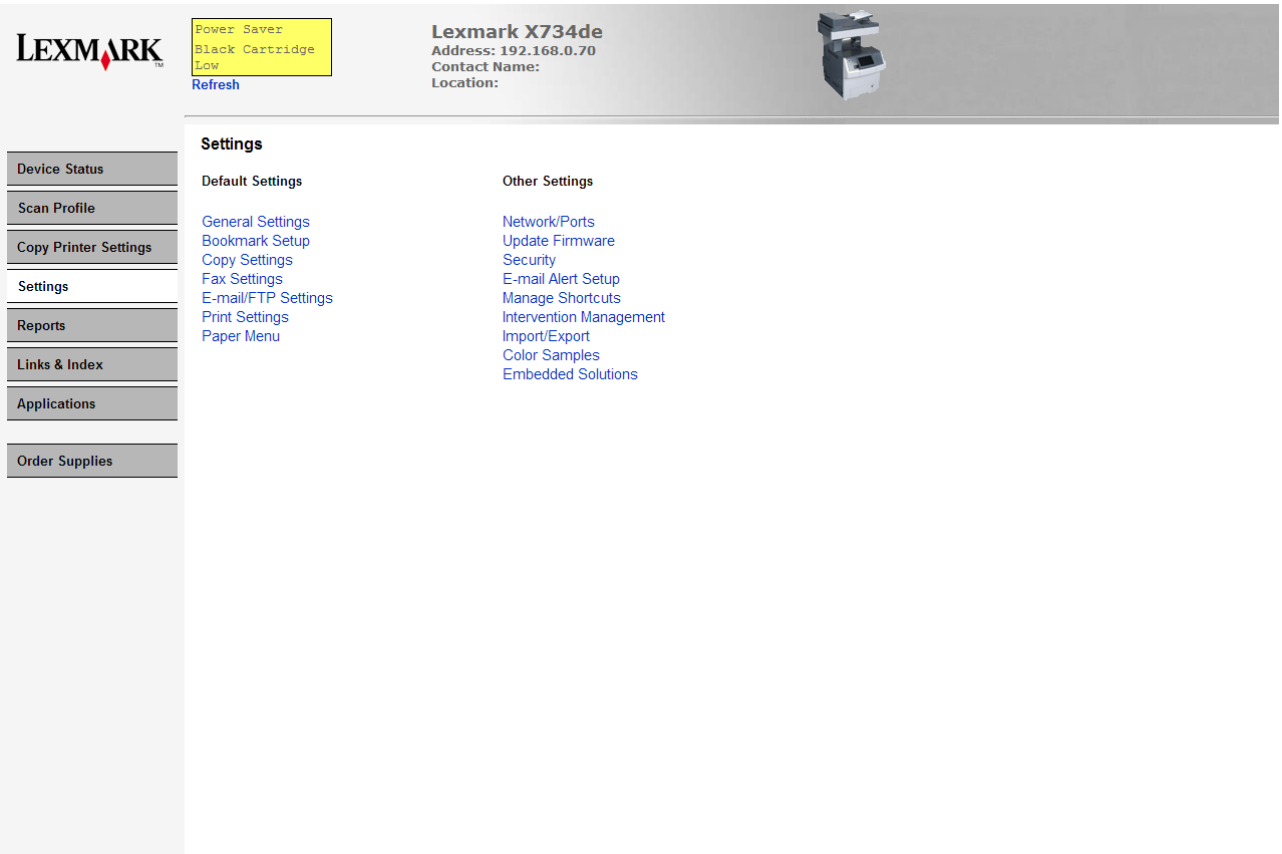
Steps to install

1. Install the Embedded Solution to MFP
2. Create the Security Template
3. Set the Access Controls
4. Configure Print Audit 6 and Print Audit Secure Server Settings

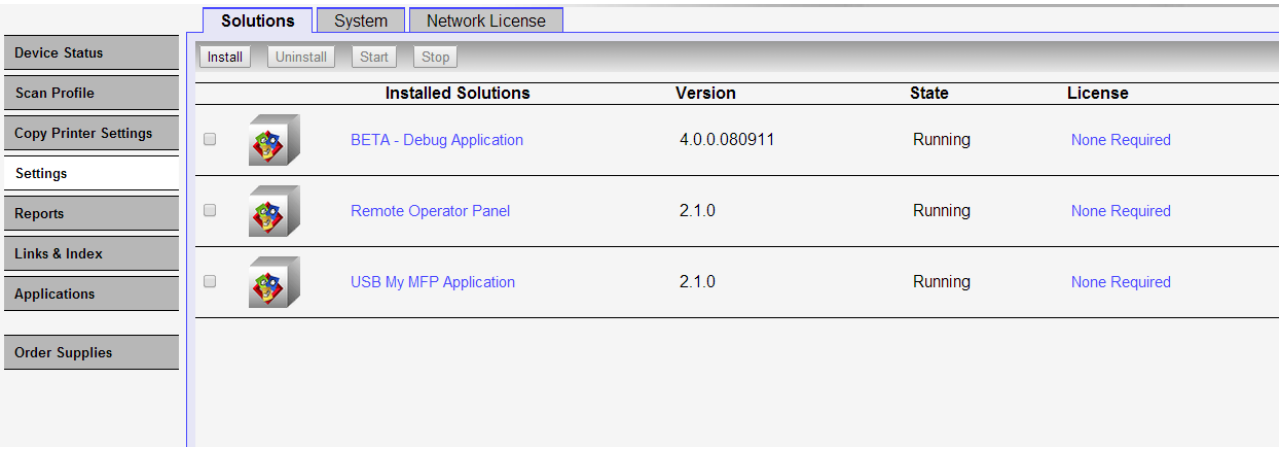
Install the Embedded Solution to MFP

Using a web browser, open the Lexmark MFP web interface

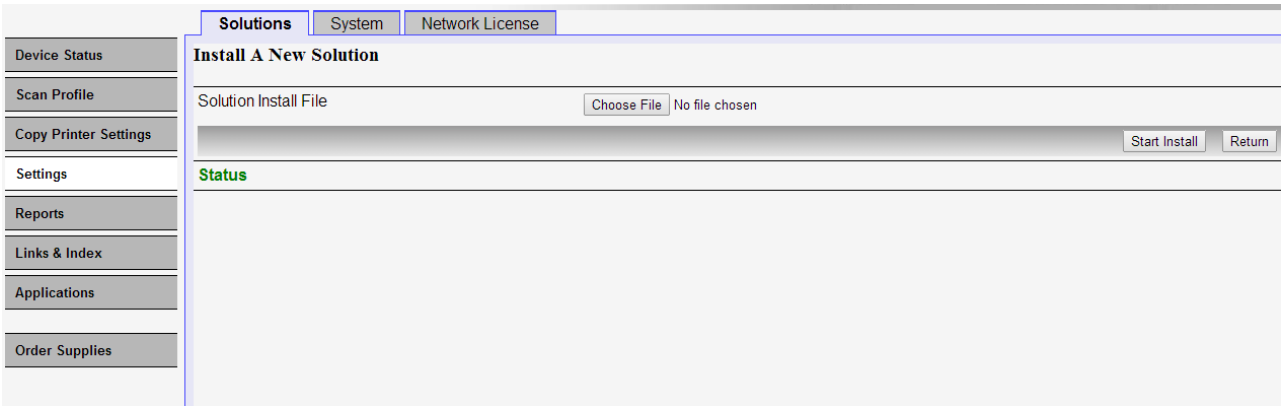
Select Settings from the menu of the left



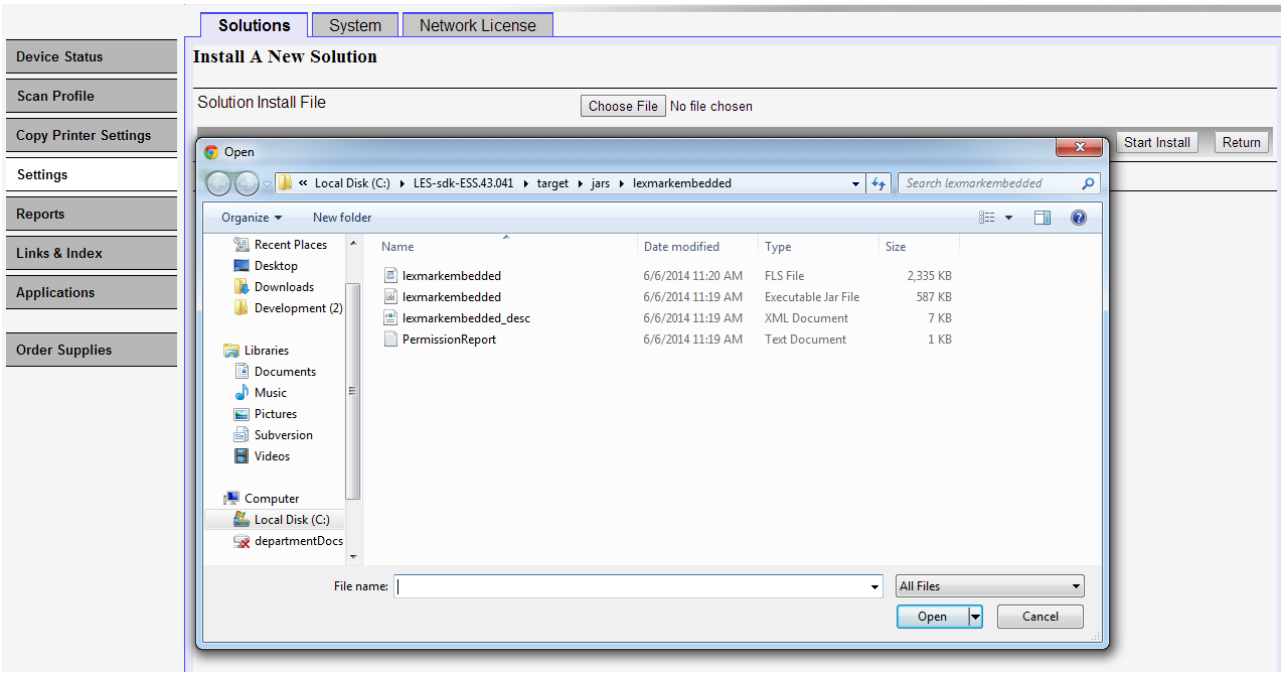
Select Embedded Solutions under Other Settings



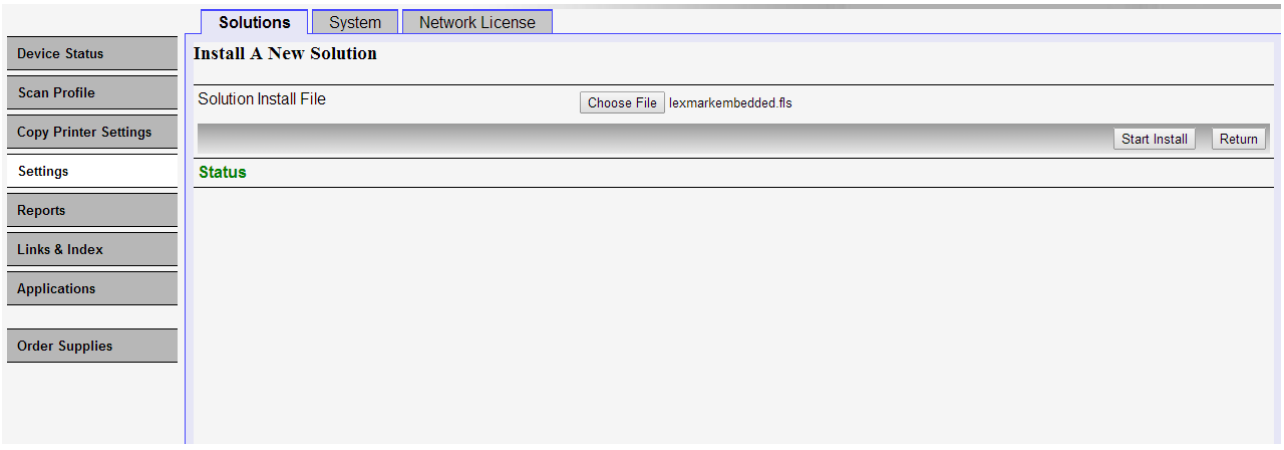
Click the Install button



Click the Choose File button



From the Open dialog, select the lexmarkembedded.fls file and click the Open button



Click the Start Install button

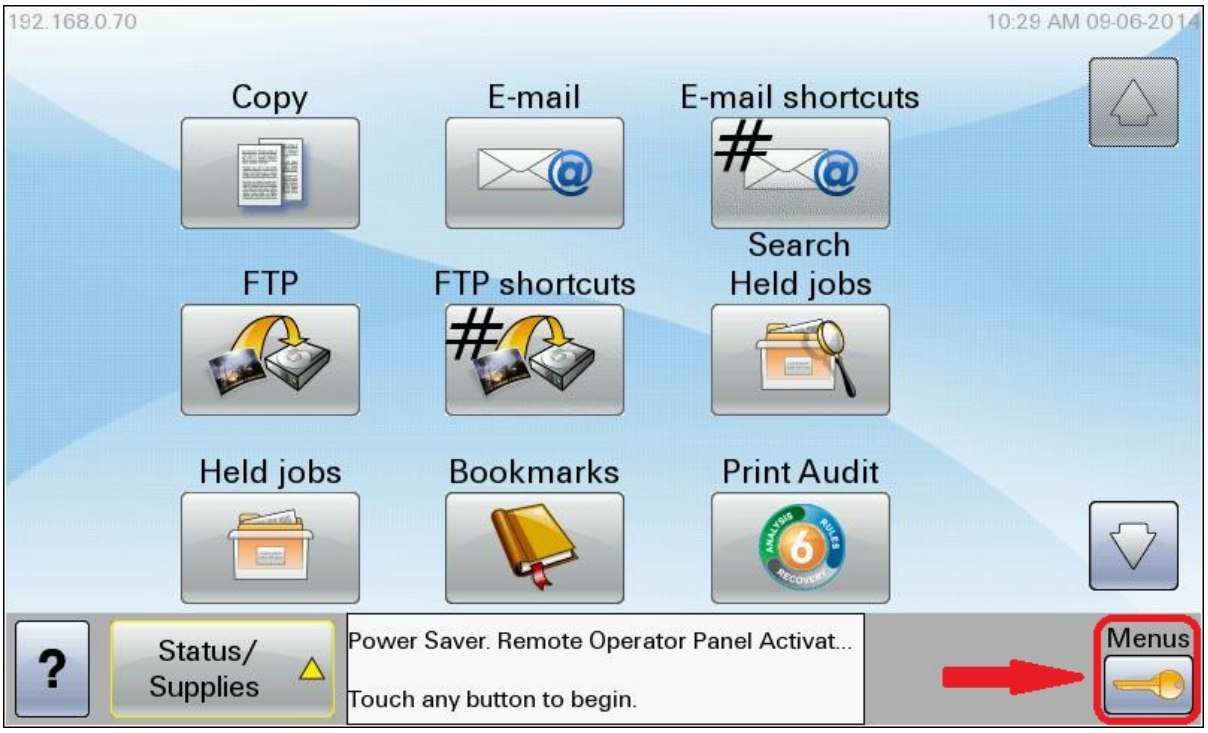
The install may take up to a minute. When the installation is done, you will see the message:

The following solutions were successfully installed.

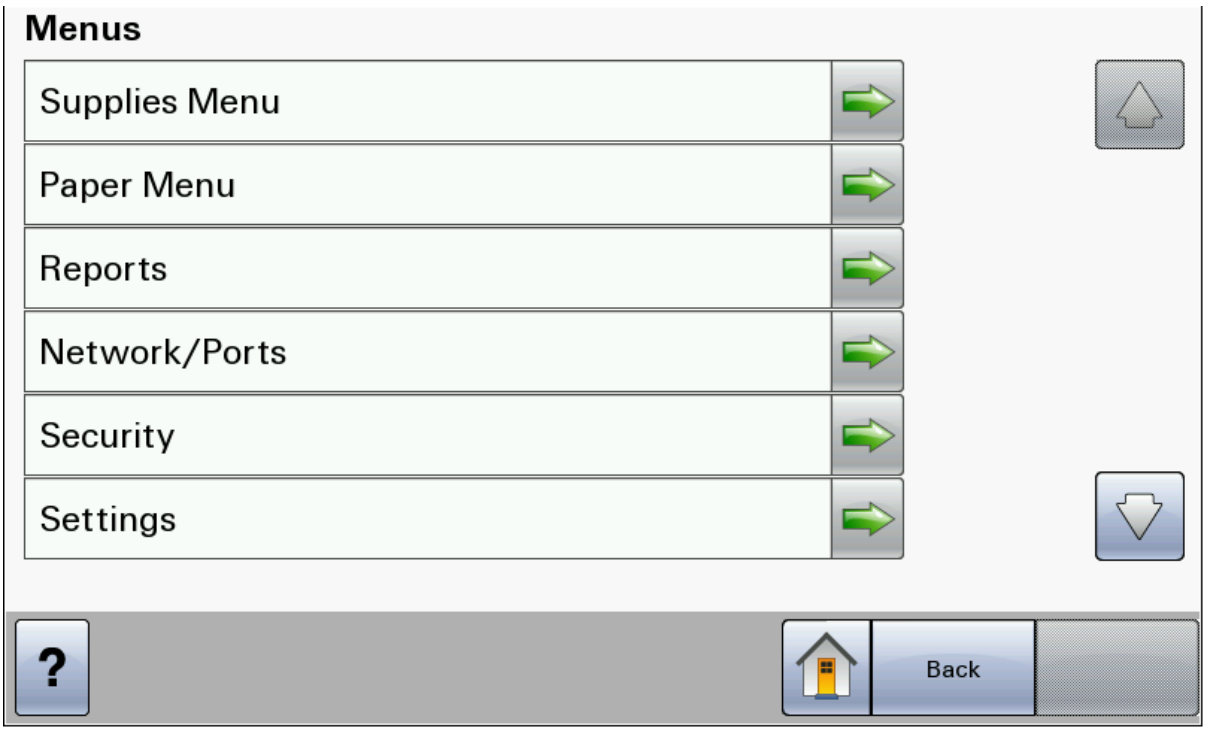
Print Audit Lexmark Embedded

Create the Security Template

Go to the Lexmark MFP panel

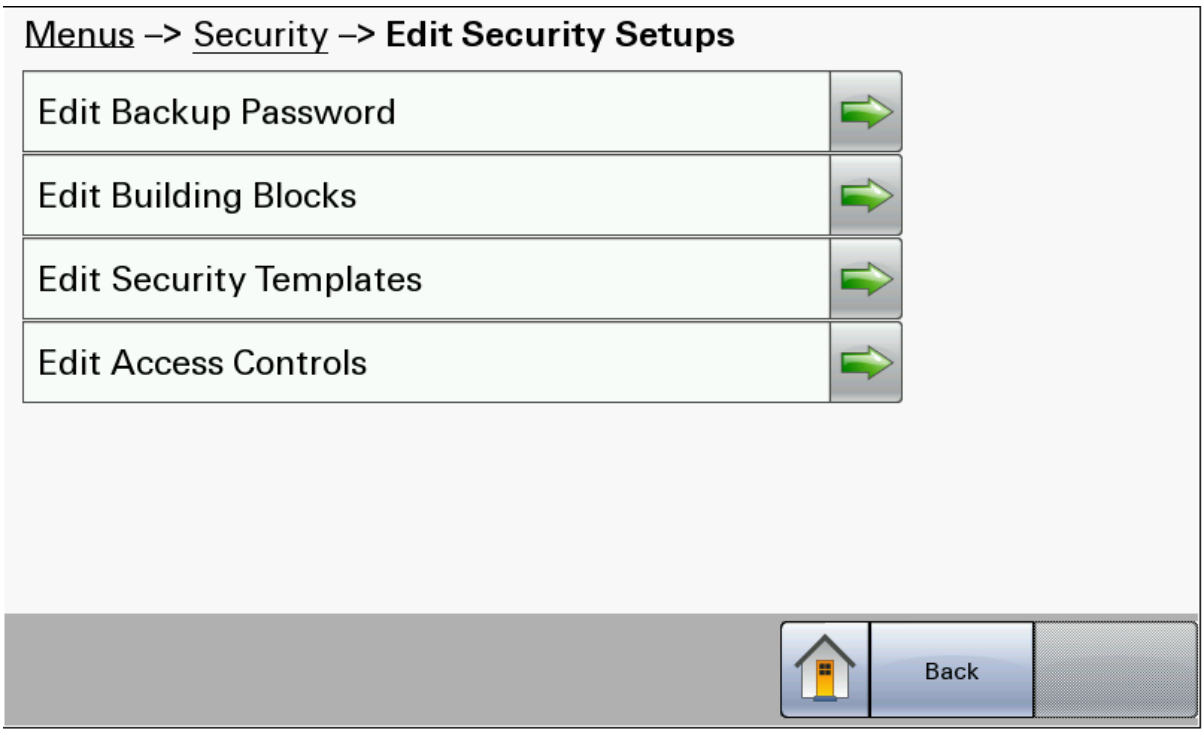


Go to Menus

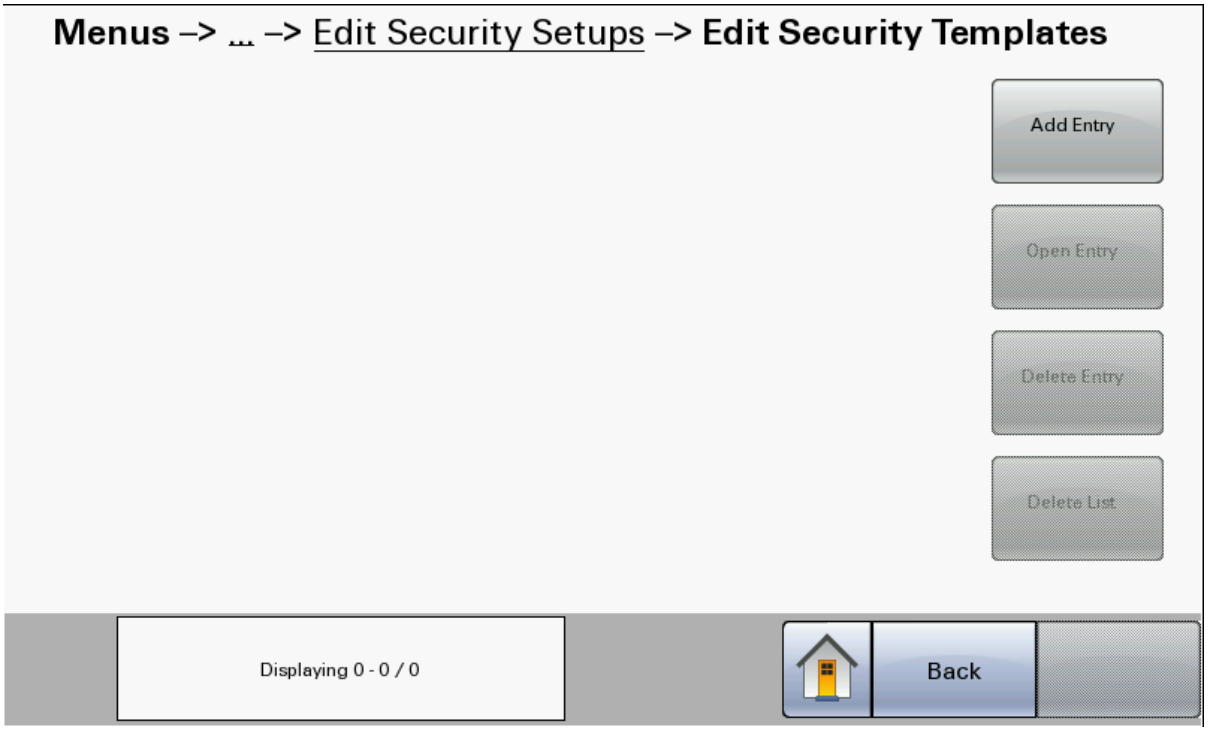


Select Security

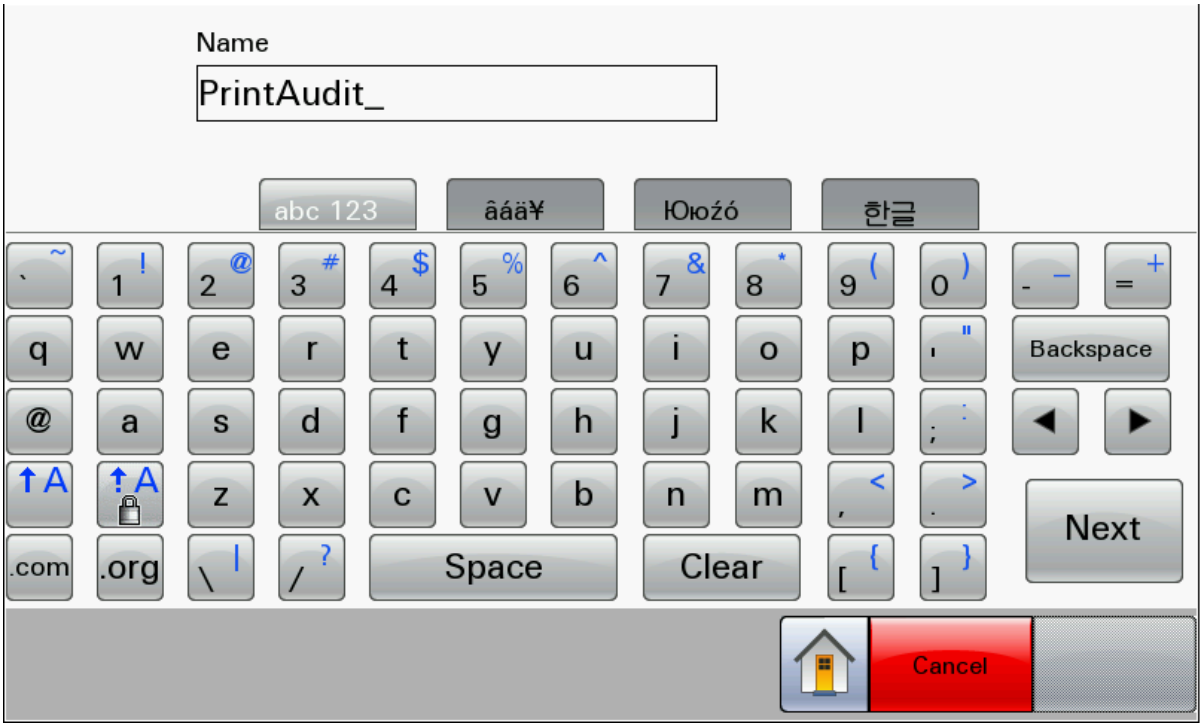
Select Edit Security Setups



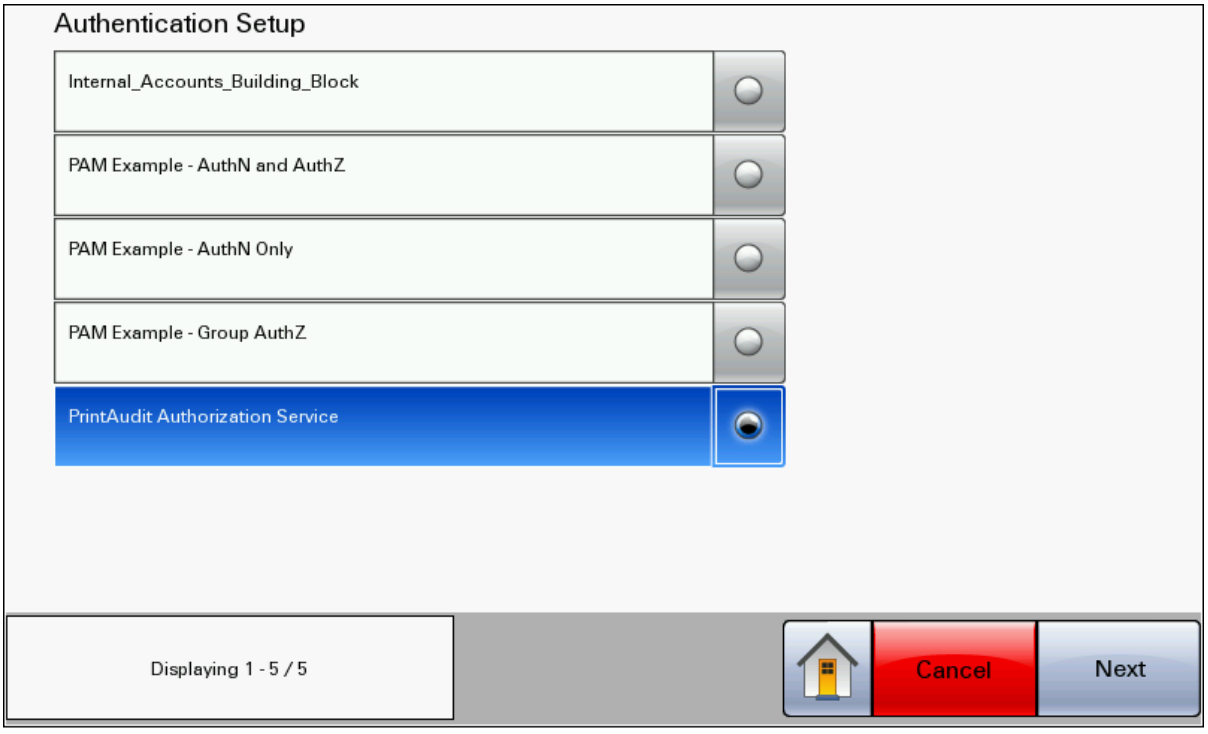
Select Edit Security Templates



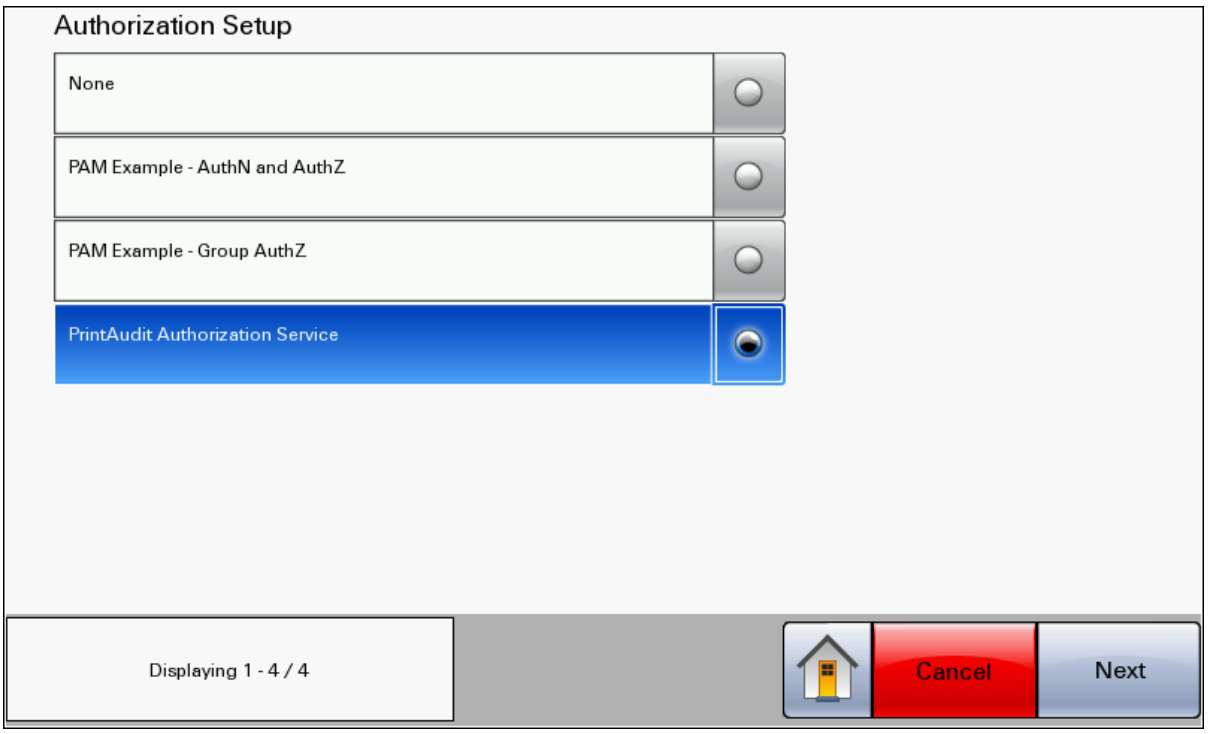
Click the Add Entry button



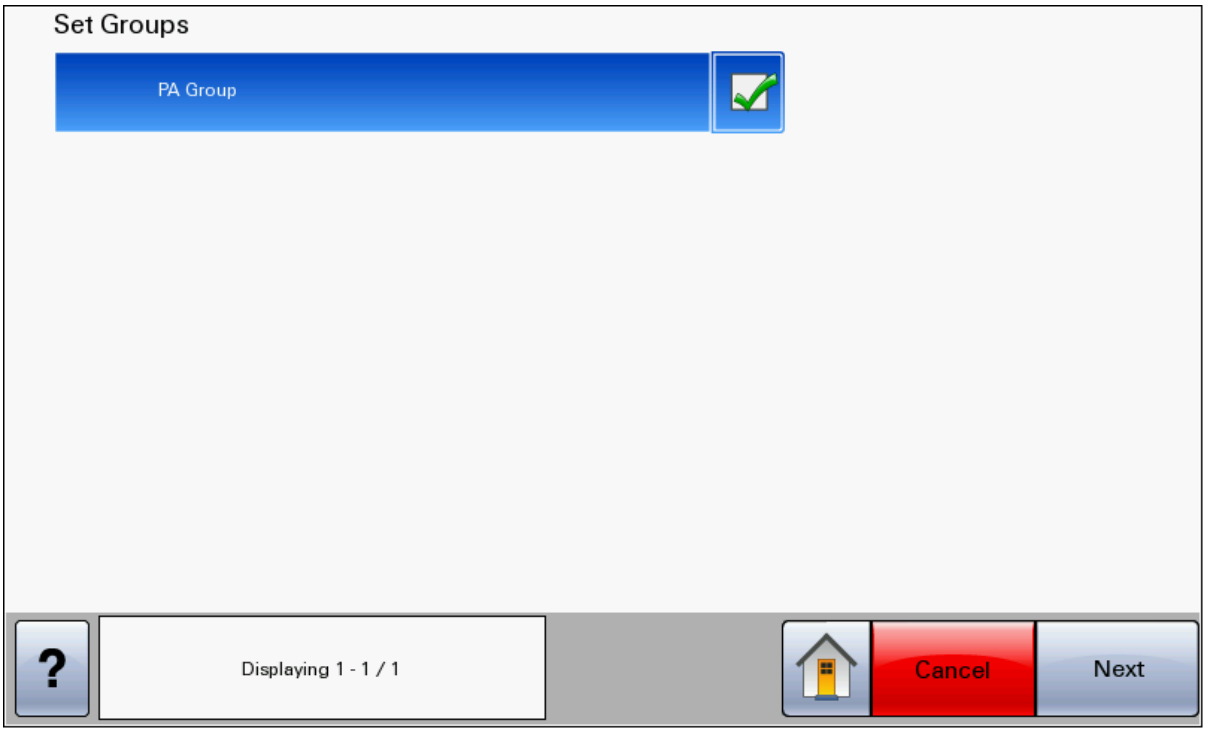
Create a name for the PrintAudit Security Template (use PrintAudit), and click the Next button



Select PrintAudit Authorization Service , and click the Next button



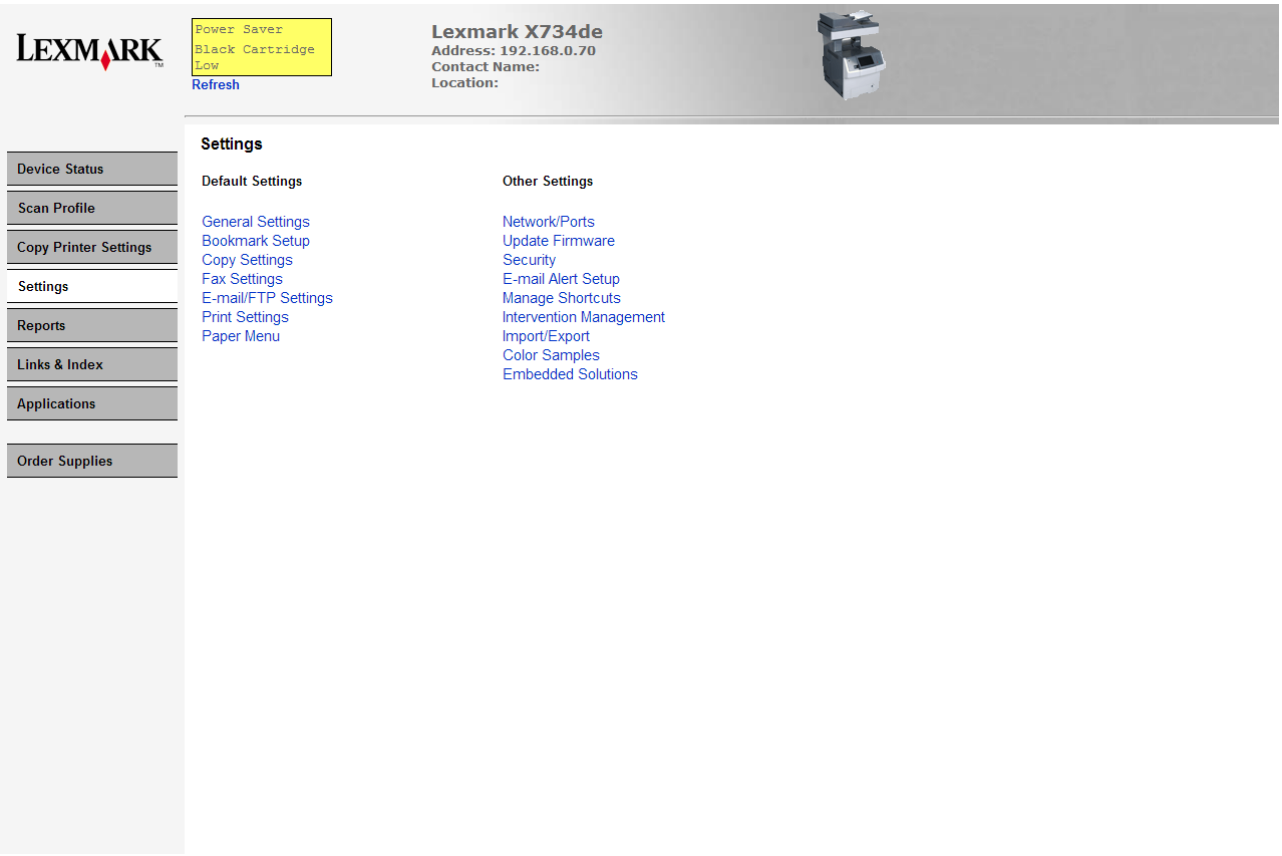
Select PA Group and click the Next button



The PrintAudit Security Template is now created

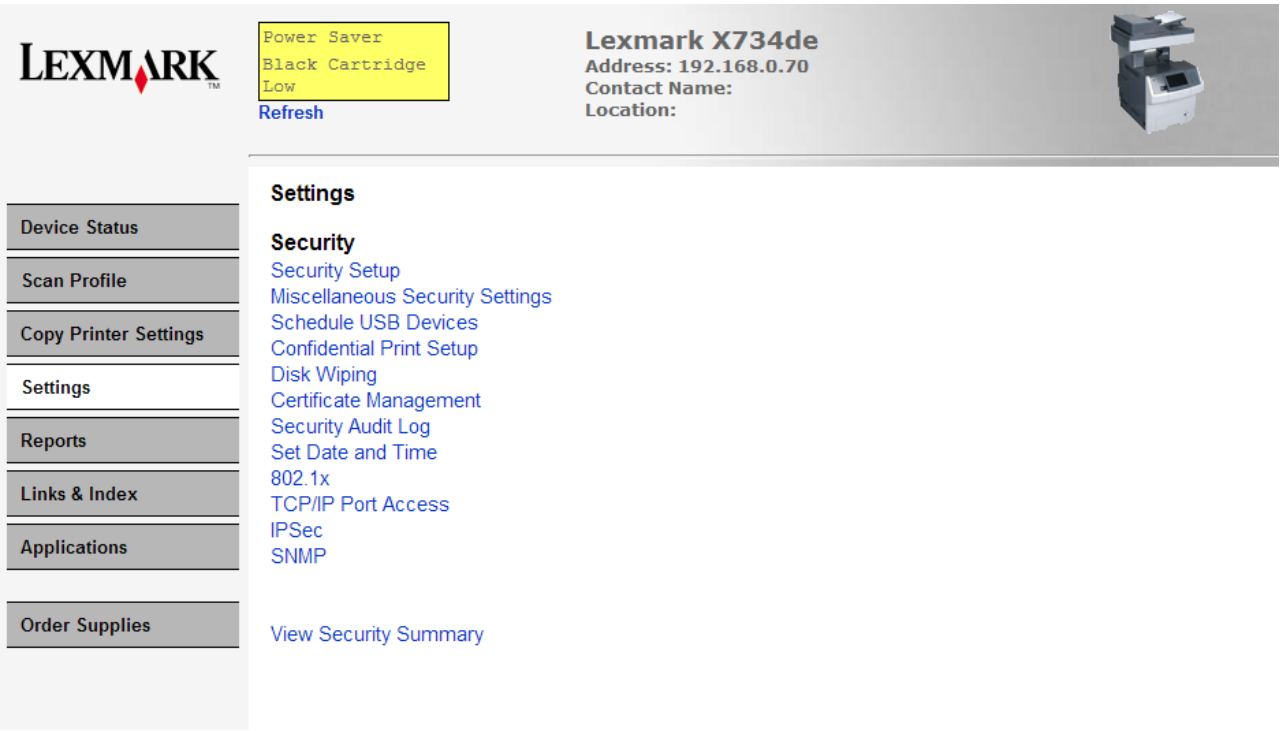
Set the Access Controls

Using a web browser, open the Lexmark MFP web interface

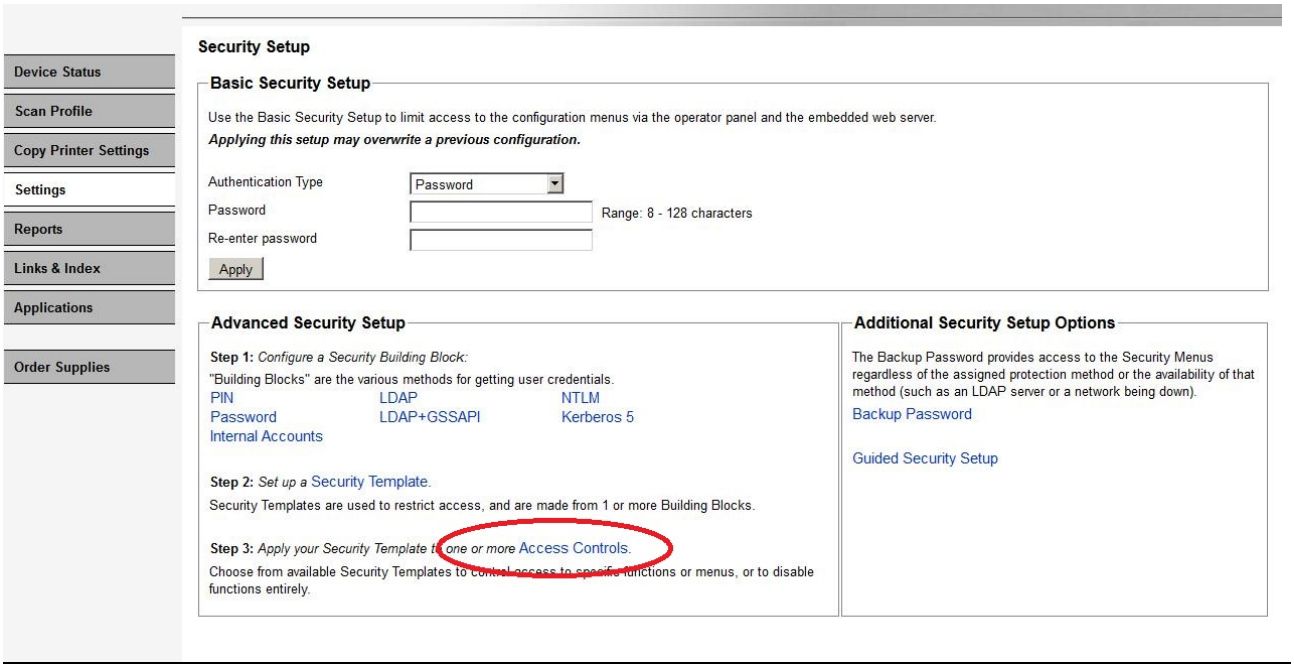


Select "Settings" from the menu on the left

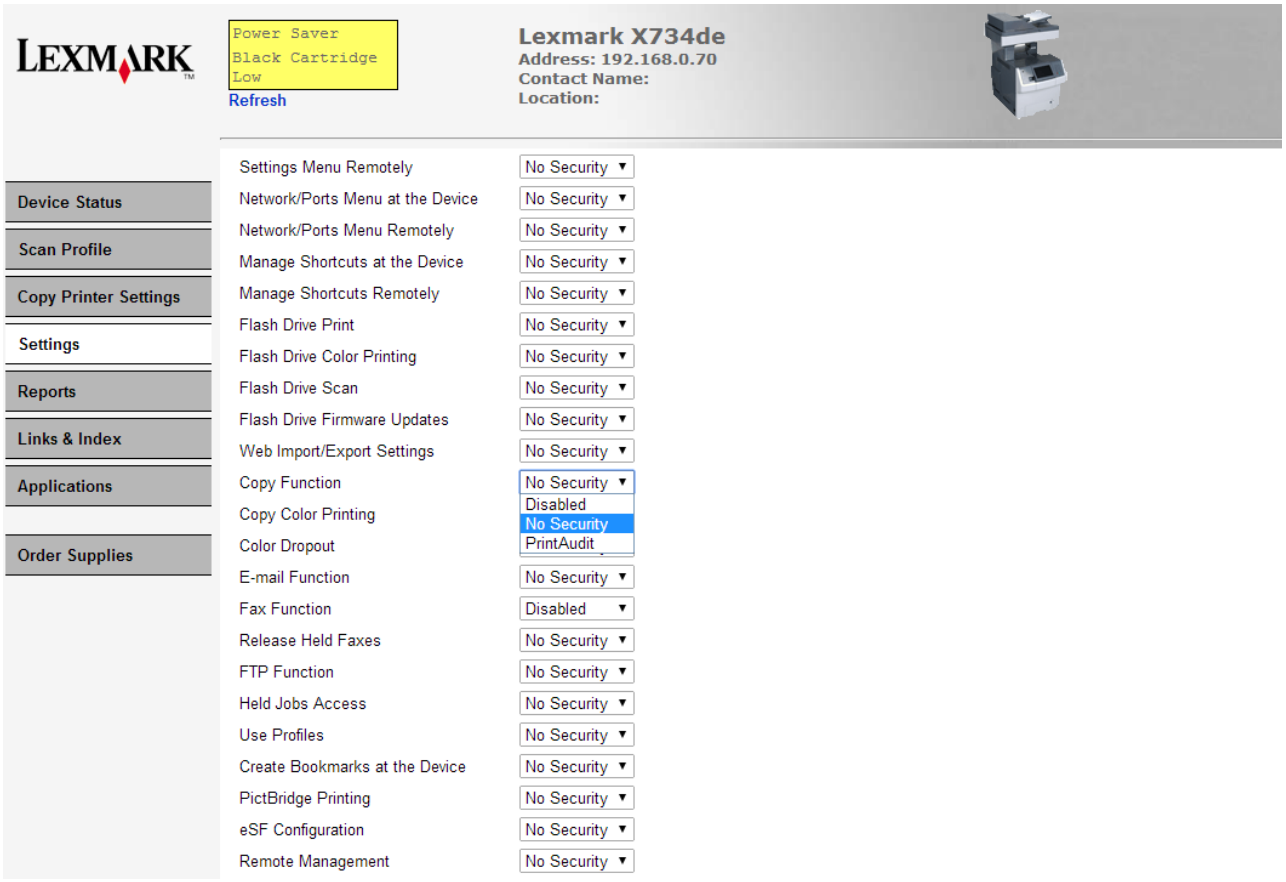
Select Security under Other Settings



Select Security Setup under Security



Select Access Controls



From the Edit Access Controls page, you can set MFP functions to use the PrintAudit security template, by selecting PrintAudit from a functions drop down control. The following functions should be set for the Lexmark PrintAudit embedded to work properly.

- Flash Drive Print

- Flash Drive Scan

- Copy Function

- Email Function

- Fax Function

- FTP Function

When you have completed setting the PrintAudit security template for the access controls, click the Submit button.

Configure the Print Audit and Print Audit Secure Settings

Basic Print Audit and Print Audit Secure settings can be applied through the Lexmark MFP Embedded webpage. These settings can also be applied through the Lexmark Embedded plugin in the Print Audit Administrator in addition to Advanced settings. Please see the <> below for further details.

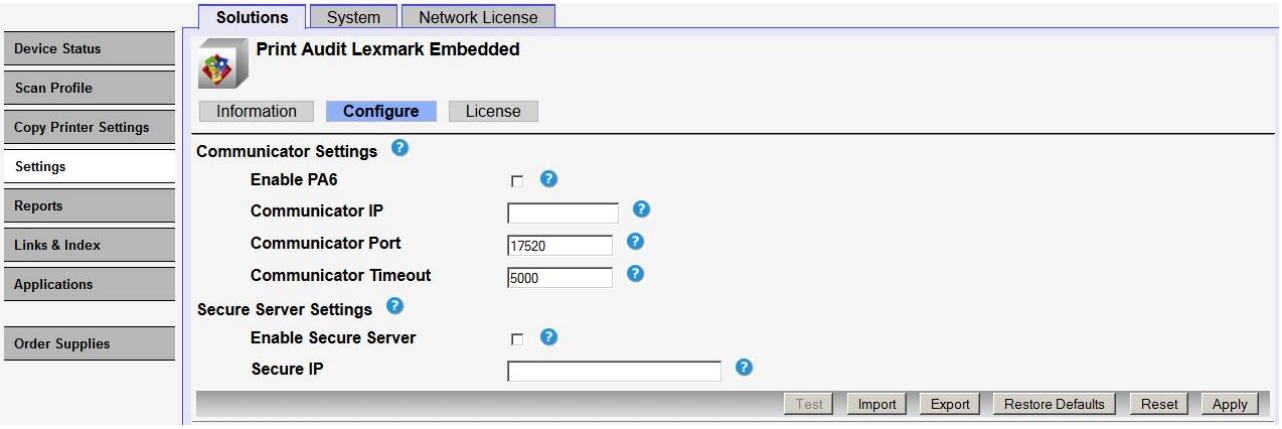
Using a browser, open the Lexmark MFP Embedded web page

Select Settings from the menu of the left

Select Embedded Solutions under Other Settings

Click on the link "Print Audit Lexmark Embedded"

Click on the "Configure" tab



Communicator Settings

- Enable PA6 - Enable tracking through Print Audit 6. Disabling this option removes the Print Audit 6 icon from the Lexmark MFP panel.
- Communicator IP - IP Address of the computer running the Database Communicator.

- Communicator Port - the port used to communicate with the Database Communicator. The default port is 17520.
- Communicator Timeout - the timeout value in milliseconds that the Embedded application will wait to communicate with the Database Communicator before a timeout occurs.

Secure Server Settings

- Enable Secure Server - Check this box to enable device to use Print Audit Secure Server.
- Secure IP - Print Audit Secure Server Web Site Location. The format is < SECURESERVERNAME>/pasecure/ where <SECURESERVERNAME> is either the Hostname or IP address of the computer running the Print Audit Secure Server application. For example, if the Secure Server name is "10.10.10.10." , the Secure IP set up would be 10.10.10.10\pasecure. Please note that "http://" is not required and if pre-populated should be removed.

When finished the configuration, click on "Apply" to save changes.

2. Configuration - Embedded for Lexmark

The following are instructions to configure Print Audit 6 with Lexmark Embedded.

Pre-configuration checklist

If you are ready to begin configuring Print Audit 6 with Embedded for Lexmark, you have:

- Installed the Print Audit Database Communicator, Database and Administration tools to a computer on the network that will be on and available at all times. The Print Audit Client should be installed on at least one workstation, to test printing and ensure that print jobs are being tracked correctly before continuing.
- Configured Print Audit 6 for user quotas, PIN codes and validated fields to be be integrated into Print Audit 6 Embedded.
- Used this guide to configure Print Audit 6 Embedded on the Lexmark eSF-enabled devices.

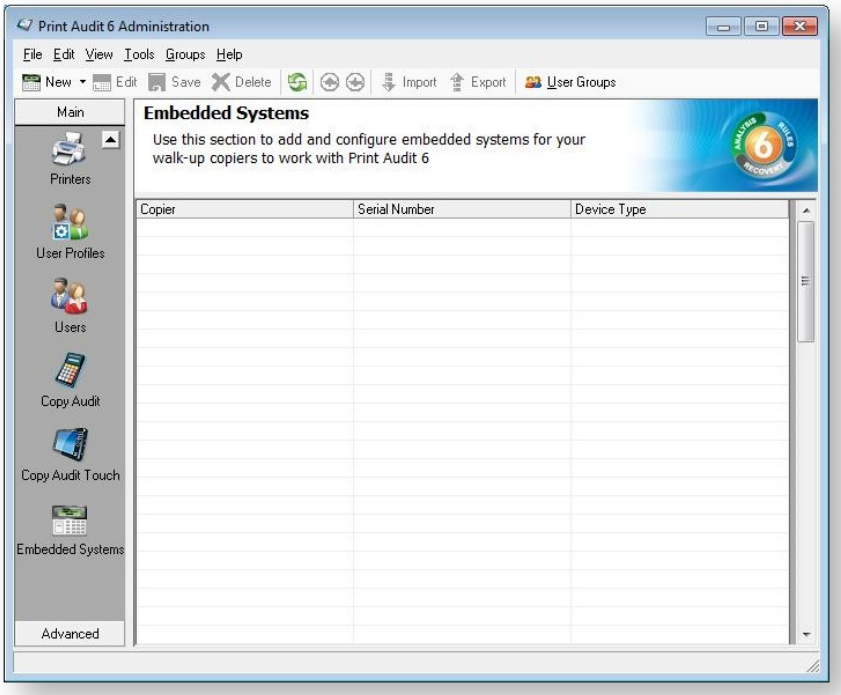
Overview

The Print Audit Administration tool provides the ability to configure Embedded for Lexmark on all the MFDs in the environment using the Embedded Systems plug-in. Configure one copier for every physical Lexmark MFD on which the Embedded Client will run.

Costs, restrictions, limits, authentication methods and custom fields may be configured for each device.

Adding, Editing and Deleting Copiers in Print Audit 6

Use the Embedded Systems section of the Administration tool to add, edit and delete Embedded for Lexmark copiers. A copier in the Administration tool represents a physical copier in the network.



To add a new copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Click the New button on the toolbar. The "Select Device Type" Window appears. From the drop down menu, select "Embedded for Lexmark".
4. At minimum, a copier name and the serial number of the copier must be provided. Please refer to the 'Embedded for Lexmark Configuration Window' section below for more information filling out the Embedded for Lexmark window.
5. Click the Save button. The Embedded for Lexmark Window closes and the copier appears in the Copiers list.

To edit a copier:

1. Run the Print Audit Administration program.

2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Edit button on the toolbar. The Embedded for Lexmark Window appears.
5. Make any needed changes to the copier.
6. Click the Save button. The Embedded for Lexmark Window closes and the copier appears in the Copiers list.

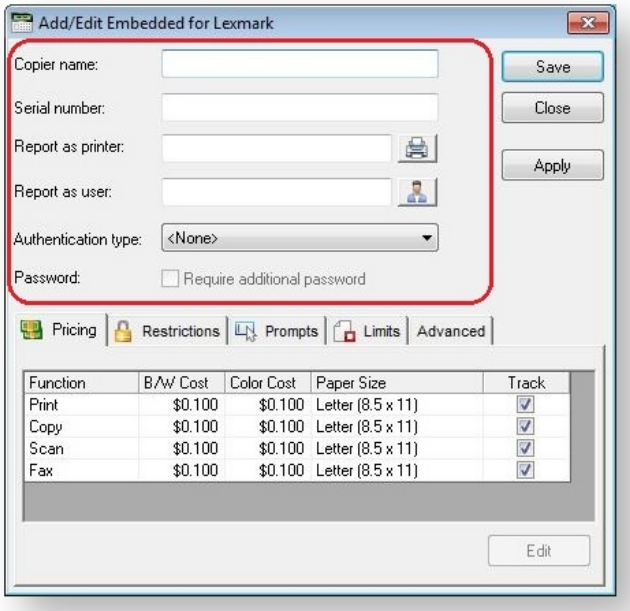
To delete a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Delete button on the toolbar. A message appears to verify removal of the copier.
5. Click the Yes button to delete the copier. The list of copiers refreshes.

Configuring the Lexmark MFP in Print Audit 6

This Embedded for Lexmark window in Print Audit 6 enables the configuration of all aspects of the Embedded for Lexmark copier device. The different elements of the window are described below.

General



Copier name - The name to describe the copier. Enter a name that is descriptive enough to distinguish the copier from others. For example " Third Floor Lexmark MX-7000N".

Serial number - The serial number of the Lexmark MFD.

Report as printer - Use this to select an already existing Print Audit printer with which to associate the copier. For example, if there is an MFD in the office that users print to which is already in the Print Audit database, choose that MFD here for the copier so that all transactions are reported as the same printer. If a printer is not selected here, Print Audit will record transactions for this copier as the copier name.

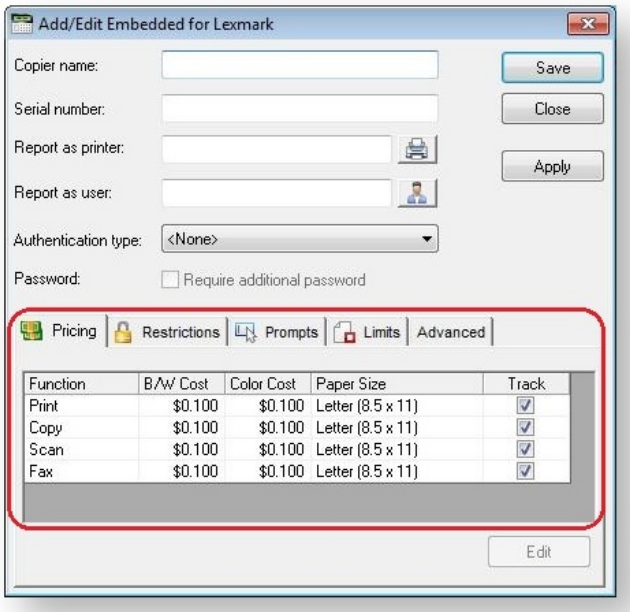
Report as user - Use this to select an existing Print Audit user whom to associate all jobs from this copier. Use this functionality to still have individual user authentication, but for reporting purposes report all jobs to a single user.

Authentication type - Select how the user will authenticate to the copier before they can do transactions.The authentication type determines how a user identifies themselves to the copier before they can do a transaction. The following options are available:

- None - Users do not have to authenticate before using the copier. All transactions are recorded to a generic user.
- PIN code - Users must enter their Print Audit PIN.
- Card Reader - Users must use their proximity card or swipe card to access the copier
- Card Reader or PIN - Users must use their proximity / swipe card or enter their Print Audit PIN to access the copier.

Require additional password - Check this box to require the user to enter an additional password before they can authenticate using the Authentication type selected above.

Pricing tab

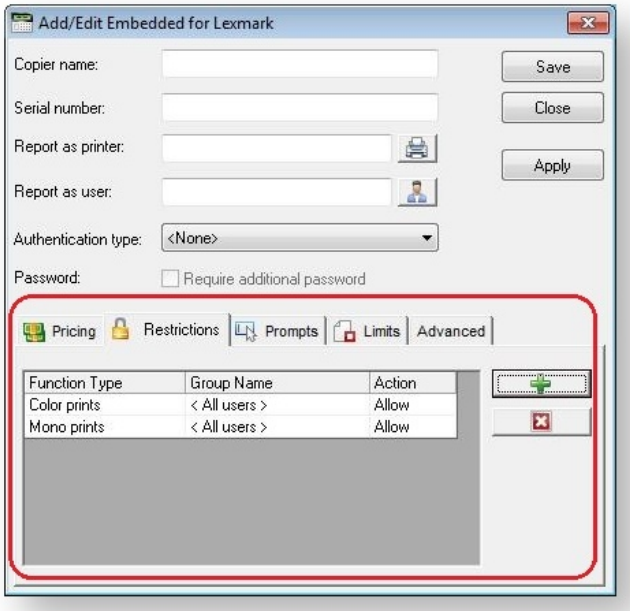


This tab contains the pricing for each function on the copier.

To edit the pricing for a particular function:

1. Clear the "Track" column for the function to disable the tracking of transactions of that type.
2. Select from the list the function that is to change and click the Edit button. The Configure Pricing and Paper Size Window appears.
3. Set the pricing as it makes sense for this copier in the organization.
4. Click the Done button. The Configure Pricing and Paper Size Window closes.

Restrictions tab (only with Print Audit 6 Rules)

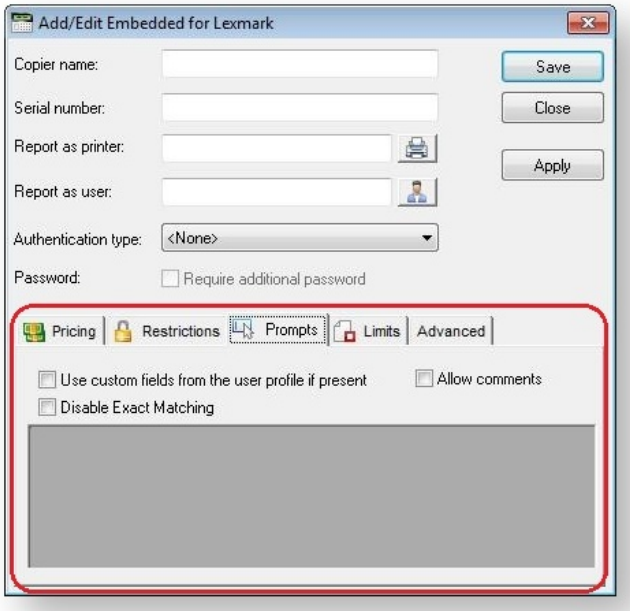


Choose to restrict access to the copier based on which user group a user belongs to.

Add button - Click this button to add a new restriction. The Configure Restriction Group window appears.

Remove button - Click this button to remove a restriction.

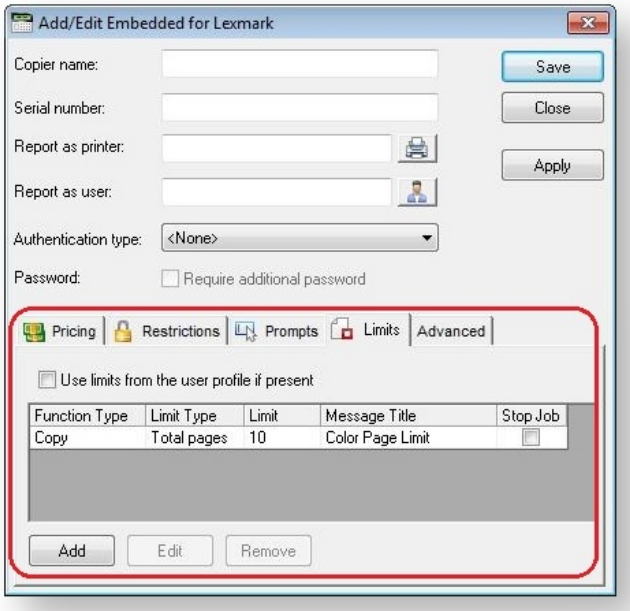
P rompts tab (only with Print Audit 6 Recovery)



This tab is only relevant when using Print Audit 6 Recovery for the charge-back of printing.

- For each Activity the user can be required to enter values for Custom Fields. Custom Fields are setup in the Custom Fields section of the Print Audit Administrator. On this tab, select from any one of the Custom Fields configured and define a custom prompt for each one.
- Use custom fields from the user profile - Check this box to override the default custom field choices with the custom fields set in a user's User Profile.
- Allow comments - Check this box if the user can enter general comments about the job.
- Custom fields - The custom fields list contains all custom fields that have been defined. To use a custom field for the activity, check the Include check box.

Limits tab (only with Print Audit 6 Rules)



This tab is only relevant when using Print Audit 6 Rules to enforce rules-based printing.

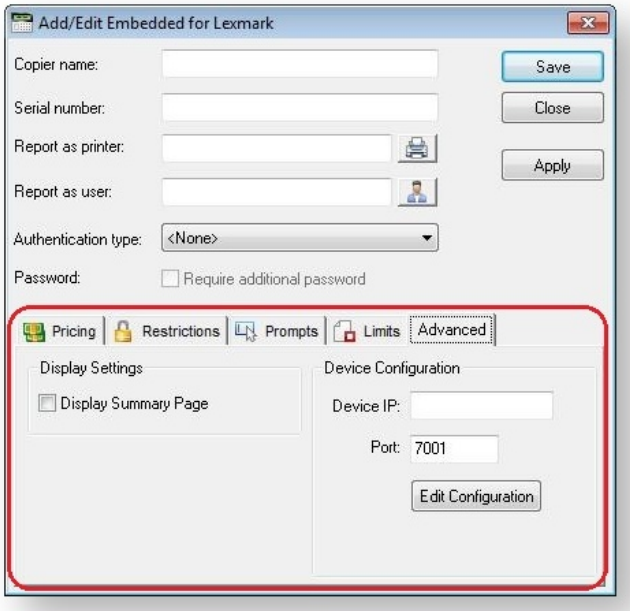
Use limits from the user profile - Check this to use limits defined in a user's profile instead of the limits defined here.

Add - Click this to add a new printing limit.

Edit - Click this to edit an existing limit.

Remove - Click this to remove an existing limit.

Advanced tab



This tab is used for pushing Print Audit and Print Audit Secure configuration out to the Lexmark device remotely as well as configuring advance features for the device.

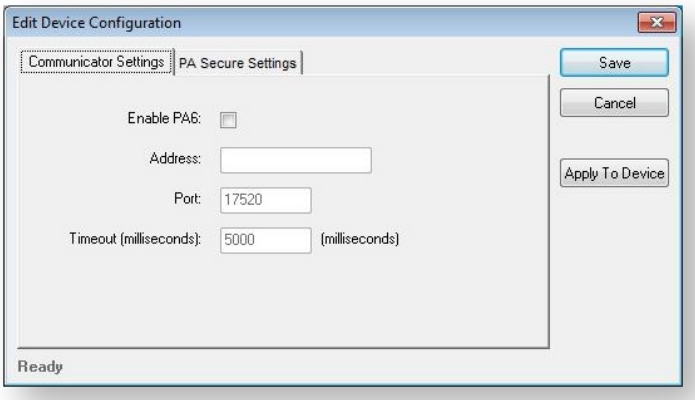
Display Summary Page - check this box to display a summary of the transaction after the job is completed.

Device IP - IP address of the Lexmark device. Note: this field is required before you can edit the configuration for the device.

Port - port used to communicate with the Lexmark device. Note: the Print Audit Embedded for Lexmark software uses port 7001.

Edit Configuration

Communicator Settings



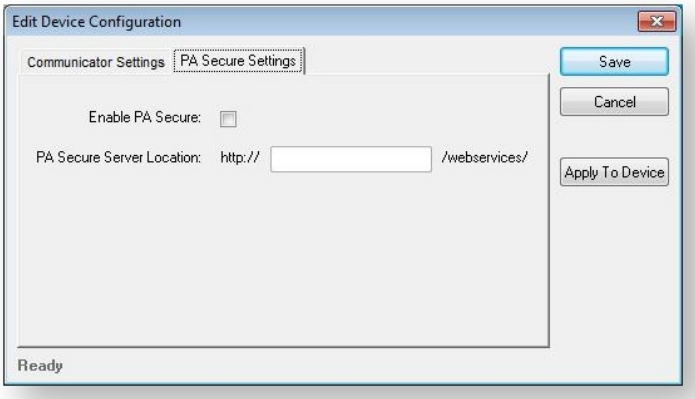
Enable PA6 - Check this box to enable the Print Audit Embedded (for Print/Scan/Fax) on the device.

Address - This is the IP address or the Hostname of the machine hosting the Database Communicator.

Port - This is the port that the Database Communicator is configured to listen on.

Timeout (milliseconds) - Configured this to set the amount of time that the Lexmark device will wait for a connection to the Database Communicator before it generates a timeout error. The time is set in milliseconds.

PA Secure Settings



Enable PA Secure - Check this box to enable the Print Audit Secure on the device.

PA Secure Server Location - Print Audit Secure Server web site location . The format is < SECURESERVERNAME>/pasecure/ where <SECURESERVERNAME> is either the Hostname or the IP address of the computer running the Print Audit Secure Server application.

Repeat the above steps for each Lexmark MFP on which Embedded for Lexmark will be used.

3. Using Lexmark Embedded with Print Audit 6

The Embedded for Lexmark Client is very easy to use. It will first prompt for required identification or billing information, before enabling the device for copy, scan, fax, or print functionality. Once the desired function is complete, return to the panel and complete the session, otherwise the MFP will timeout the session. When the session ends, the copy, scan, fax, or print transaction is sent to the Print Audit 6 database, and the Embedded Client resets to be ready for the next user.

The standard set of steps to using Embedded for Lexmark to track job information is as follows:

1. **Start the Transaction -** Press the Start button on the screen. The Embedded Client retrieves its configuration and proceeds to prompt for the required information. The Cancel button can be used at any time to return to the Start screen.

1. **Authenticate -** If configured to ask for a PIN Code, the Embedded Client displays a login screen. To login:
    a. Press the PIN Code button. An input form displays.
    b. Enter a PIN Code using the Lexmark keyboard or the touch screen.
    c. Press the OK button to accept the input.
    d. Press the OK button on the Login screen to validate the PIN Code.
2. **Enter Custom Field Information -** If configured to ask for Custom Field information, the Embedded Client will prompt for on or more values from the user. To enter values for a searchable field:
    a. Press the button on the touch screen that corresponds to the Custom Field Name.
    b. Enter a full or partial code on the screen and click OK.
    c. If only one match is found for the field, the Embedded Client asks for the next Custom Field value if any is configured.
    d. If Print Audit finds more than one match, a list of values will display. Use the touch screen to navigate through the values.

e. When the desired value is found, press the button corresponding to the value. It appears highlighted.

f. Press the OK button to accept the value.

g. Press the OK button again to move to the next screen.

3. **To enter values for a non-searchable field:**

   a. Press the button that corresponds to the desired value. It appears highlighted.

   b. Use the arrows on the touch screen to navigate through the choices.

   c. Press the OK button to accept the value. The Embedded Client will request the next Custom Field value if any is configured.

4. **Enter any Comments -** If configured, the Embedded Client will request any Comments for the job. Press OK if to proceed without entering comments. To enter comments:

   a. Press the Comments button on the touch screen. An input form appears.

   b. Use the input form to enter comments.

   c. Press the OK button to close the input form.

   d. Press the OK button on the Comments screen to accept the comments.

5. **Verify Selections -** After all information has been input, a summary screen appears showing the current balance if any, along with the custom values selected. Press the OK button to accept the selections and begin the job.

6. **Complete the Job -** After the job is completed, press the "**" (Logout)" button on the Lexmark MFP keypad. This completes the transaction, and transmits the job information to the Print Audit database. If the "**" (Logout)" button is not used to end the session, the Lexmark MFP will eventually timeout the session, return to the Start screen and transmit the job information to the Print Audit database.

Note

If declining balances are enabled for the current user each copy/fax/scan operation will debit the account balance in real-time. Once the balance of the current user reaches zero all MFP copy/fax/scan functions will be locked for that user until such time that the user logs in again with a positive balance.

4. Using Lexmark Embedded with Print Audit Secure

The Print Audit Secure Embedded for Lexmark Client is very easy to use. It will first prompt for required information. The prompts which appear are dependent on how the Secure Embedded Client is configured. Once the prompted information is provided, the device will release the secure job(s). Then the Secure Embedded Client resets to be ready for the next user. If the session is not manually finished, the Lexmark MFP will timeout.

Following, are the standard set of steps to using Secure Embedded for Lexmark to release a print job.

1. Authenticate

1. **PIN Code authentication -** If configured to request a PIN Code, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Pin Code Field
    b. Enter a PIN Code using the Lexmark keyboard or the touch screen.
    c. Press the Login button to accept the input.
2. **Authenticate with a Username -** If configured to ask for a Username, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Username Field
    b. Enter a Username
    c. Click on the Password Field
    d. Enter a Password
    e. Press the Login button to accept the input.
3. **Authenticate with a swipe card -** If configured to ask for a swipe card, the Secure Embedded Client displays a login screen. To login:
    a. Swipe a card in a card reader attached to the MFP.

2. Release Print Jobs

1. To release all the compatible print jobs, click the Release All button.
2. To release only certain jobs, press the checkbox next to the jobs to be released.
3. Click the Release button. The selected job(s) will now print.

3. Delete Print Jobs

To delete print jobs, press the checkbox next to the jobs to be remove and press the Delete button.

4. Complete the Job

When finished releasing print jobs, press the Logout button on the Lexmark MFP screen. This will notify Print Audit Secure that the transaction is complete. If this step is not completed, the Lexmark MFP will eventually reset back to the Start screen.

5. Troubleshooting - Embedded for Lexmark

Please refer to this section if issues are encountered with the operation of Embedded for Lexmark. If a resolution is not found in this section, please contact Print Audit technical support.

Receiving error "Error launching Print Audit Secure - Print Audit Secure could not be launched. Please contact your administrator".

This error occurs when the Lexmark device cannot contact the PA Secure Server Location.

1. Verify that the web service URL (contained in the Print Audit Embedded for Lexmark plugin or in the Secure Server Settings section of the Configure embedded page) is correct.
2. Verify that the Secure Server is correctly installed and is accessible.

Receiving error "User ID not authorized for access"

This message will appear when there is a restriction set up in the Print Audit Administrator Lexmark plugin that restricts the user from accessing the MFP function.

When I select a a function on the Lexmark device, I don't receive a prompt for any code.

1. Verify that the Database Communicator settings are correct and that the Database Communicator Service is running.
    a. Verify that the Database Communicator settings are correct in the Print Audit Embedded for Lexmark plugin or in the Secure Server Settings section of the Configure embedded page.
    b. Open the Communicator Configuration and verify that the Database Communicator is running.
2. Verify that there is a valid license for Lexmark Embedded (eSF).
    a. Open the Print Audit Administrator.
    b. Go to "Tools --> View/Change License".
    c. Click on the "Connectors and Addons" tab.
    d. Verify that there are sufficient licenses for "Lexmark Embedded (eSF)" in the Connector/Addon list.

3. Verify that the Lexmark has been configured in the Print Audit Administrator.
    a. The serial number for the device is correct.
    b. An Authentication type or a custom field prompt has been set up for the device.

Embedded For Sharp Documentation

Print Audit Embedded installs directly onto supported Sharp OSA® -enabled multifunction peripherals, allowing users to control and recover all printing, copying, faxing and scanning costs. Review the documentation below for help installing and configuring Print Audit Embedded. You can also use the Knowledge Base to find more information.

Browse Documents:

Browse Other Product Documentation:

Print Audit 6 Infinite Device Management Print Audit Secure Rapid Assessment Key Embedded for Sharp

Embedded for Kyocera Mita Embedded for Lexmark Embedded for Xerox Embedded for HP

Copy Audit Touch Copy Audit Numeric

Embedded for Sharp-Install and Setup

Print Audit Embedded for Sharp is used alongside Print Audit 6 to provide authenticated access to Sharp MFPs, for the purpose of securing device functionality, and tracking usage. Users must authenticate at the MFP, by login, PIN, or card swipe identification, before they may access MFP functions.

When additionally used in conjunction with Print Audit Secure, users will also be able to select and release secure print documents directly from the MFP panel.
This guide provides instructions to install and configure Embedded for Sharp with Print Audit 6.

When used with Print Audit 6, Embedded for Sharp will track:

- walk-up copying
- scanning
- faxing
- printing from the document server

When Print Audit Secure is added, Embedded for Sharp can additionally provide:

- secure release of all printing
- Follow Me printing

Components

Embedded for Sharp consists of two main components:

1. Print Audit 6 - Embedded for Sharp Configuration:

Embedded for Sharp is configured using the Embedded Systems plug-in for the Print Audit 6 Administration tool. Support for Embedded for Sharp exists in Print Audit 6.1.0 or newer.

2. Embedded Client:

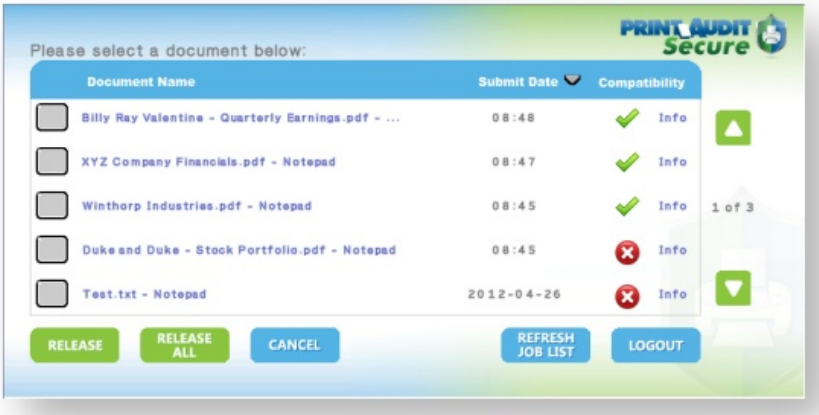
This software runs on the MFP. The Embedded Client provides a user interface directly on the panel of the Sharp MFP to enable the tracking of copies, scans or faxes, or the printing of documents stored in the MFP's Document Server.

In addition to tracking the number of pages in a copy, scan, fax, or print job, the Embedded Client tracks additional information about the job. For example, the Embedded Client can request a PIN Code from the user to identify and track who is creating the photocopy. Or, it can request a Client Code to identify which customer or cost center should be billed for a fax transmission.

Print Audit 6

Print Audit 6 is a client application that tracks all printing directly from the desktop where the print job was issued. Every job, along with its attributes, are collected and stored in the Print Audit database, where it is available for reporting on printing volume and trends.
Print Audit 6 is available in 3 different modules, Analysis, Rules, and Recovery, which respectively, enable Analysis Reporting from the collected print data, the ability to create printing rules for rules-based printing, and the ability to allocate the cost of print jobs to a user, customer, or cost center.
When used with Embedded for Sharp, Print Audit 6 can also track copy, scan, and fax jobs, and jobs that are printed from the document server.

Print Audit Secure



Print Audit Secure on Sharp OSA-enabled device

Print Audit Secure allows for print jobs to be held on the server until an authenticated user releases them from the MFP panel, or from a Print Audit Secure release station. When a printer is managed by Print Audit Secure, incoming print jobs are prevented from being automatically output, by holding them in a secure queue on the server. When used with Embedded for Sharp, users will authenticate at the MFP, view their held jobs on the MFP panel, select one or more jobs and release or delete them directly from the MFP front panel.

Authentication Devices

Print Audit Embedded for Sharp OSA supports Authentication Devices, such as swipe card or proximity card readers, within an Embedded for Sharp environment. When an Authentication Device is configured in an environment with Embedded for Sharp, users must authenticate at an Authentication Device before they are allowed to access the supported Sharp MFP controlled by the device.

Licensing

To enable the Print Audit Embedded for Sharp OSA the following is required:

1. **One Print Audit Embedded for Sharp OSA license per controlled Sharp MFP -** Print Audit, Embedded for Sharp is licensed on a per-MFP basis. To install Embedded for Sharp on 15 MFPs, licenses must be purchased for each of the 15 MFPs. MFP licenses can be purchased as part of any Print Audit license, and are additional to the Print Audit 6 client licenses needed to track print jobs originating from Microsoft Windows and Apple Macintosh workstations. In the event that there are insufficient licenses, Print Audit will stop tracking some or all of the MFPs—MFPs will continue to function as normal, but no information will be tracked.

2. **OSA–enabled Sharp MFPs -** Print Audit Embedded for Sharp OSA is only supported on OSA-enabled MFPs.
3. **Print Audit 6.6 or higher -** Print Audit Embedded for Sharp requires Print Audit 6 to configure the MFPs. Consult the Print Audit 6 Installation Guide for more information.

Optional

1. **Print Audit Secure 1.1 or higher -** Consult the Print Audit Secure Installation instructions for more information
2. **One Authentication Device per Sharp MFP-** Print Audit Embedded for Sharp OSA supports HID proximity and contactless smart cards for authentication. Users can enter validation data by presenting the card at the card reader. If an authentication devices are to be used in the environment, one authentication device is required per MFP.

1. Installation

This section only addresses the installation requirements and configuration of Print Audit 6 for use with Embedded for Sharp. For complete instructions on installing and configuring Print Audit 6, please refer to the Print Audit 6 Installation information found online. Refer to that documentation to perform the following steps to install Print Audit 6 in conjunction with Print Audit Embedded for Sharp.

System Requirements

- **Windows 2000 or newer**
- **MS-SQL Server 2005 Express or better -** running embedded applications on with an Access database is not recommended.
- **Print Audit 6.8.0** or newer*
    - download the latest version from www.printaudit.com.
    - The Print Audit 6 Database Communicator, Database, and Administrative tools must be installed on a Windows 2000 or newer computer with Internet Explorer version 4.0 or newer.
- **Internet Information Services (IIS)**
    - IIS must be installed before .Net4
    - If running IIS 7, other IIS subcomponents will need to be installed such as Web Management Tools and .NET Extensibility, ASP.NET, ISAPI Extensions & filters. These features can be turned on by using Window Features in the Programs and Features on the Windows Control Panel.

- *IIS is included in Windows 2000 or newer and can be installed with Windows or through the Windows Components of Add/Remove Programs application in the Control Panel. IIS 7.0 (Included in Windows 2008 and Windows Vista) requires that the IIS 6 Management Compatibility component is installed as well.*

- **.Net 4.0**
  - If the .Net framework was installed before IIS, then the framework must be reinstalled to ensure the .NET components are registered properly with IIS. IIS cannot be configured correctly if .NET is installed first.
  - *For more information or to download .Net, go Microsoft's website (www.microsoft.com) and perform a search for '.Net4.0. The download file is 'dotnetfx.exe'.*
- **Sharp OSA2,OSA3, or OSA4 enabled device with an External Accounting Module (MX-AMX3)**

Optional

- Print Audit Secure 1.1 is supported with Embedded for Sharp

Installation Walkthrough

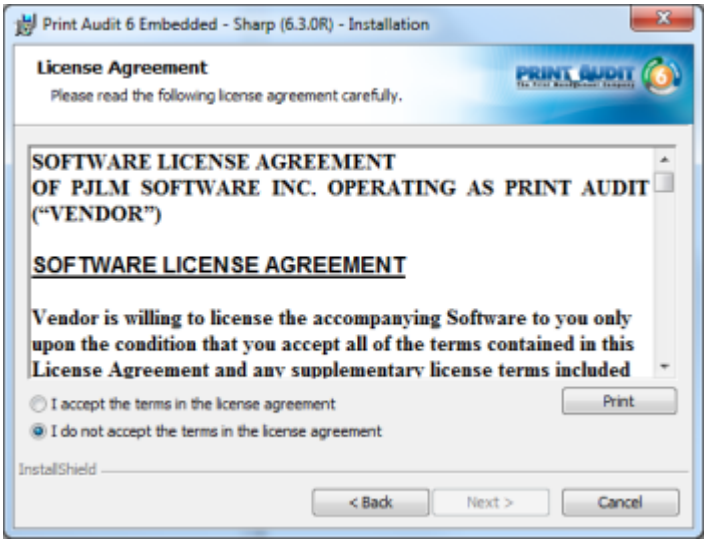
Before you install!

Before you begin the installation, check to make sure that both IIS and .Net have been installed (as per the Requirements section above).
IIS must be installed before .Net, otherwise .Net will need to be reinstalled to ensure the .NET components are registered properly with IIS. IIS cannot be configured correctly if .NET is installed first.

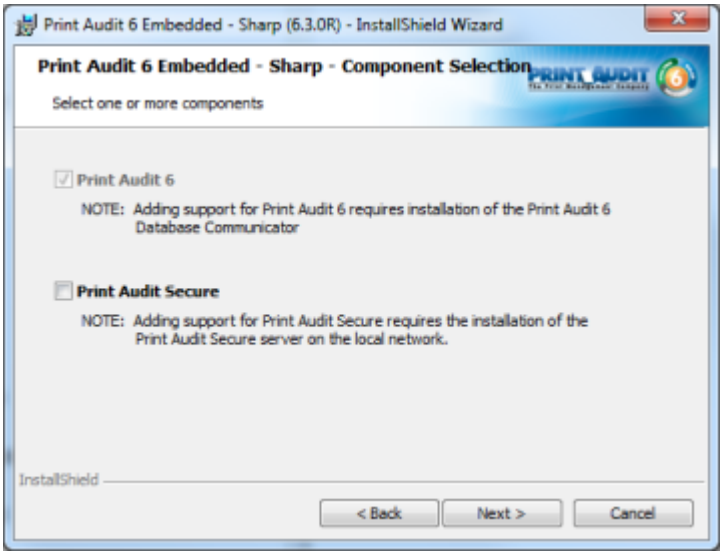
1. Double click on the pa6sharpsetup.exe file to begin the installation.

2. On the "Welcome to Print Audit Secure Client Setup Wizard" window click Next.

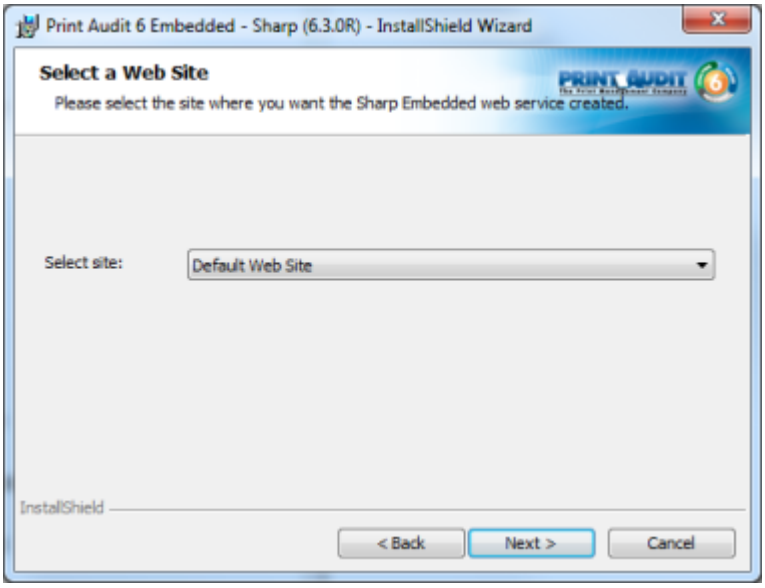
3. Read the End User License Agreement and select the checkbox if you accept. Click Next.



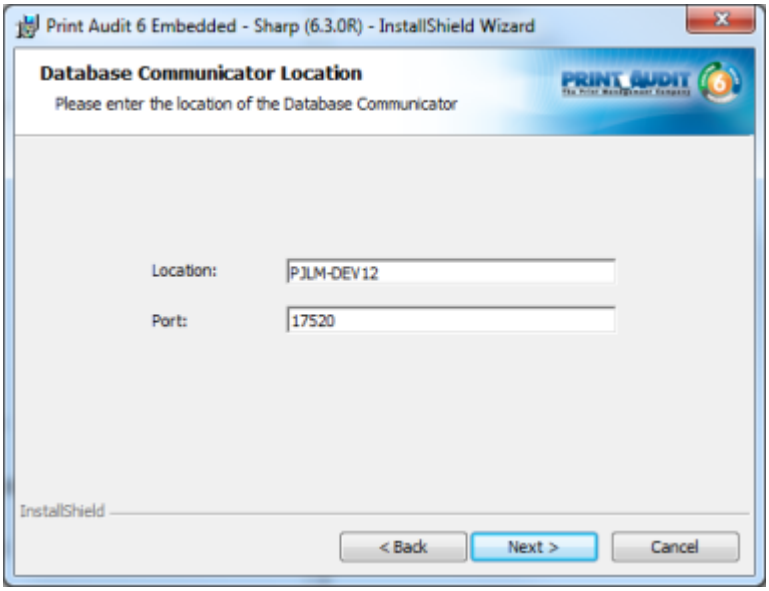
4. Select the component(s) with which the Sharp Embedded installation will interface. The Print Audit 6 component is a required component for device registration. Embedded for Sharp will not operate without it. Print Audit Secure is optional. When selected, the installer will ask for the location of the PA Secure web services.



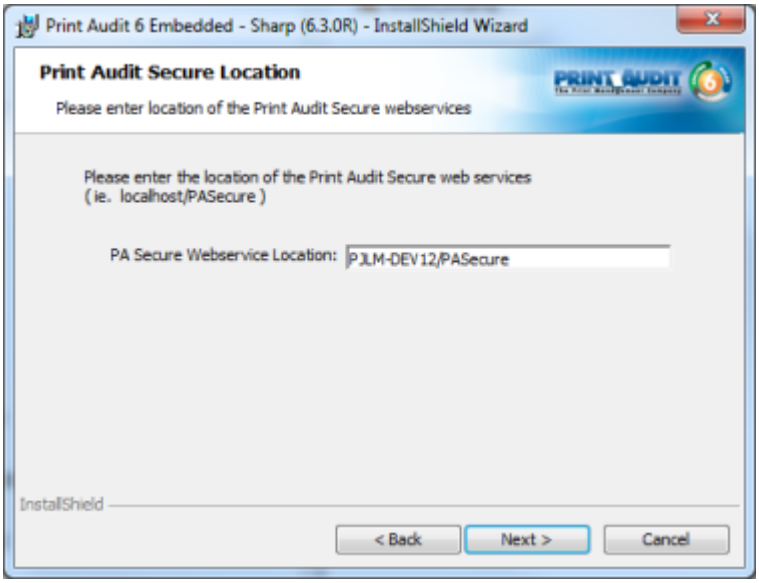
5. Select the Website name where the Embedded for Sharp web service will be created. It is recommended to use the Default Web Site. Click Next.



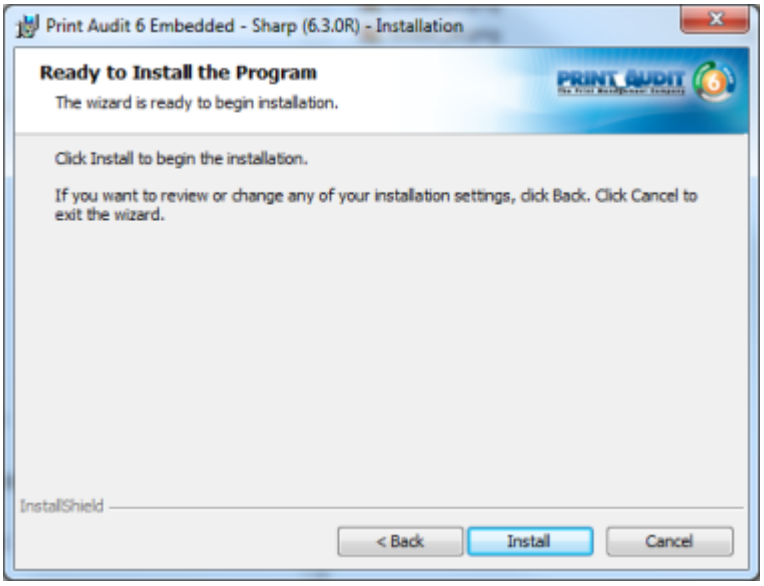
6. Enter the location where the Print Audit 6 Database Communicator resides.



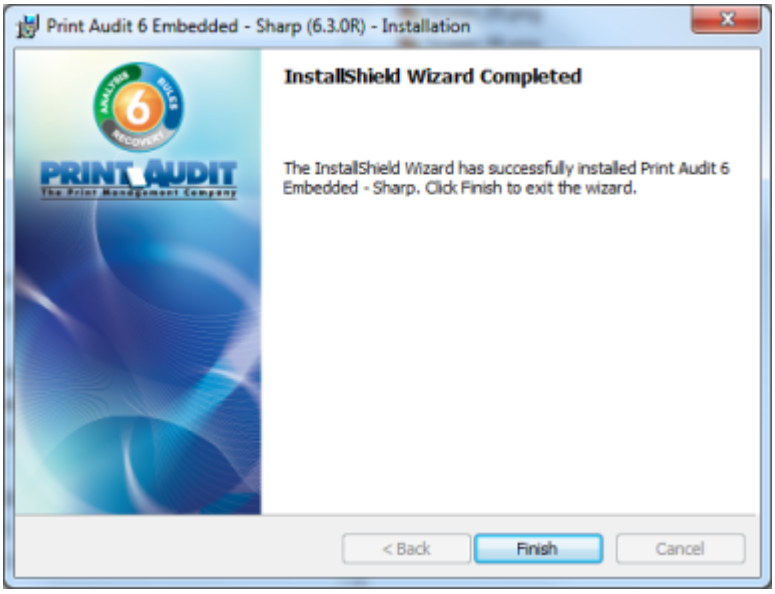
7. Enter the location of the Print Audit Secure web services. This location defaults to the server where the embedded software is being installed and to the default Print Audit Secure site.



8. Select Install to begin installing Embedded for Sharp.



9. When the installation is complete, click Finish.



10. After installation ensure the Application Pool is set to ASP.NET v4.0.

2. Configuration

The following are instructions to configure Print Audit 6 with Sharp Embedded.

Pre-configuration checklist

If you are ready to begin configuring Print Audit 6 with Embedded for Sharp, you have:

- Installed the Print Audit Database Communicator, Database and Administration tools to a computer on the network that will be on and available at all times. The Print Audit Client should be installed on at least one workstation, to test printing and ensure that print jobs are being tracked correctly before continuing.
- Configured Print Audit 6 for user quotas, PIN codes and validated fields to be be integrated into Print Audit 6 Embedded.
- Installed the Print Audit 6 for Sharp Embedded software on a computer that has Internet Information Services (IIS) and .Net installed, and is acting as a web server.
- Used this guide to configure Print Audit 6 Embedded on the Sharp OSA-enabled devices.

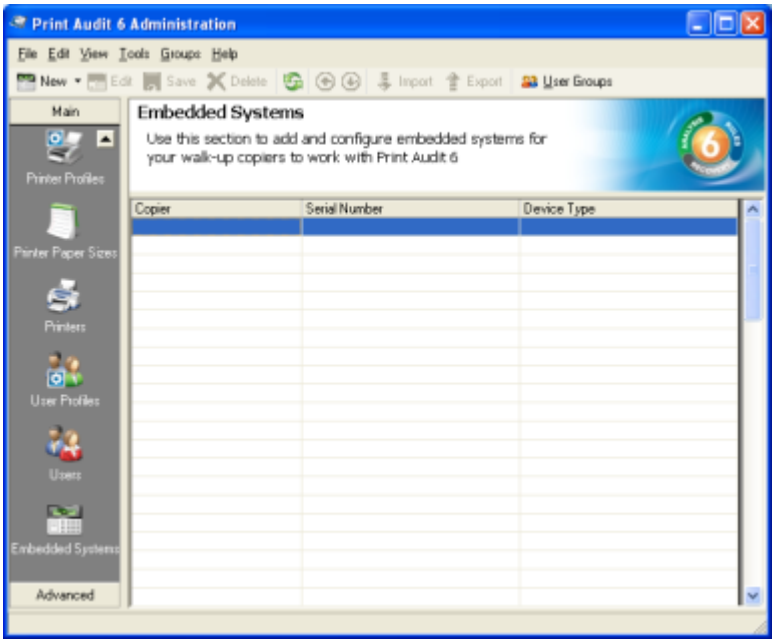
Overview

The Print Audit Administration tool provides the ability to configure Embedded for Sharp on all the MFDs in the environment using the Embedded Systems plug-in. Configure one copier for every physical Sharp MFD on which the Embedded Client will run.

Costs, restrictions, limits, authentication methods and custom fields may be configured for each device.

Adding, Editing and Deleting Copiers

Use the Embedded Systems section of the Administration tool to add, edit and delete Embedded for Sharp copiers. A copier in the Administration tool represents a physical copier in the network.



To add a new copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Click the New button on the toolbar. The Embedded for Sharp Window appears.
4. At minimum, a copier name and the serial number of the copier must be provided. Please refer to the 'Embedded for Sharp Configuration Window' section below for more information filling out the Embedded for Sharp window.
5. Click the Save button. The Embedded for Sharp Window closes and the copier appears in the Copiers list.

To edit a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Edit button on the toolbar. The Embedded for Sharp Window appears.
5. Make any needed changes to the copier.
6. Click the Save button. The Embedded for Sharp Window closes and the copier appears in the Copiers list.

To delete a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Delete button on the toolbar. A message appears to verify removal of the copier.
5. Click the Yes button to delete the copier. The list of copiers refreshes.

Configuring the Sharp MFP in Print Audit 6

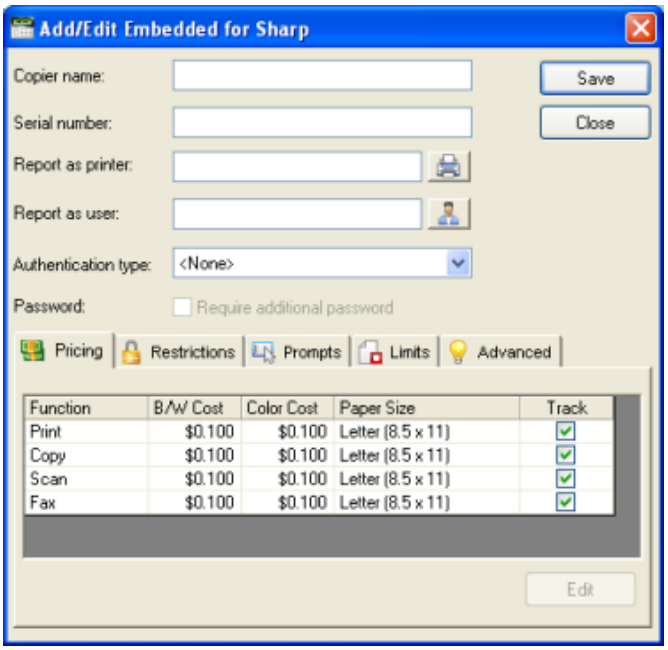
This Embedded for Sharp window in Print Audit 6 enables the configuration of all aspects of the Embedded for Sharp copier device. The different elements of the window are described below.

General

Copier name - The name to describe the copier. Enter a name that is descriptive enough to distinguish the copier from others. For example "Third Floor Sharp MX-7000N".

Serial number - The serial number of the Sharp MFD.

Report as printer - Use this to select an already existing Print Audit printer with which to associate the copier. For example, if there is an MFD in the office that users print to which is already in the Print Audit database, choose that MFD here for the copier so that all transactions are reported as the same printer. If a printer is not selected here, Print Audit will record transactions for this copier as the copier name.



Report as user - Use this to select an existing Print Audit user whom to associate all jobs from this copier. Use this functionality to still have individual user authentication, but for reporting purposes report all jobs to a single user.

Authentication type - Select how the user will authenticate to the copier before they can do transactions.The authentication type determines how a user identifies themselves to the copier before they can do a transaction. The following options are available:

- None - Users do not have to authenticate before using the copier. All transactions are recorded to a generic user.
- PIN code - Users must enter their Print Audit PIN.

NOTE: Check the 'Require additional password' box on the Embedded for Sharp Window to require an additional password before users can authenticate.

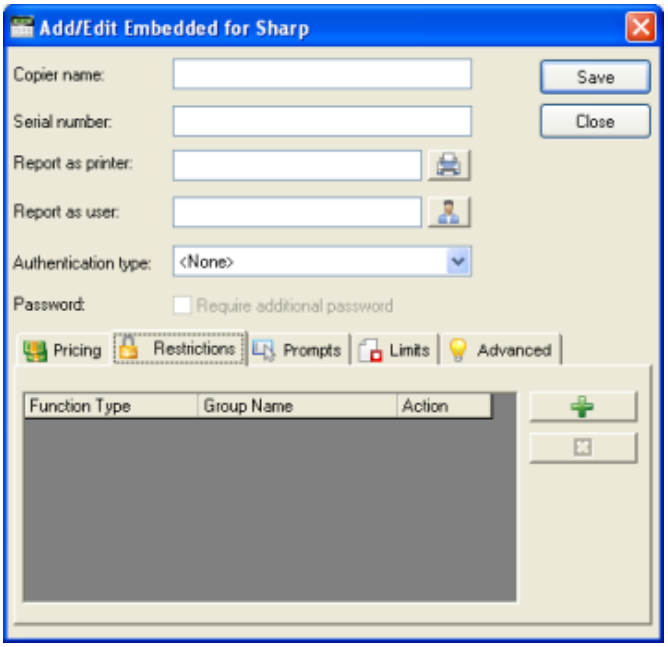
Require additional password - Check this box to require the user to enter an additional password before they can authenticate using the Authentication type selected above.

Pricing tab

This tab contains the pricing for each function on the copier.

To edit the pricing for a particular function:

1. Clear the "Track" column for the function to disable the tracking of transactions of that type.



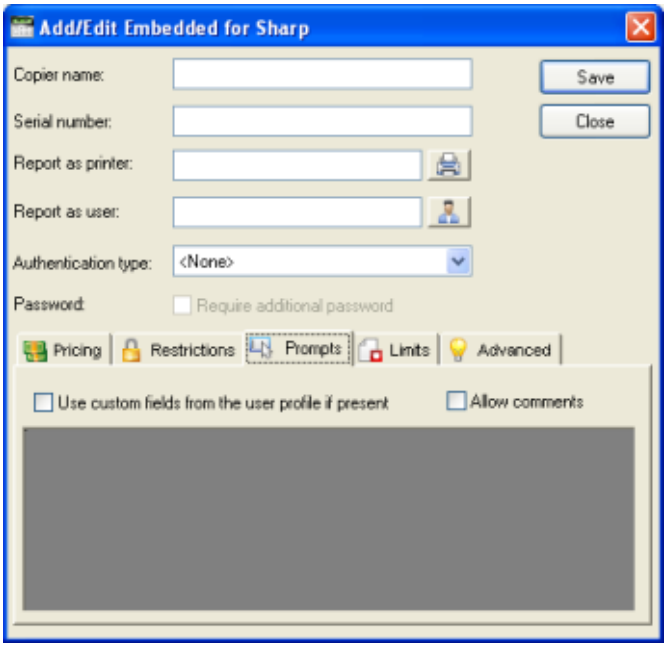
2. Select from the list the function that is to change and click the Edit button. The Configure Pricing and Paper Size Window appears.
3. Set the pricing as it makes sense for this copier in the organization.
4. Click the Done button. The Configure Pricing and Paper Size Window closes.

Restrictions tab (only with Print Audit 6 Rules)

Choose to restrict access to the copier based on which user group a user belongs to.

Add button - Click this button to add a new restriction. The Configure Restriction Group window appears.

Remove button - Click this button to remove a restriction.



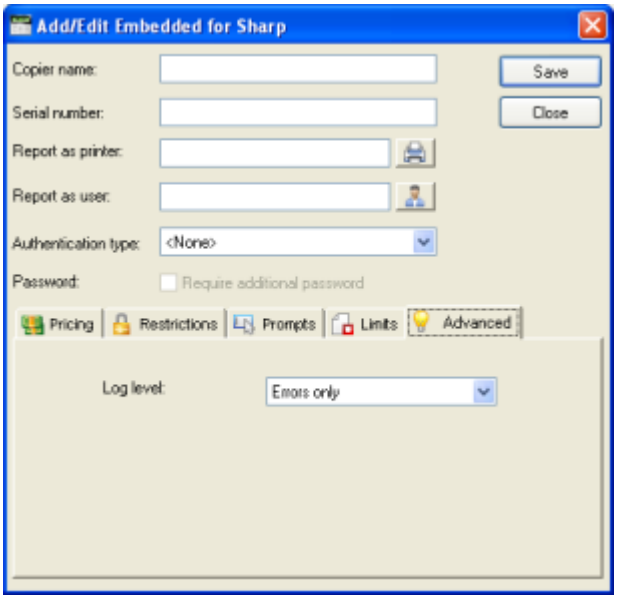
Prompts tab (only with Print Audit 6 Recovery)

This tab is only relevant when using Print Audit 6 Recovery for the charge-back of printing.

- For each Activity the user can be required to enter values for Custom Fields. Custom Fields are setup in the Custom Fields section of the Print Audit Administrator. On this tab, select from any one of the Custom Fields configured and define a custom prompt for each one.
- Use custom fields from the user profile - Check this box to override the default custom field choices with the custom fields set in a user's User Profile.
- Allow comments - Check this box if the user can enter general comments about the job.
- Custom fields - The custom fields list contains all custom fields that have been defined. To use a custom field for the activity, check the Include checkbox.

Advanced tab

Log Level - Use this drop down box to change amount of information the Embedded Client will log. Unless instructed to change this setting by technical support, leave this set to Errors Only.



Extended Configuration Settings

Described below are a small number of configuration settings which are only available by making modifications to the following file:
C:\Program Files (x86)\Print Audit Inc\Print Audit 6\Sharp Embedded\webservice\PrintAuditEmbedded.config

Database Communicator Location:

When Print Audit Embedded for Sharp is first installed, it prompts for the residing location of the Print Audit Database Communicator. To modify this location after installation, open PrintAuditEmbedded.config, and modify the COMMUNICATOR_HOST value with the new computer name where the Database Communicator will reside:
<add key="COMMUNICATOR_HOST" value="HOSTNAME" />
In this example, HOSTNAME is the name of the computer where the Database Communicator will reside.

Database Communicator Port:

To modify the port number of the Database Communicator, modify the COMMUNICATOR_PORT value:
<add key="COMMUNICATOR_PORT" value="17520" />

Database Communicator Timeouts:

To modify the number of seconds to allow the embedded application to query the Database Communicator before timing out, modify the COMMUNICATOR_QUERYTIMEOUT value:
<add key="COMMUNICATOR_QUERYTIMEOUT" value="30" />

To modify the number of seconds that the embedded application will wait for a response from the

Database Communicator whenever there is an attempt to establish communication with the Database Communicator over TCP/IP, modify the COMMUNICATOR_CONNECTTIMEOUT value:
<add key="COMMUNICATOR_CONNECTIMEOUT" value="5" />

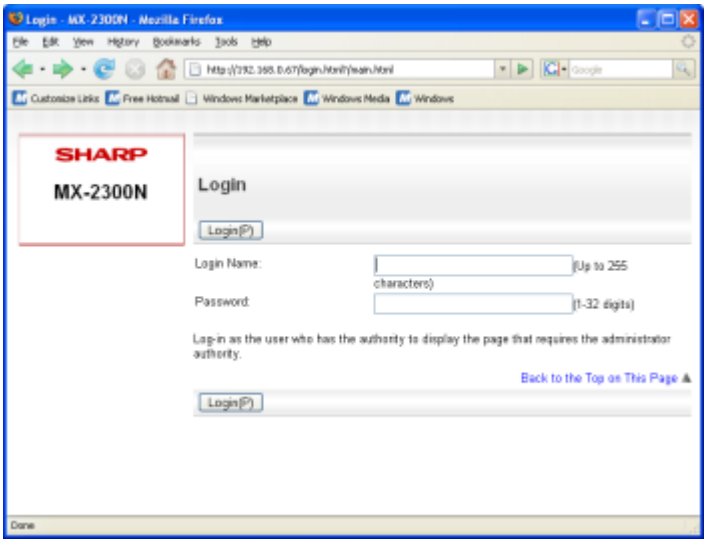
Appearance of searchable field results:

To adjust the number of columns that will display the results of custom field search, modify the the GRID_NUM_OF_COLUMNS value. The maximum number of columns to display is 3.
<add key="GRID_NUM_OF_COLUMNS" value="2" />

Enablement of welcome screen:

When a user logs into Sharp Embedded on an MFP, a welcome screen appears by default. To disable the appearance of this screen and allow the user to immediate access to the MFP functions , modify the SKIP_LOGOUT_PAGE value.
<add key="SKIP_LOGOUT_PAGE" value="0" />
A value of "0" will display the welcome screen.
A value of "1" will disable the appearance of the welcome screen.

5. Configuring Sharp MFPs with the Embedded Client for Sharp



Installing the Panel Interface

Embedded for Sharp must be configured on the devices to run as an External Authority application. Follow the steps below to configure a Sharp MFP to use Embedded for Sharp:

1. Open a web browser.
2. Browse to the IP address of the Sharp MFP. The login page for the Sharp MFP will appear.
3. Enter a login name and password, then click the Login button. If the login name and password is unknown, please contact the network administrator.
4. On the main page, navigate to Application Settings->External Application Settings.
5. Set External Account Control to "Enable".

6. Set Application Name to "Print Audit 6 - Embedded - Sharp".
7. Set Address for Application UI to http://xxx.xxx.xxx.xxx/pa6sharp/pages/Start.aspx, where xxx.xxx.xxx.xxx corresponds to the IP address of the computer where Embedded for Sharp is installed.
8. Set Address for Web Service to http://xxx.xxx.xxx.xxx/pa6sharp/pages/Service.asmx where xxx.xxx.xxx.xxx corresponds to the IP address of the computer where Embedded for Sharp is installed.
9. Set the Timeout to 20 seconds.
10. Click the Submit button.

Repeat the above steps for each Sharp MFP on which Embedded for Sharp will be used. The Troubleshooting section of this document should be consulted if there are issues running the panel.

3. Using Sharp Embedded with Print Audit 6

The Embedded for Sharp Client is very easy to use. It will first prompt for required identification or billing information, before enabling the device for copy, scan, fax, or print functionality. Once the desired function is complete, return to the panel and complete the session, otherwise the MFP will timeout the session. When the session ends, the copy, scan, fax, or print transaction is sent to the Print Audit 6 database, and the Embedded Client resets to be ready for the next user.

The standard set of steps to using Embedded for Sharp to track job information is as follows:

1. **Start the Transaction -** Press the Start button on the screen. The Embedded Client retrieves its configuration and proceeds to prompt for the required information. The Cancel button can be used at any time to return to the Start screen.
2. **Authenticate -** If configured to ask for a PIN Code, the Embedded Client displays a login screen. To login:
    a. Press the PIN Code button. An input form displays.
    b. Enter a PIN Code using the Sharp keyboard or the touch screen.
    c. Press the OK button to accept the input.
    d. Press the OK button on the Login screen to validate the PIN Code.
3. **Enter Custom Field Information -** If configured to ask for Custom Field information, the Embedded Client will prompt for on or more values from the user. To enter values for a searchable field:
    a. Press the button on the touch screen that corresponds to the Custom Field Name.
    b. Enter a full or partial code on the screen and click OK.
    c. If only one match is found for the field, the Embedded Client asks for the next Custom Field value if any is configured.

d. If Print Audit finds more than one match, a list of values will display. Use the touch screen to navigate through the values.

e. When the desired value is found, press the button corresponding to the value. It appears highlighted.

f. Press the OK button to accept the value.

g. Press the OK button again to move to the next screen.

4. **To enter values for a non-searchable field:**

   a. Press the button that corresponds to the desired value. It appears highlighted.

   b. Use the arrows on the touch screen to navigate through the choices.

   c. Press the OK button to accept the value. The Embedded Client will request the next Custom Field value if any is configured.

5. **Enter any Comments -** If configured, the Embedded Client will request any Comments for the job. Press OK if to proceed without entering comments. To enter comments:

   a. Press the Comments button on the touch screen. An input form appears.

   b. Use the input form to enter comments.

   c. Press the OK button to close the input form.

   d. Press the OK button on the Comments screen to accept the comments.

6. **Verify Selections -** After all information has been input, a summary screen appears showing the current balance if any, along with the custom values selected. Press the OK button to accept the selections and begin the job.

7. **Complete the Job -** After the job is completed, press the "**" (Logout)" button on the Sharp MFP keypad. This completes the transaction, and transmits the job information to the Print Audit database. If the "**" (Logout)" button is not used to end the session, the Sharp MFP will eventually timeout the session, return to the Start screen and transmit the job information to the Print Audit database.

Note

If declining balances are enabled for the current user each copy/fax/scan operation will debit the account balance in real-time. Once the balance of the current user reaches zero all MFP copy/fax/scan functions will be locked for that user until such time that the user logs in again with a positive balance.

4. Using Sharp Embedded with Print Audit Secure

The Print Audit Secure Embedded for Sharp Client is very easy to use. It will first prompt for required information. The prompts which appear are dependent on how the Secure Embedded Client is configured. Once the prompted information is provided, the device will release the secure job(s). Then the Secure Embedded Client resets to be ready for the next user. If the session is not manually finished, the Sharp MFP will timeout.

Following, are the standard set of steps to using Secure Embedded for Sharp to release a print job.

1. Authenticate

1. **PIN Code authentication -** If configured to request a PIN Code, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Pin Code Field
    b. Enter a PIN Code using the Sharp keyboard or the touch screen.
    c. Press the Login button to accept the input.
2. **Authenticate with a Username -** If configured to ask for a Username, the Secure Embedded Client displays a login screen. To login:
    a. Click on the Username Field
    b. Enter a Username
    c. Click on the Password Field
    d. Enter a Password
    e. Press the Login button to accept the input.
3. **Authenticate with a swipe card -** If configured to ask for a swipe card, the Secure Embedded Client displays a login screen. To login:
    a. Swipe a card in a card reader attached to the MFP.

2. Release Print Jobs

1. To release all the compatible print jobs, click the Release All button.
2. To release only certain jobs, press the checkbox next to the jobs to be released.
3. Click the Release button. The selected job(s) will now print.

3. Delete Print Jobs

To delete print jobs, press the checkbox next to the jobs to be remove and press the Delete button.

4. Complete the Job

When finished releasing print jobs, press the Logout button on the Sharp MFP screen. This will notify Print Audit Secure that the transaction is complete. If this step is not completed, the Sharp MFP will eventually reset back to the Start screen.

5. Troubleshooting

Please refer to this section if issues are encountered with the operation of Embedded for Sharp. If a resolution is not found in this section, please contact Print Audit technical support.

Error: Could not access the accounting server. Contact your Admin
This could indicate that the ASP.NET runtime in the IIS configuration is set to the wrong version. Embedded for Sharp requires the .NET 4.0 runtime or newer to be configured in IIS. When installed , Embedded for Sharp defaults to the overall .NET setting for the website, which may not be correct .

1. To change IIS to use a different .NET runtime:
2. Open the Windows Internet Information Services interface.
3. Expand the website where Embedded for Sharp is installed.
4. Go to the Properties page for the pa6sharp virtual directory.
5. Click the ASP.NET tab.
6. Select 4.0.30319 in the ASP.NET version drop-down.
7. Click the Apply button.

NOTE: In IIS 6.0 (Windows 2003) and IIS 7.0 (Windows 2008 and Vista) a separate Application Pool for Embedded for Sharp may need to be created if .NET 1.0 or 1.1 apps are running in the DefaultAppPool.

This error could also indicate that the web server that Embedded for Sharp is installed turned off or otherwise not available through the network.

Error: The device has not been configured
The MFP has not been configured in the Administrator. Please run the Administration tool, go to the "Embedded Systems" plug-in and setup the MFP.

Error: Unable to connect to Database Communicator
This error occurs if the MFP cannot connect to the Database Communicator. Please check the following:

1. The Database Communicator is running.

2. The correct host name and port are set for the Database Communicator. To change the host and port, edit the PrintAuditEmbedded.config file installed with the Sharp Embedded for PA6 package.

Error: Print Audit License is not Valid
If for some reason the Sharp MFP cannot validate the Print Audit license, or if there are not enough Embedded for Sharp licenses for the MFPs, this error displays. Please contact Print Audit or an authorized dealer to purchase or update the Print Audit license.

Error: Unable to save file: C:\\Windows\Downloaded Installations\PrintAudit 6 Embedded – Sharp.msi
Access is denied
The installer must be executed with administrator privileges. Right-click PA6Sharp6xxR.exe and select 'Run as Administrator'. Enter username & password if necessary.

6. IIS Configuration/Setup for Print Audit Embedded for Sharp

Please note that this document is meant as an aid to installing and configuring IIS /. NET 4 for use with Print Audit Embedded for Sharp rather than a step by step guide. The actual sequence of steps will depend on the components installed on the server and the order in which they have been installed. Modifications to an existing IIS installation should be done by a qualified administrator.

Installing .NET version 4

Print Audit 6 Embedded for Sharp requires .NET Framework version 4. Please note that .NET should be installed prior to installing IIS. If it is not installed first, it may be necessary to use the " aspnet_regiis -ir" registration utility.

IIS 6 (Server 2008)

.NET version 4 isn't included by default with Server 2008. It can be downloaded from Microsoft's web site.

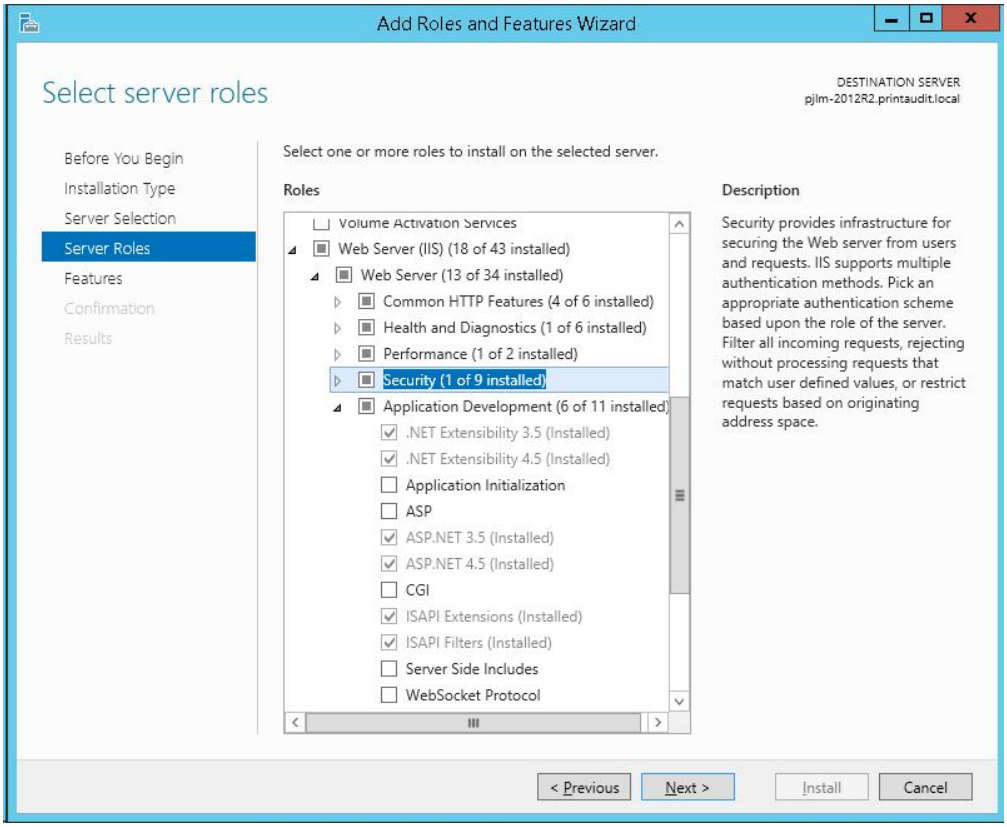
IIS 7 or higher (Server 2012 and higher)

.NET version 4 is added as a Feature using the "Add Roles and Features Wizard".

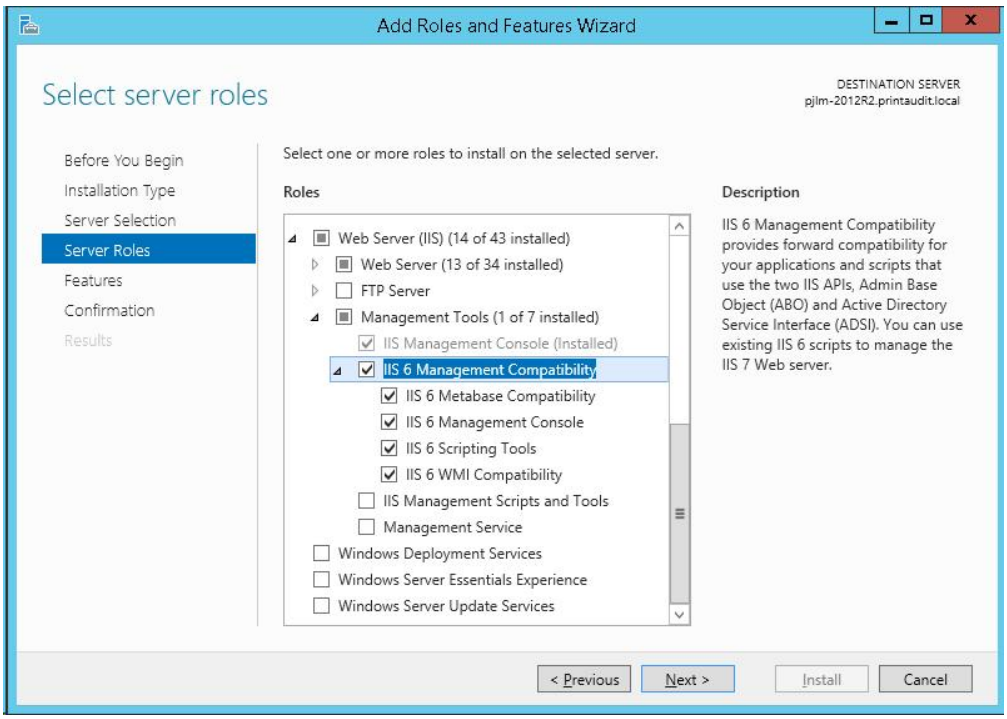
Installing IIS Components

Print Audit 6 Embedded for Sharp requires that IIS version 6 or higher be installed first. The following components are required above the base IIS installation:

Application Development

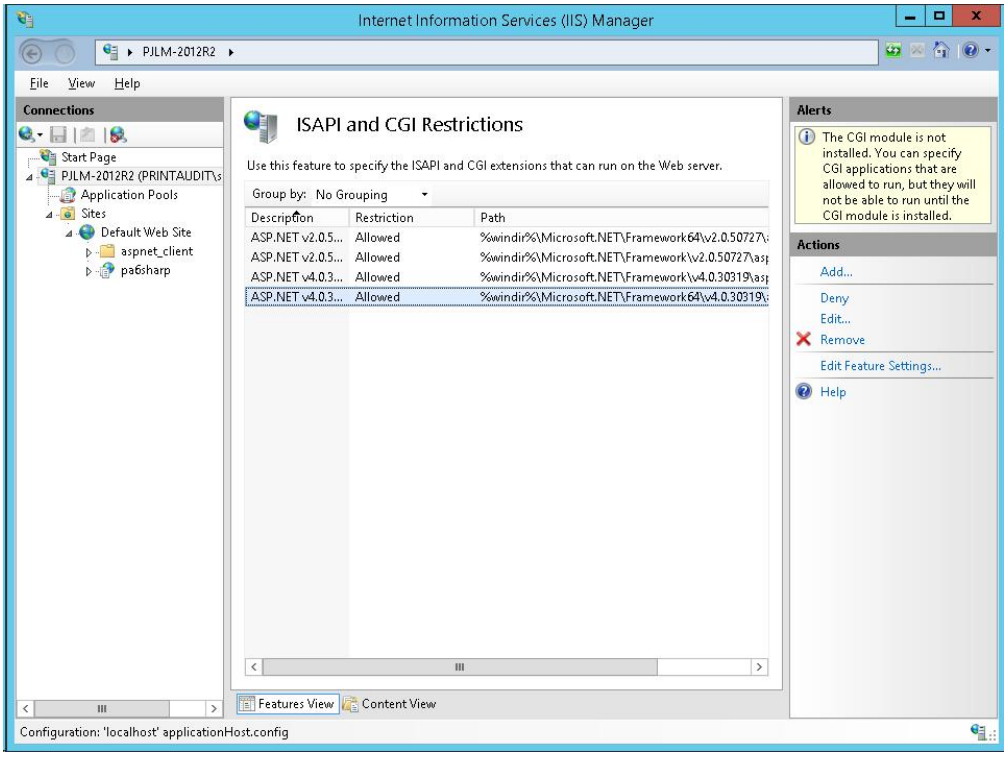


IIS 6 Management Compatibility Tools



Allowing the ASP.NET Version 4 Extension

The ASP.NET version 4 extension needs to be allowed before it can be used. This is done using the Internet Information Services (IIS) Manager under "ISAP and CGI Restrictions".

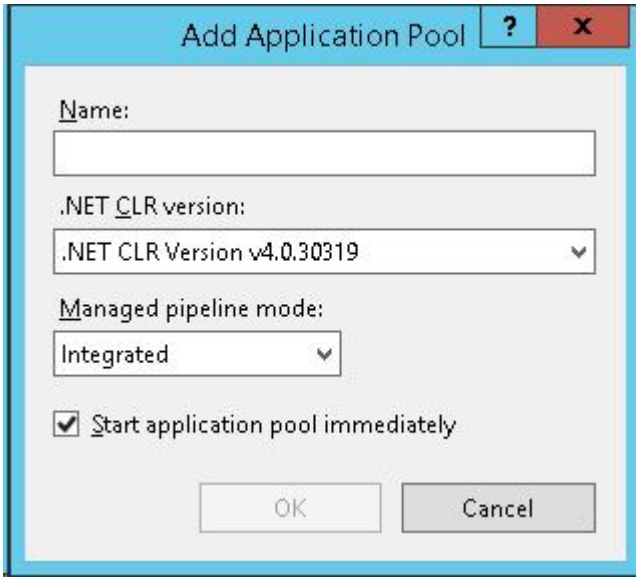


Creating Application Pools in IIS for Print Audit Embedded

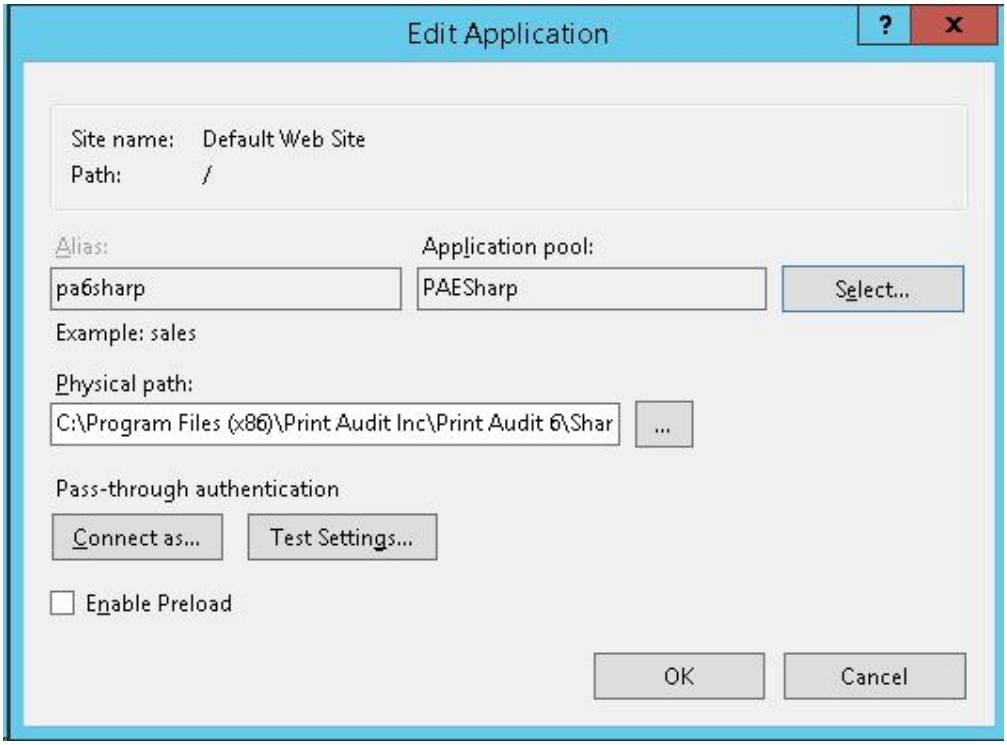
Print Audit 6 for Sharp Embedded installs under the "DefaultAppPool" in IIS. It is recommended that you give Print Audit 6 for Sharp it's own Application Pool especially if there are other web sites running on the IIS server.

To create an Application Pool for Print Audit Embedded:

1. Open the Internet Information Services (IIS) Manager.
2. Highlight the server name under "Connections" and expand it. Click on "Application Pools".
3. Under "Actions", click on "Add Application Pool..."



4. Give the Application Pool a meaningful name. Set the .NET version to 4.0.30319. The " Managed pipeline mode" should be set to "Integrated".
5. Click OK.
6. Expand "Sites" to locate the web ite that the Embedded application has been installed under. The default is "Default Web Site". Expand the web site and locate the site named "pa6sharp".
7. Highlight the site. Under "Actions", click on "Basic Settings..."
8. Click on "Select..." by "Application Pool..." Change the Application pool to the one created above. Click OK


Edit Application
Site name: Default Web Site
Path: /
Alias:
Application pool:
pa6sharp
PAESharp
Select...
Example: sales
Physical path:
C:\Program Files (x86)\Print Audit Inc\Print Audit 6\Shar
...
Pass-through authentication
Connect as...
Test Settings...
Enable Preload
OK
Cancel

Embedded for Xerox Documentation

Print Audit Embedded installs directly onto supported Xerox EIP® -enabled multifunction peripherals, allowing users to control and recover all printing, copying, faxing and scanning costs. Review the documentation below for help installing and configuring Print Audit Embedded. You can also use the Knowledge Base to find more information.

Browse Documents:

Collapse allExpand all Collapse all

Browse Other Product Documentation:

Print Audit 6 Infinite Device Management Print Audit Secure Rapid Assessment Key Embedded for Sharp

Embedded for Kyocera Mita Embedded for Lexmark Embedded for Xerox Embedded for HP

Copy Audit Touch Copy Audit Numeric

Embedded for Xerox Installation and Setup Guide

Print Audit Embedded for Xerox is used alongside Print Audit 6 to provide authenticated access to Xerox MFPs, for the purpose of securing device functionality, and tracking usage. Users must authenticate at the MFP by login, PIN, or card swipe identification before they may access MFP functions. When used in conjunction with Print Audit Secure, users will also be able to select and release secure print documents directly from the MFP panel.

This guide provides instructions to install and configure Embedded for Xerox with Print Audit 6.

When used with Print Audit 6, Embedded for Xerox will track:

- walk-up copying
- scanning
- faxing
- Print From

When Print Audit Secure is added, Embedded for Xerox can additionally provide:

- Secure release of all printing
- "Follow Me" printing

Components

Embedded for Xerox consists of two main components:

1. Print Audit 6 - Embedded for Xerox Configuration:

Embedded for Xerox is configured using the Embedded Systems plug-in for the Print Audit 6 Administration tool. Support for Embedded for Xerox exists in Print Audit 6.10.0 or newer.

2. Embedded Client:

This software runs on the MFP. The Embedded Client provides a user interface directly on the panel of the Xerox MFP to enable the tracking of copies, scans or faxes, or the printing of documents stored in the MFP's Document Server.In addition to tracking the number of pages in a copy, scan, fax, or print job, the Embedded Client tracks additional information about the job. For example, the Embedded Client can request a PIN Code from the user to identify and track who is creating the photocopy. Or, it can request a Client Code to identify which customer or cost center should be billed for a fax transmission.

Print Audit 6

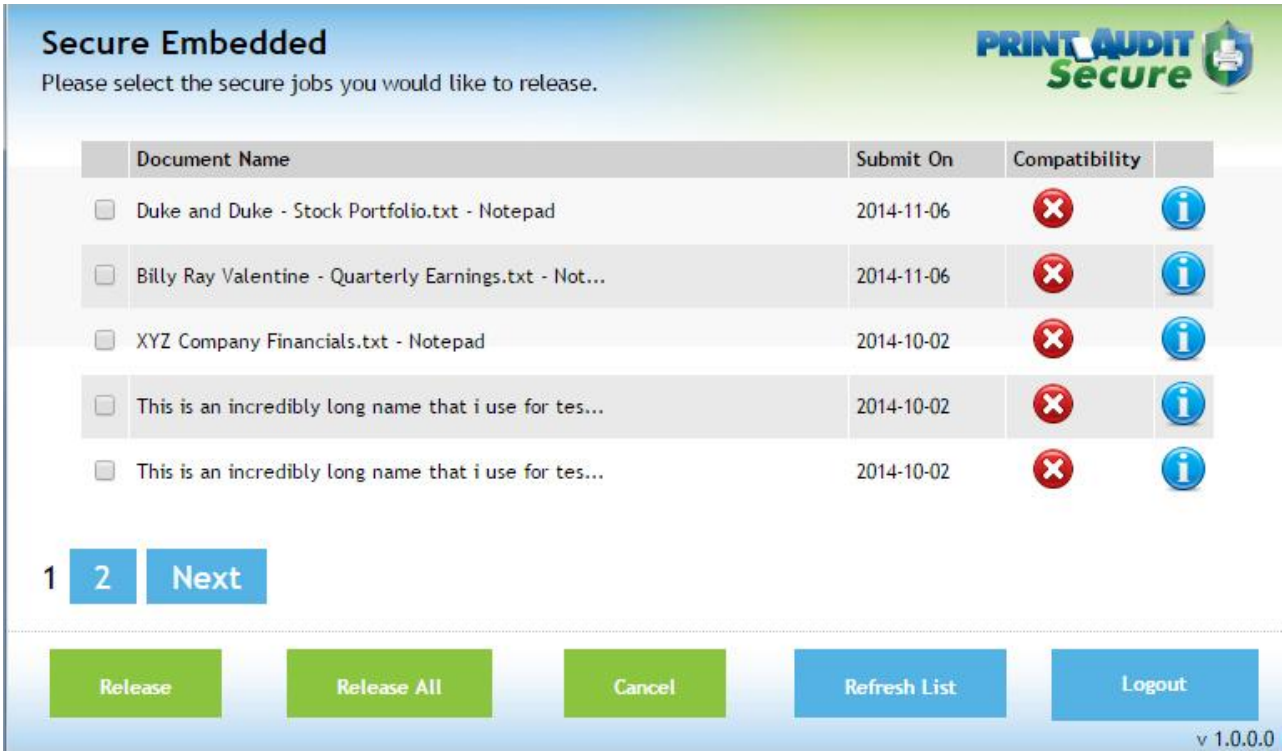
Print Audit 6 is a client application that tracks all printing directly from the desktop where the print job was issued. Every job, along with its attributes, are collected and stored in the Print Audit database, where it is available for reporting on printing volume and trends.

Print Audit 6 is available in 3 different modules (Analysis, Rules, and Recovery) which respectively, enable Analysis Reporting from the collected print data, the ability to create printing rules for rules-based printing, and the ability to allocate the cost of print jobs to a user, customer, or cost center.

When used with Embedded for Xerox, Print Audit 6 can also track copy, scan, and fax jobs, and jobs that are printed from the document server.

Print Audit Secure

Print Audit Secure allows for print jobs to be held on the server until an authenticated user releases them from the MFP panel, or from a Print Audit Secure release station. When a printer is managed by Print Audit Secure, incoming print jobs are prevented from being automatically output, by holding them in a secure queue on the server. When used with Embedded for Xerox, users will authenticate at the MFP, view their held jobs on the MFP panel, select one or more jobs and release or delete them directly from the MFP front panel.



Authentication Devices

Print Audit Embedded for Xerox supports Authentication Devices, such as swipe card or proximity card readers, within an Embedded for Xerox environment. When an Authentication Device is configured in an environment with Embedded for Xerox, users must authenticate at an Authentication Device before they are allowed to access the supported Xerox MFP controlled by the device.

Licensing

To enable the Print Audit Embedded for Xerox the following is required:

1. **One Print Audit Embedded for Xerox license per controlled Xerox MFP** - Print Audit, Embedded for Xerox is licensed on a per-MFP basis. To install Embedded for Xerox on 15 MFPs, licenses must be purchased for each of the 15 MFPs. MFP licenses can be

purchased as part of any Print Audit license, and are additional to the Print Audit 6 client licenses needed to track print jobs originating from Microsoft Windows and Apple Macintosh workstations. In the event that there are insufficient licenses, Print Audit will stop tracking some or all of the MFPs—MFPs will continue to function as normal, but no information will be tracked.

2. **EIP–enabled Xerox MFPs** - Print Audit Embedded for Xerox is only supported on Xerox EIP (version 2.5 and up).
3. **Print Audit 6.10 or higher** - Print Audit Embedded for Xerox requires Print Audit 6 to configure the MFPs. Consult the Print Audit 6 Installation Guide for more information.

Optional

1. **Print Audit Secure 1.3 or higher** - Consult the Print Audit Secure Installation instructions for more information
2. **One Authentication Device per Xerox MFP** - Print Audit Embedded for Xerox supports HID proximity and contactless smart cards for authentication. Users can enter validation data by presenting the card at the card reader. If an authentication device is to be used in the environment, one authentication device is required per MFP.

Limitations

Print Audit Embedded would ideally function identically across all makes and models. However, due to differences among the proprietary platforms, it is sometimes not possible to implement all features and functionality of the product. The following are a list of known limitations, when using Print Audit Embedded for Xerox:

1. **Ability to Return to Print Audit Embedded**: Once a user has logged in and Print Audit Embedded unlocks the device, allowing a user to choose a task on the panel, there is no method to return to the Print Audit Embedded application. Therefore, it is not possible for a user to attribute jobs to more than one custom field per logged on session, as is possible with other versions of Print Audit Embedded.
2. **Limitation of color or monochrome output**: There is no method available to control user-based color or monochrome output limitations.
3. **Cost Allowances**: There is no method to preventing a user from exceeding their account limit, if there was available credit in their account when they logged in. If they exceed their limit, they could go beyond their minimum balance. However, if the user attempts to login with no available balance, they will be denied from using the device.
4. **Swipe Card Registration**: Currently, this feature is not available due to limitations.

1. Installation - Embedded for Xerox

This section only addresses the installation requirements and configuration of Print Audit 6 for use with Print Audit Embedded for Xerox. For complete instructions on installing and configuring Print Audit 6, please refer to the Print Audit 6 Installation information found online. Refer to that documentation to perform the following steps to install Print Audit 6 in conjunction with Print Audit Embedded for Xerox.

Before you Install

Important!

Once Print Audit Embedded for Xerox is installed, the user will be required to authenticate to this application before being able to access any applications on the MFP. If the user attempts to open any application without first authenticating to Print Audit Embedded for Xerox, an error message will be generated.

System Requirements

- **Print Audit Embedded for Xerox is only supported on Xerox EIP (version 2.5 and up).**
- **Windows 2008 or newer** - requires Internet Information Services 6 or better**.**
- **MS-SQL Server 2005 Express or better -** running embedded applications on with an Access database is not recommended.
- **Print Audit 6.10.0 or newer**
  - Download the latest version from the www.printaudit.com/software-updates.asp.
  - The Print Audit 6 Database Communicator, Database, and Administrative tools must be installed on a Windows 2008 or newer computer.
- **Internet Information Services (IIS)**
- IIS must be installed before .Net4
- If running IIS 7, other IIS subcomponents will need to be installed such as Web Management Tools and .NET Extensibility, ASP.NET, ISAPI Extensions & filters. These features can be turned on by using Window Features in the Programs and Features on the Windows Control Panel.
- IIS is included in Windows 2008 or newer and can be installed with Windows or through the Windows Components of Add/Remove Programs application in the Control Panel. IIS 7.0 (Included in Windows 2008 and Windows Vista) requires that the IIS 6 Management Compatibility component is installed as well.

- **.Net 2.0**
    - The .Net 2.0 frame work is required for the Authentication application which works alongside the main Xerox Embedded application.
- **.Net 4.5**
- If the .Net framework was installed before IIS, then the framework must be reinstalled to ensure the .NET components are registered properly with IIS. IIS cannot be configured correctly if .NET is installed first.
- For more information or to download .Net, go Microsoft's website (www.microsoft.com) and perform a search for '.Net4.0. The download file is 'dotnetfx.exe'.

Optional

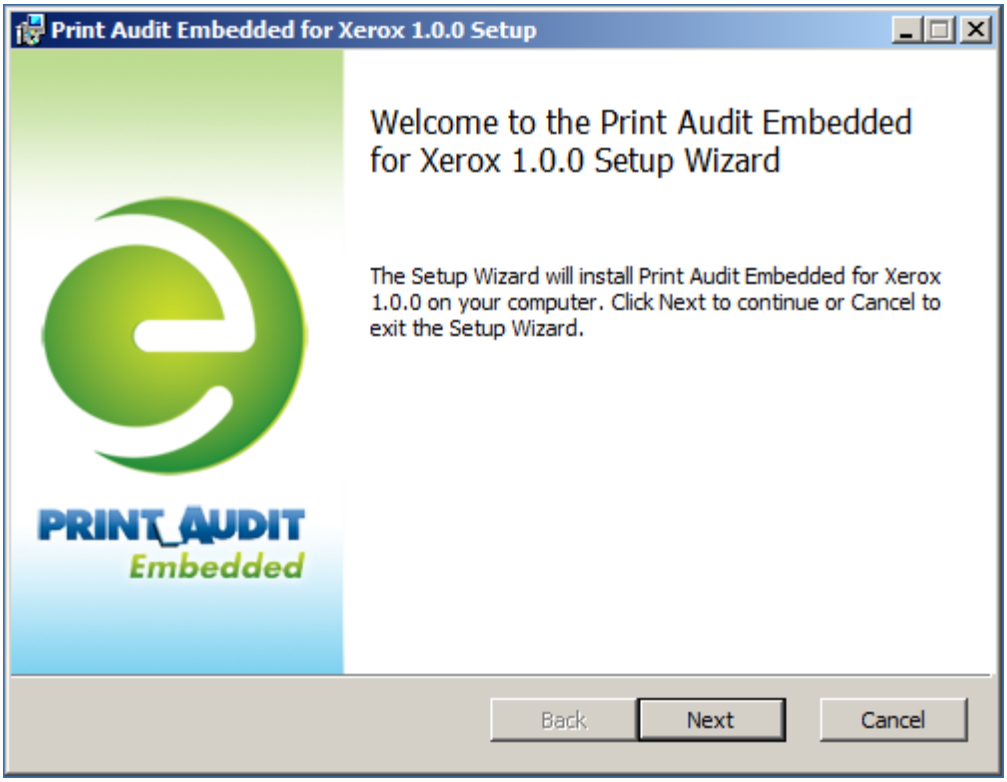
Print Audit Secure 1.3 is supported with Embedded for Xerox

Installation Walkthrough

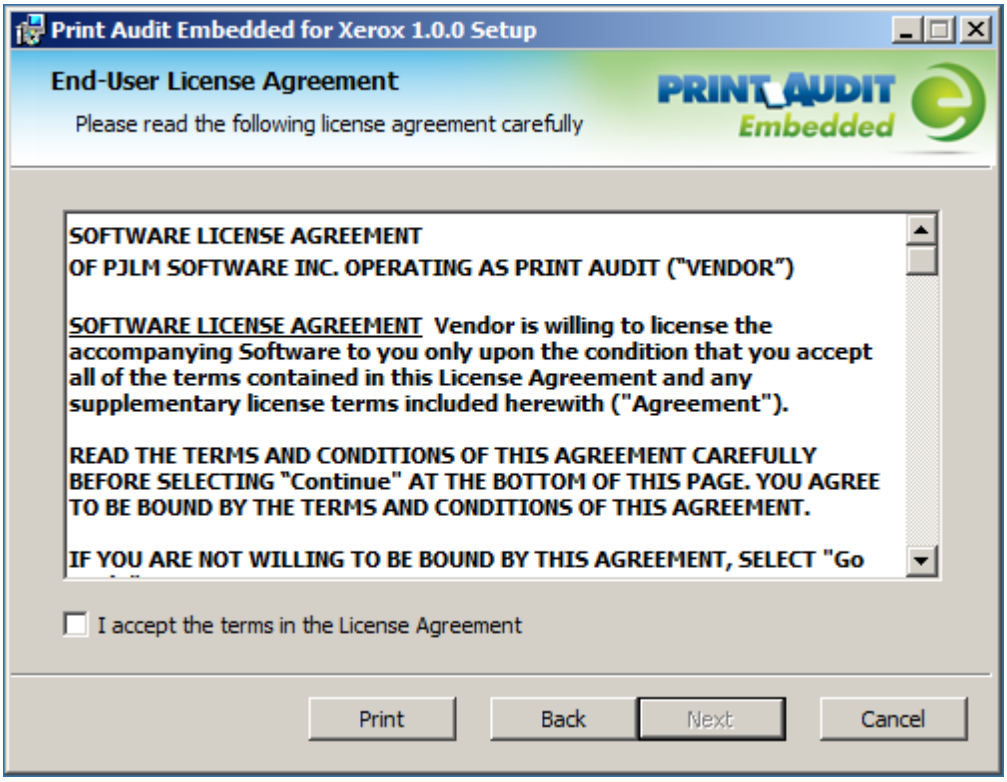
Before you begin the installation, check to make sure that both IIS and .Net have been installed as per the Requirements section above. IIS must be installed before .Net, otherwise .Net will need to be reinstalled to ensure the .NET components are registered properly with IIS. IIS cannot be configured correctly if .NET is installed first.

1. Double click on the paxeSetup.exe file to begin the installation.

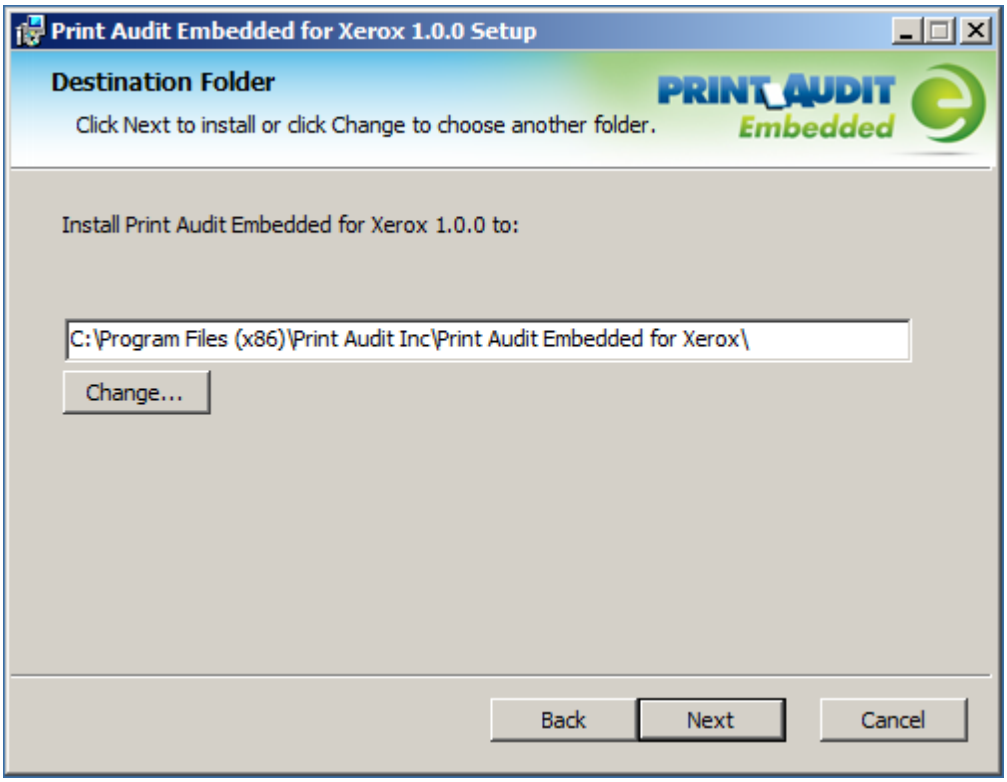
2. On the "Welcome to the Xerox Embedded 1.0.0 Setup Wizard" window click Next.



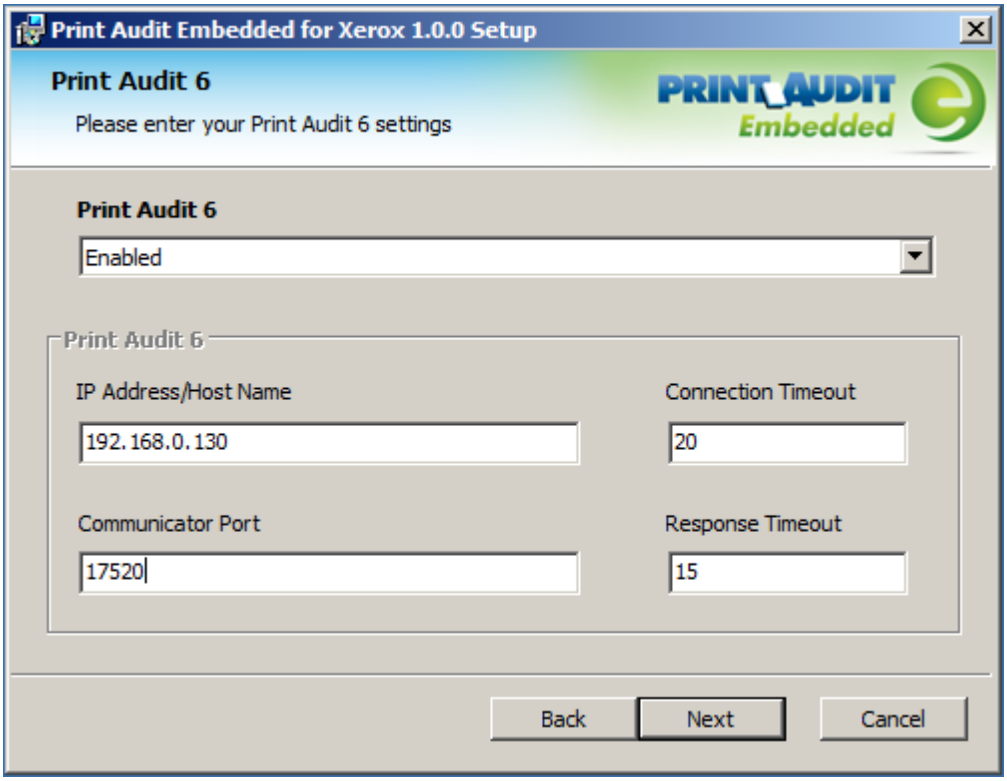
3. Read the End User License Agreement and select the checkbox if you accept. Click Next.



4. Select the install location. A default location will be available to you. Click Next.



5. Enter the Print Audit 6 configuration details. Click Next when finished.



a. From the dropdown box, choose Enabled or Disabled to enable/disable the Print Audit Embedded for Xerox application for use with Print Audit 6.

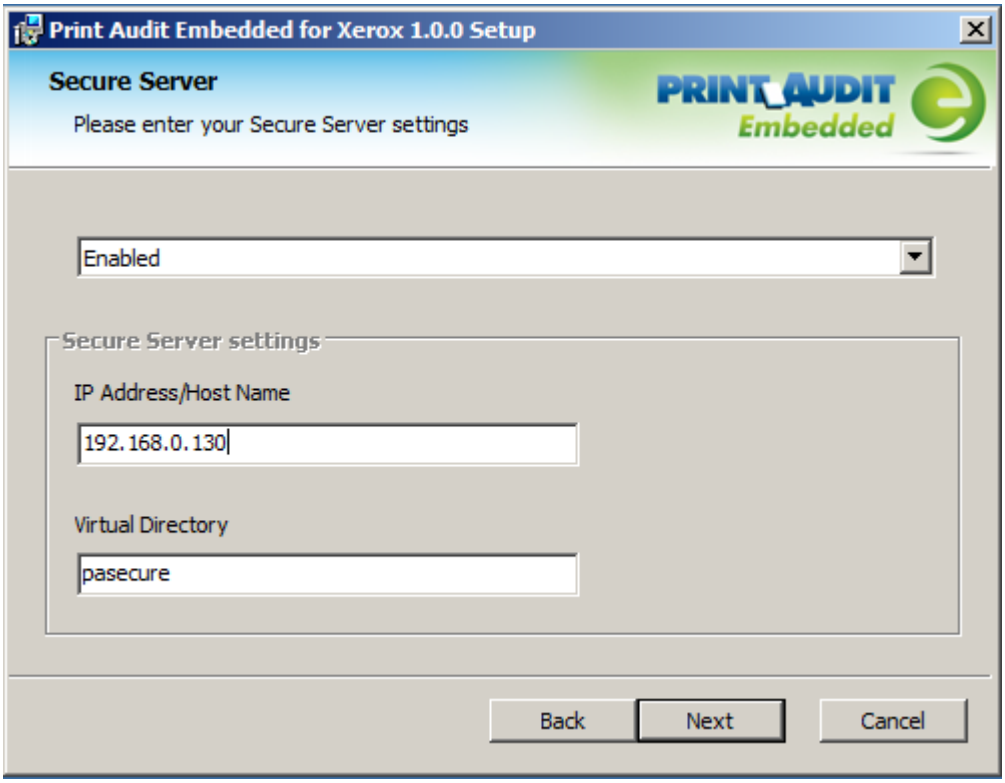
b. IP Address/Host Name - the IP Address or Host Name of the server running the Print Audit 6 Database Communicator.

c. Communicator Port - the port number the Database Communicator is set to listen on. The default is 17520.

d. Connection Timeout - the time in seconds that the Print Audit Embedded for Xerox application will wait before a connection to the Database Communicator fails. The default is 20 seconds.

e. Response Timeout - the time in seconds that the Print Audit Embedded for Xerox application will wait before a response from the Database Communicator before failing. The default is 15 seconds.

6. Enter the Print Audit Secure Server details. Click Next when finished.

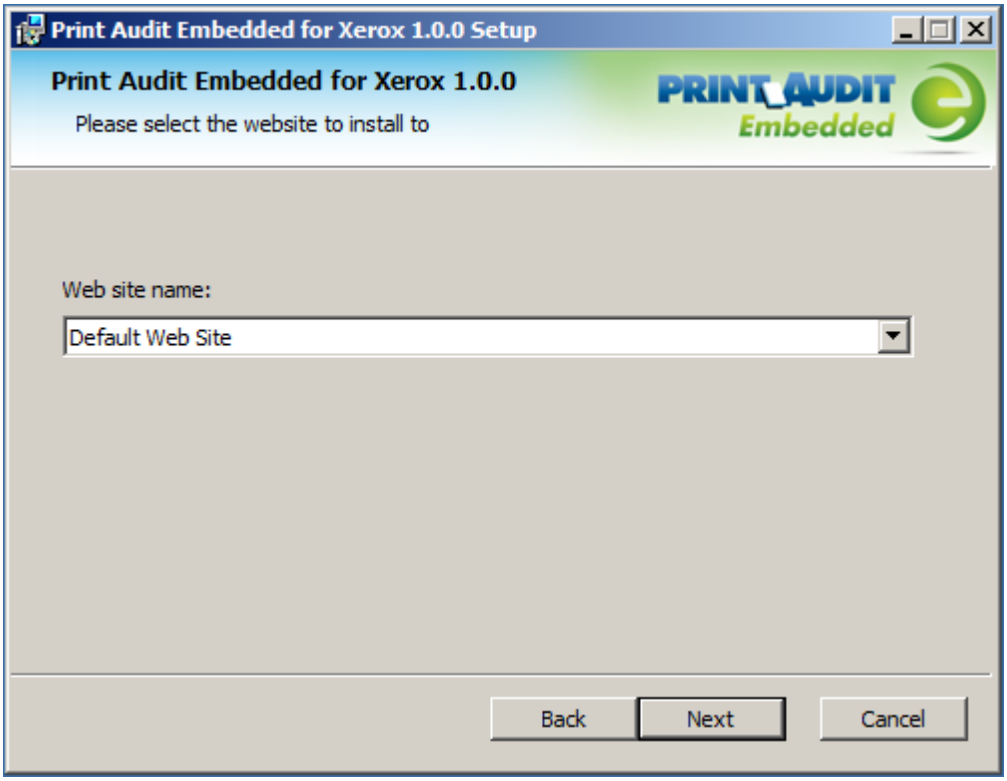


a. From the dropdown box, choose Enabled or Disabled to enable/disable the Print Audit Embedded for Xerox application for use with Print Audit Secure.

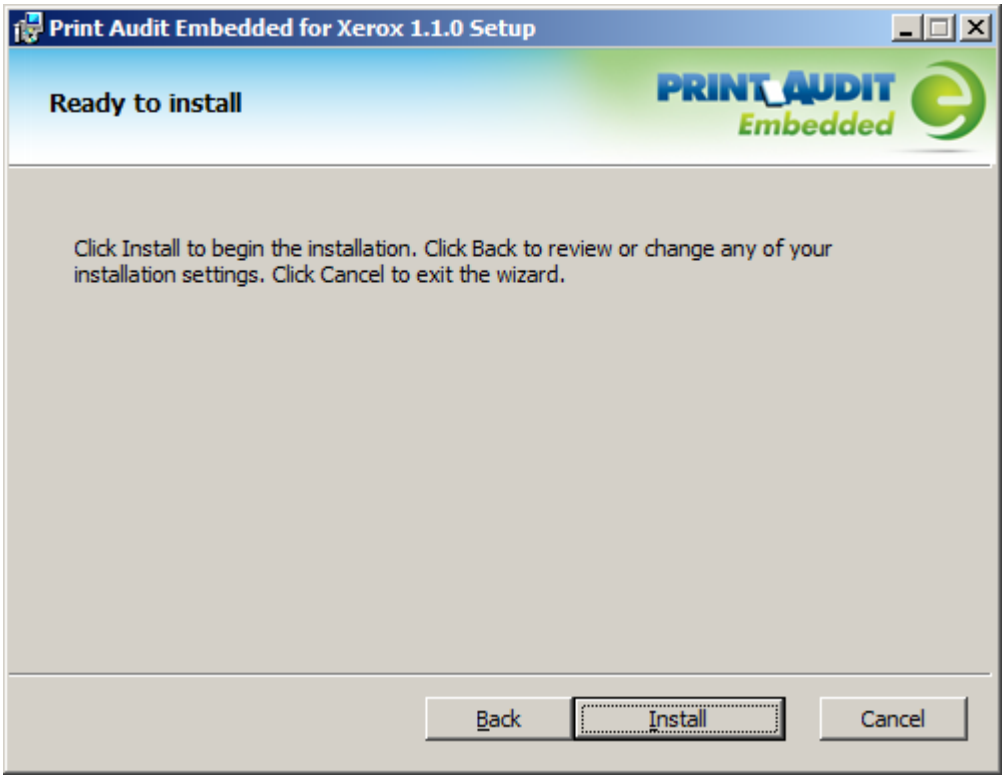
b. IP Address/Host Name - the IP Address or Host Name of the server running the Print Audit Secure Server.

c. Virtual Directory - the name of the virtual directory configured on the Print Audit Secure Server. The default is "pasecure".

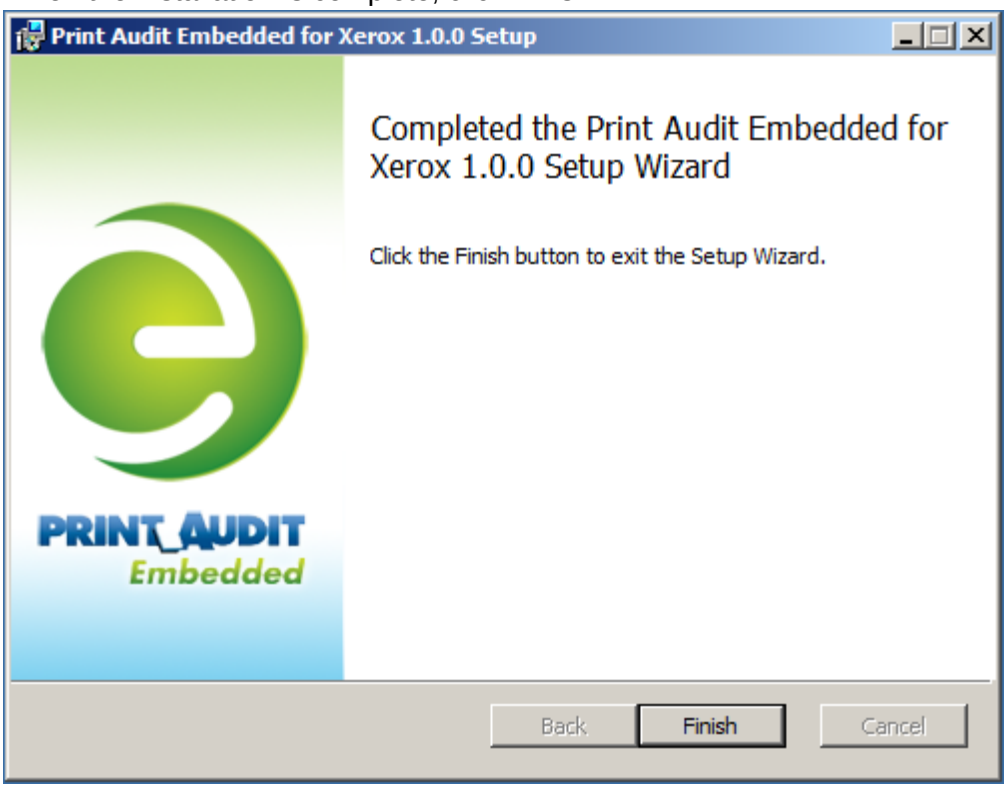
7. Select the Website name where the Embedded for Xerox web service will be created. It is recommended to use the Default Web Site. Click Next.



8. Click Install to begin installing Embedded for Xerox.



9. When the installation is complete, click Finish.



10. (Optional) Verify that IIS settings are correct. See the IIS Configuration/Setup for Print Audit Embedded for Xerox section in this document.

Notes on Print Audit Embedded for Xerox Logging

The Print Audit Embedded for Xerox can create some very large log files by when set to Debug logging. By default, the Print Audit Embedded for Xerox installer sets the logging level to "Info". We recommend that logging only be set to "Debug" on the advice of a qualified support technician.

Using Administrator credentials, open the file:

C:\Program Files (x86)\Print Audit Inc\Print Audit Embedded for Xerox\Main\NLog.config

At the bottom of the NLog.config file you will see this:

<logger name="service" minlevel="Debug" writeTo="service.file" />

<logger name="webapp" minlevel="Debug" writeTo="webapp.file" />

<logger name="authentication" minlevel="Debug" writeTo="authentication.file" />

By default, the logger will only keep a maximum of 10 log files at a time. The log files roll over once per day. If needed for troubleshooting purposes, the maximum number of logs can be increase by changing the maxArchiveFiles value. For example, maxArchiveFiles="10" will tell the logger to only keep 10 archived log files at a time.

Please note that any change to the NLog.config file will require a restart of the IIS service to take effect.

2. Configuration Embedded for Xerox

This Embedded for Xerox window in Print Audit 6 enables the configuration of all aspects of the Embedded for Xerox copier device. The different elements of the window are described below.

Pre-configuration checklist

If you are ready to begin configuring Print Audit 6 with Embedded for Xerox, you have:

- Installed the Print Audit Database Communicator, Database and Administration tools to a computer on the network that will be on and available at all times. The Print Audit Client should be installed on at least one workstation, to test printing and ensure that print jobs are being tracked correctly before continuing.
- Configured Print Audit 6 for user quotas, PIN codes and validated fields to be integrated into Print Audit 6 Embedded.
- Installed the Print Audit 6 for Xerox Embedded software on a computer that has Internet Information Services (IIS) and .Net installed, and is acting as a web server.
- Used this guide to configure Print Audit 6 Embedded on the Xerox EIP-enabled devices.

Overview

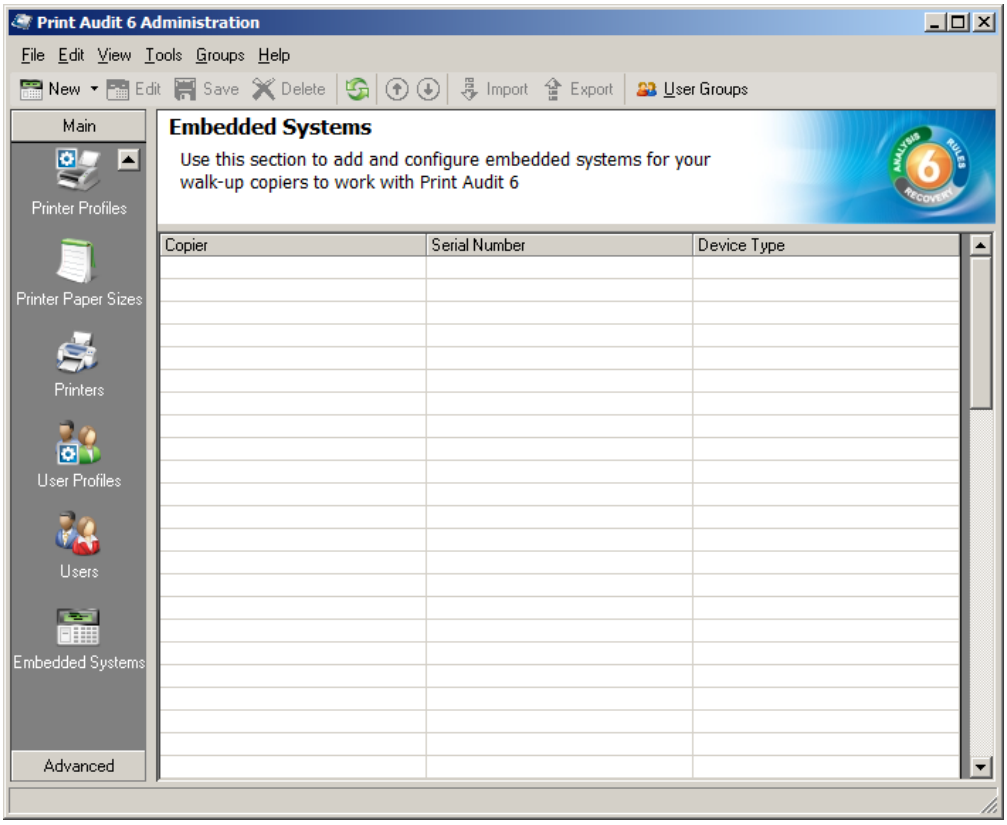
The Print Audit Administration tool provides the ability to configure Embedded for Xerox on all the MFP's in the environment using the Embedded Systems plug-in. Configure one copier for every physical Xerox MFP on which the Embedded Client will run.

Costs, limits, authentication methods and custom fields may be configured for each device.

Adding, Editing and Deleting Copiers in Print Audit 6

Use the Embedded Systems section of the Administration tool to add, edit and delete Embedded for Xerox copiers. A copier in the Administration tool represents a physical copier in the network.

To add a new copier:



1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Click the New button on the toolbar.
4. Select Embedded for Xerox from the dropdown list of embedded applications.
5. Press OK. The Add/Edit Embedded for Xerox window will appear.
6. At minimum, a copier name and the serial number of the copier must be provided. Please refer to the 'Embedded for Xerox Configuration Window' section below for more information about filling out the Embedded for Xerox window.
7. Click the Save button. The Embedded for Xerox Window closes and the copier appears in the Copiers list.

To edit a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.

3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Edit button on the toolbar. The Embedded for Xerox Window appears.
5. Make any needed changes to the copier.
6. Click the Save button. The Embedded for Xerox Window closes and the copier appears in the Copiers list.

To delete a copier:

1. Run the Print Audit Administration program.
2. Click the Embedded Systems button on the left hand side of the Print Audit Administration window. The list of existing copiers appears on the right side. It may be necessary to scroll the left side down to reveal the Embedded Systems button.
3. Select the copier to be edited from the list of copiers. It appears highlighted.
4. Click the Delete button on the toolbar. A message appears to verify removal of the copier.
5. Click the Yes button to delete the copier. The list of copiers refreshes.

Configuring Print Audit 6 with the Xerox MFP

This Embedded for Xerox window in Print Audit 6 enables the configuration of all aspects of the Embedded for Xerox copier device. The different elements of the window are described below.

General

Copier name - The name to describe the copier. Enter a name that is descriptive enough to distinguish the copier from others. For example "Third Floor Xerox WorkCentre 7835".

Serial number - The serial number of the Xerox MFP.

Report as printer - Use this to select an already existing Print Audit printer with which to associate the copier. For example, if there is an MFP in the office that users print to which is already in the Print Audit database, choose that MFP here for the copier so that all transactions are reported as the same printer. If a printer is not selected here, Print Audit will record transactions for this copier as the copier name.

Report as user - Use this to select an existing Print Audit user whom to associate all jobs from this copier. Use this functionality to still have individual user authentication, but for reporting purposes report all jobs to a single user.

Authentication type - Select how the user will authenticate to the copier before they can do transactions. The authentication type determines how a user identifies themselves to the copier before they can do a transaction. The following options are available:

- None - Users do not have to authenticate before using the copier. All transactions are recorded to a generic user.

- PIN code - Users must enter their Print Audit PIN.
- Card Reader
- Card Reader or PIN
- Active Directory - Print Audit Embedded for Xerox can authenticate directly against an Active Directory server. When this option is selected, at least one Active Domain must be entered in the AD Domain(s) field. Multiple domains can be used if they are separated by a comma (,). When this authentication method is used, users will have to select the domain from a dropdown on the Print Audit Embedded for Xerox application as well as entering their Username/Password.

Require additional password - Check this box to require the user to enter an additional password before they can authenticate using the Authentication type selected above.

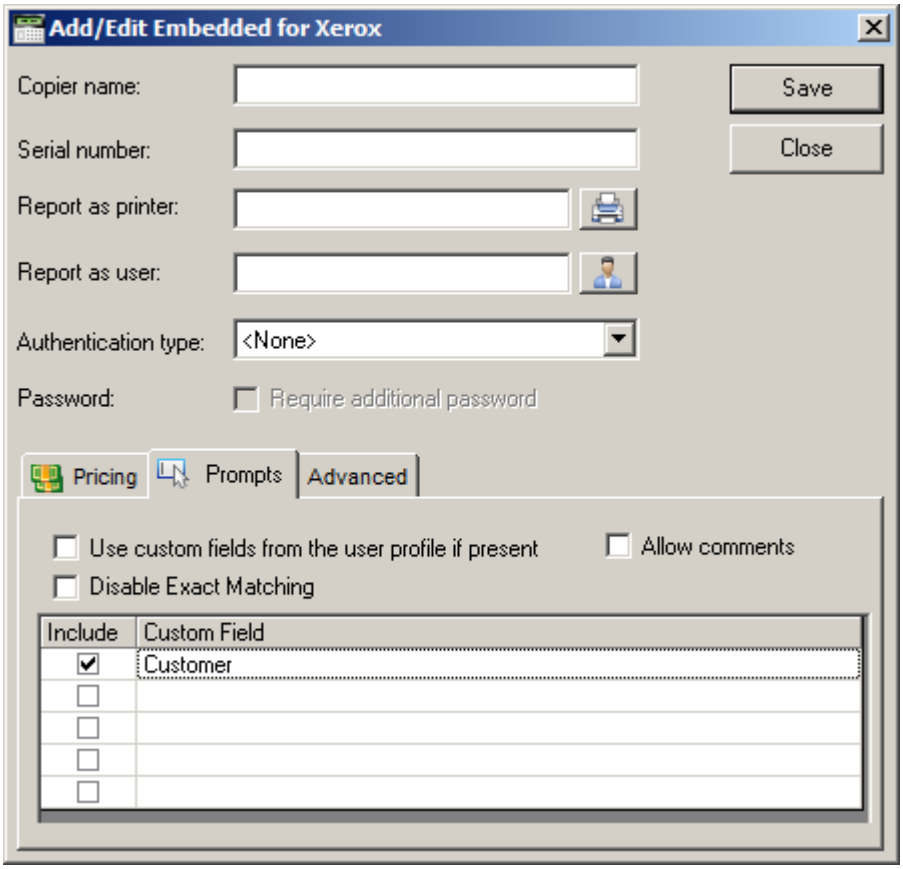
Pricing tab

This tab contains the pricing for each function on the copier.

To edit the pricing for a particular function:

1. Clear the "Track" column for the function to disable the tracking of transactions of that type.
2. Select from the list the function that is to change and click the Edit button. The Configure Pricing and Paper Size Window appears.
3. Set the pricing as it makes sense for this copier in the organization.
4. Click the Done button. The Configure Pricing and Paper Size Window closes.

P rompts tab (only with Print Audit 6 Recovery)



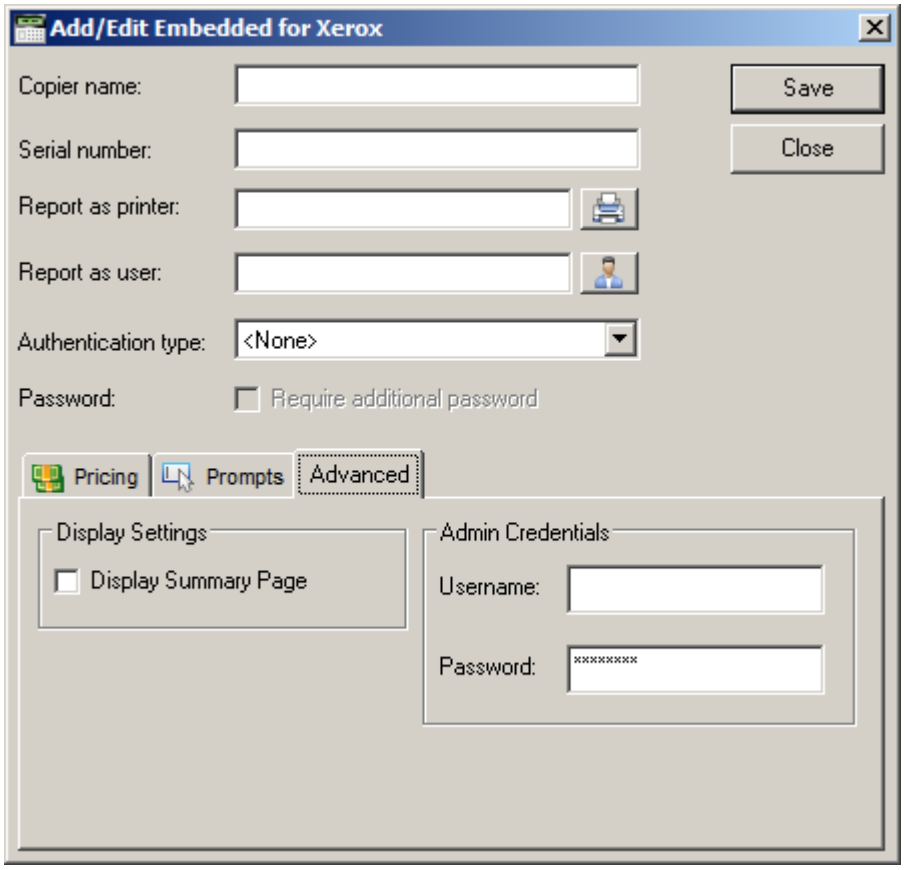
This tab is only relevant when using Print Audit 6 Recovery for the charge-back of printing.

- For each Activity the user can be required to enter values for Custom Fields. Custom Fields are setup in the Custom Fields section of the Print Audit Administrator. On this tab, select from any one of the Custom Fields configured and define a custom prompt for each one.
- Use custom fields from the user profile - Check this box to override the default custom field choices with the custom fields set in a user's User Profile.
- Allow comments - Check this box if the user can enter general comments about the job.
- Disable Exact Match - Check this box if the user can enter the custom field directly in the field and proceeds to the next step without selecting from the list.
- Custom fields - The custom fields list contains all custom fields that have been defined. To use a custom field for the activity, check the Include check box.

Advanced tab

This tab is relevant for display options.

- Display Summary Page - check this box if you would like to view the summary page of all selected prompt / comment values.



- Admin Credentials - enter the login credentials for the MFP admin. This is used to lock and unlock the device services.

Extended configuration settings

Described below are a small number of configuration settings which are only available by making modifications to the following file:

C:\Program Files (x86)\Print Audit Inc\Xerox Embedded\Main\App_Data\AppSettings.config

Enabling Print Audit 6 Job Tracking:

To modify Print Audit 6 Job Tracking support, open *AppSettings*.config, and modify the ENABLE_PA_EMBEDDED value with 'True' or 'False':

<add key=" ENABLE_PA_EMBEDDED " value="True" />

In this example, job tracking is enabled.

Database Communicator Location:

To modify Print Audit Database Communicator location after installation, open *AppSettings*.config, and modify the COMMUNICATOR_HOST value with the new computer name where the Database Communicator will reside:

<add key="COMMUNICATOR_HOST" value="HOSTNAME" />

In this example, HOSTNAME is the name of the computer where the Database Communicator will reside.

Database Communicator Port:

To modify the port number of the Database Communicator, modify the COMMUNICATOR_PORT value:

<add key="COMMUNICATOR_PORT" value="17520" />

Database Communicator Timeouts:

To modify the number of seconds to allow the embedded application to query the Database Communicator before timing out, modify the COMMUNICATOR_QUERYTIMEOUT value:

<add key="COMMUNICATOR_QUERYTIMEOUT" value="30" />

To modify the number of seconds that the embedded application will wait for a response from the Database Communicator whenever there is an attempt to establish communication with the Database Communicator over TCP/IP, modify the COMMUNICATOR_CONNECTTIMEOUT value:

<add key="COMMUNICATOR_CONNECTIMEOUT" value="5" />

Enabling support for Print Audit Secure:

To modify Print Audit 6 Job Tracking support, open *AppSettings*.config, and modify the ENABLE_PASECURE_EMBEDDED value with 'True' or 'False':

<add key=" ENABLE_PASECURE_EMBEDDED " value="False" />

In this example, support for Print Audit Secure is disabled.

Print Audit Secure Location:

To modify the Print Audit Secure IP Address after installation, open *AppSettings*.config, and modify the SECUREIPADDRESS value with the IP Address/host name where the Print Audit Secure server will reside:

<add key=" SECUREIPADDRESS " value="10.121.56.111" />

In this example, 10.121.56.111 is IP Address where the Print Audit Secure Server will reside.

Print Audit Secure Virtual Directory:

SECUREVIRTUALDIRECTORY value with the new computer name where the Print Audit Secure web application will reside:

<add key=" SECUREVIRTUALDIRECTORY " value="PASecure" />

In this example, PASecure is the name of the computer where the Database Communicator will reside.

Print Audit Xerox Server IP Address:

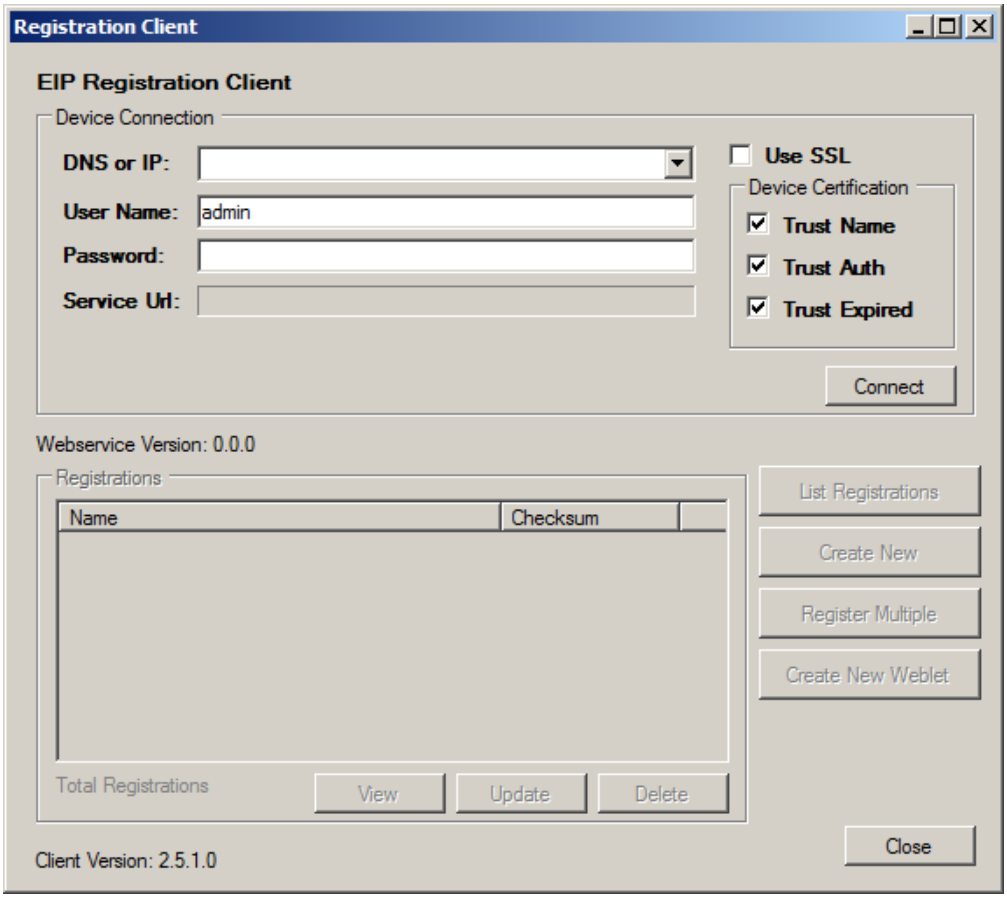
ServerIpAddress value of the computer hosting the IIS server for Print Audit Embedded for Xerox. Please Note: this entry is required for using Print Audit Embedded for Xerox with a Swipe/Prox card reader. See the entry "Configuring a Card Reader for Print Audit Embedded for Xerox".

<add key="ServerIpAddress" value="192.168.0.15"/>

In this example,192.168.0.15 is the IP Address of the IIS server hosting the Print Audit Embedded for Xerox application.

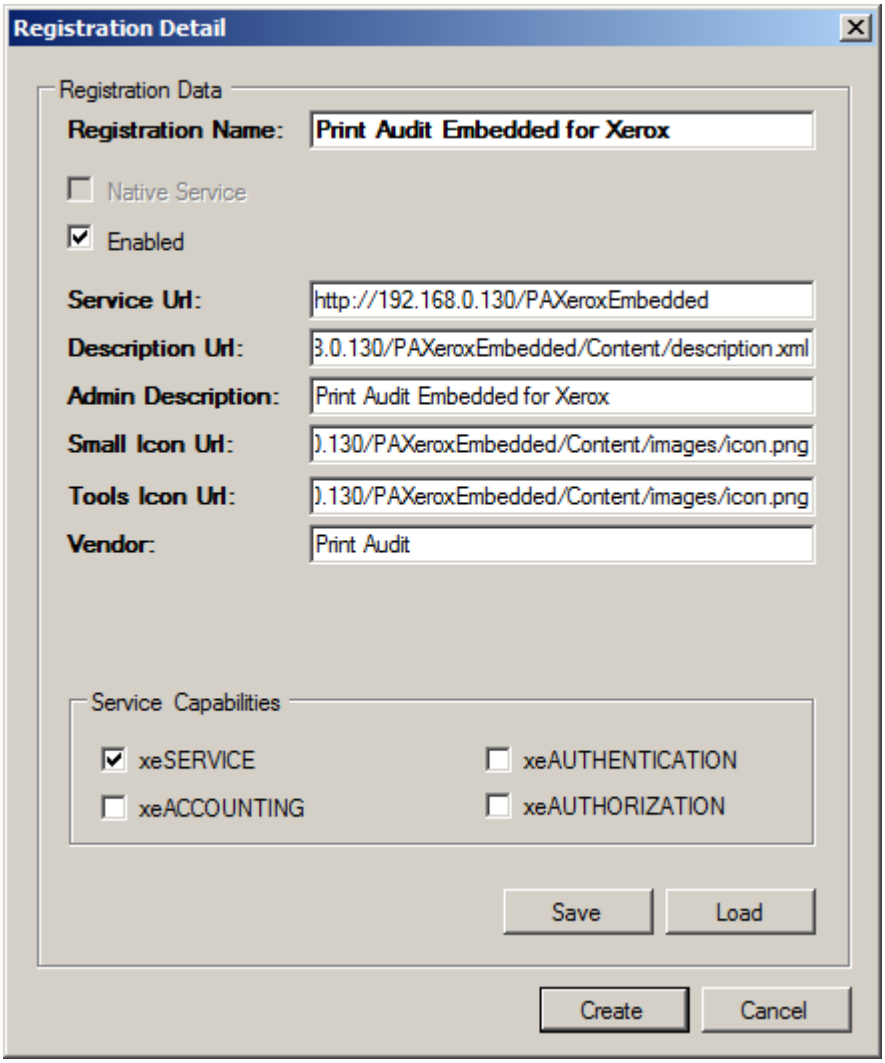
Configuring the Xerox MFPs with the Embedded Client for Xerox

Registering Xerox Embedded on the Xerox MFPs Device



1. Obtain a copy of the Registration Client tool by clicking here if you do not have a copy.
2. Open the Registration Client tool.
3. Enter Xerox MFP's connection information which includes:
   - IP Address or DNS name (Fully Qualified Domain Name)
   - Admin User Name
   - Admin Password
4. Click "Connect" to gain access to the list of device services.
5. Click "Create New" to register new application
   (Note: If the application is already registered but you would like to make edits to the configuration or delete it. Click the "List " button and select the application from the list provided to you. The registration options will be provided to you on the right hand side which include: View, Update and Delete)

6. When the Registration Detail Form is presented. Please fill out the following information:



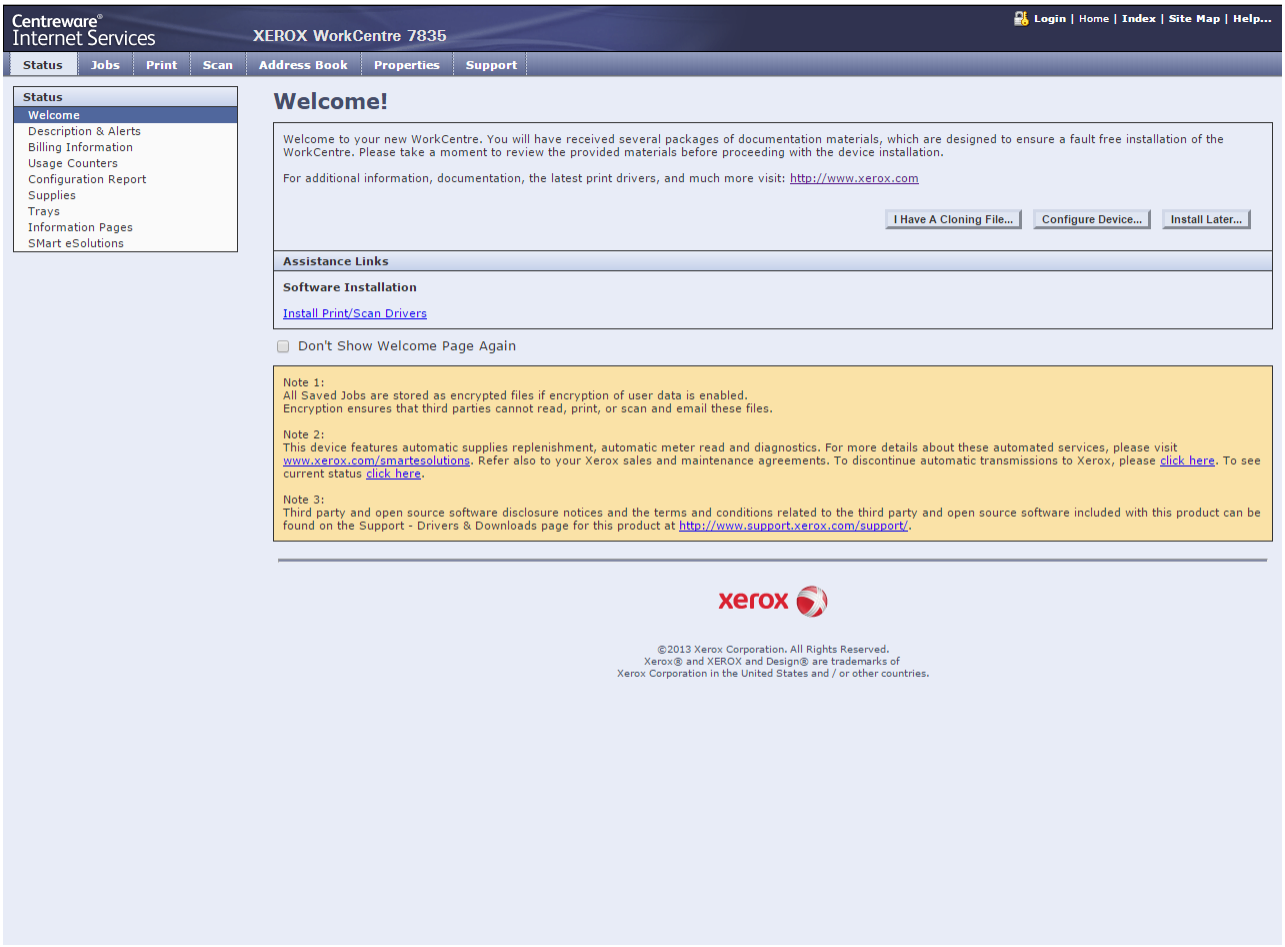
(Note: The IP address provided "192.168.0.130" is an example of the install location. Please replace this with the IP address of where your Xerox Embedded hosted solution was installed)

Registration Name: Print Audit Embedded for Xerox
Select: Enabled
Service URL: http://192.168.0.130/PAXeroxEmbedded
Description URL: http://192.168.0.130/PAXeroxEmbedded/Content/description.xml
Admin Description: Print Audit Embedded for Xerox
Small Icon URL: http://192.168.0.130/PAXeroxEmbedded/Content/images/icon.png
Tools Icon URL: http://192.168.0.130/PAXeroxEmbedded/Content/images/icon.png
Vendor: Print Audit

7. Click "Create" to register the application.

Configuring the Panel Interface

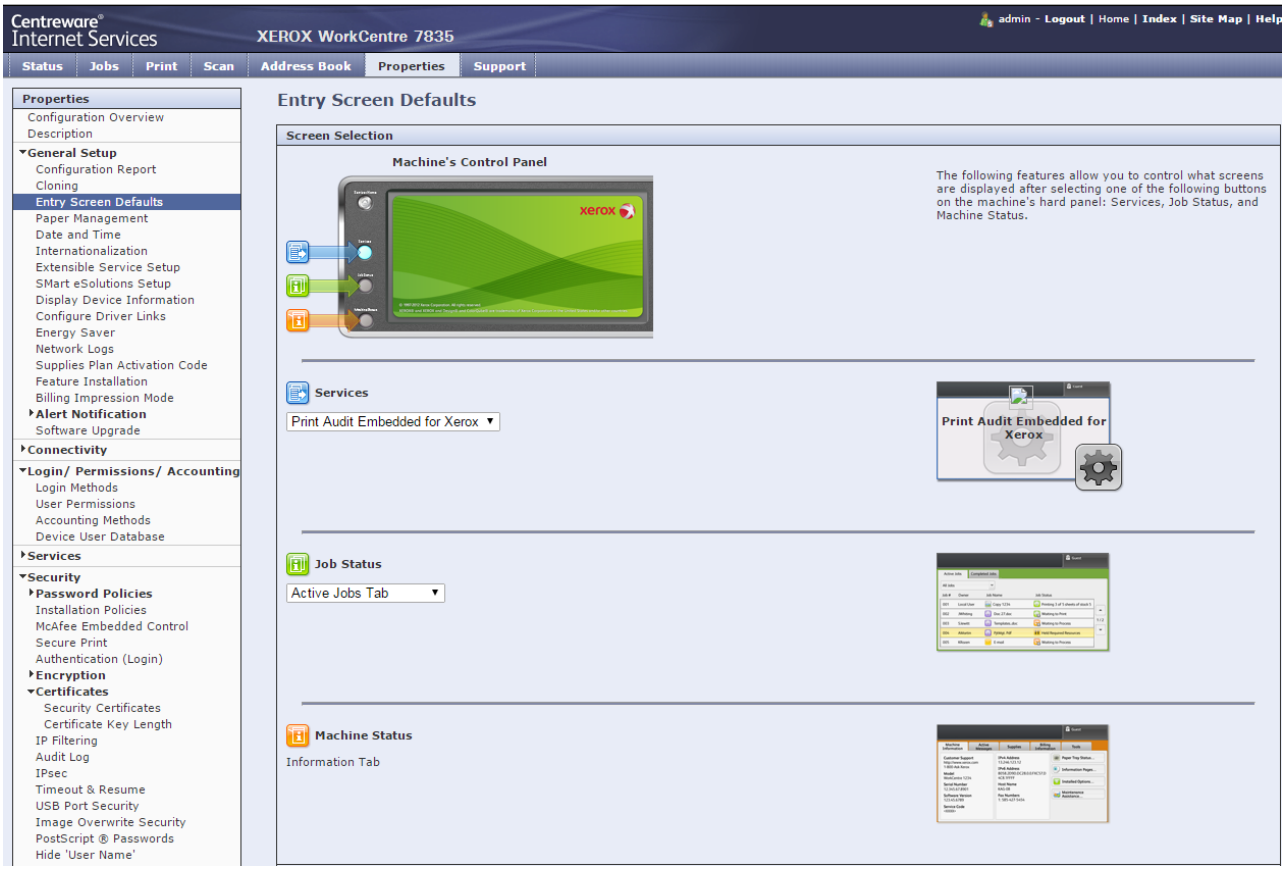
Please Note: These instructions are modeled after the XEROX WorkCenter 7835 and may be slightly different depending on the device in question.



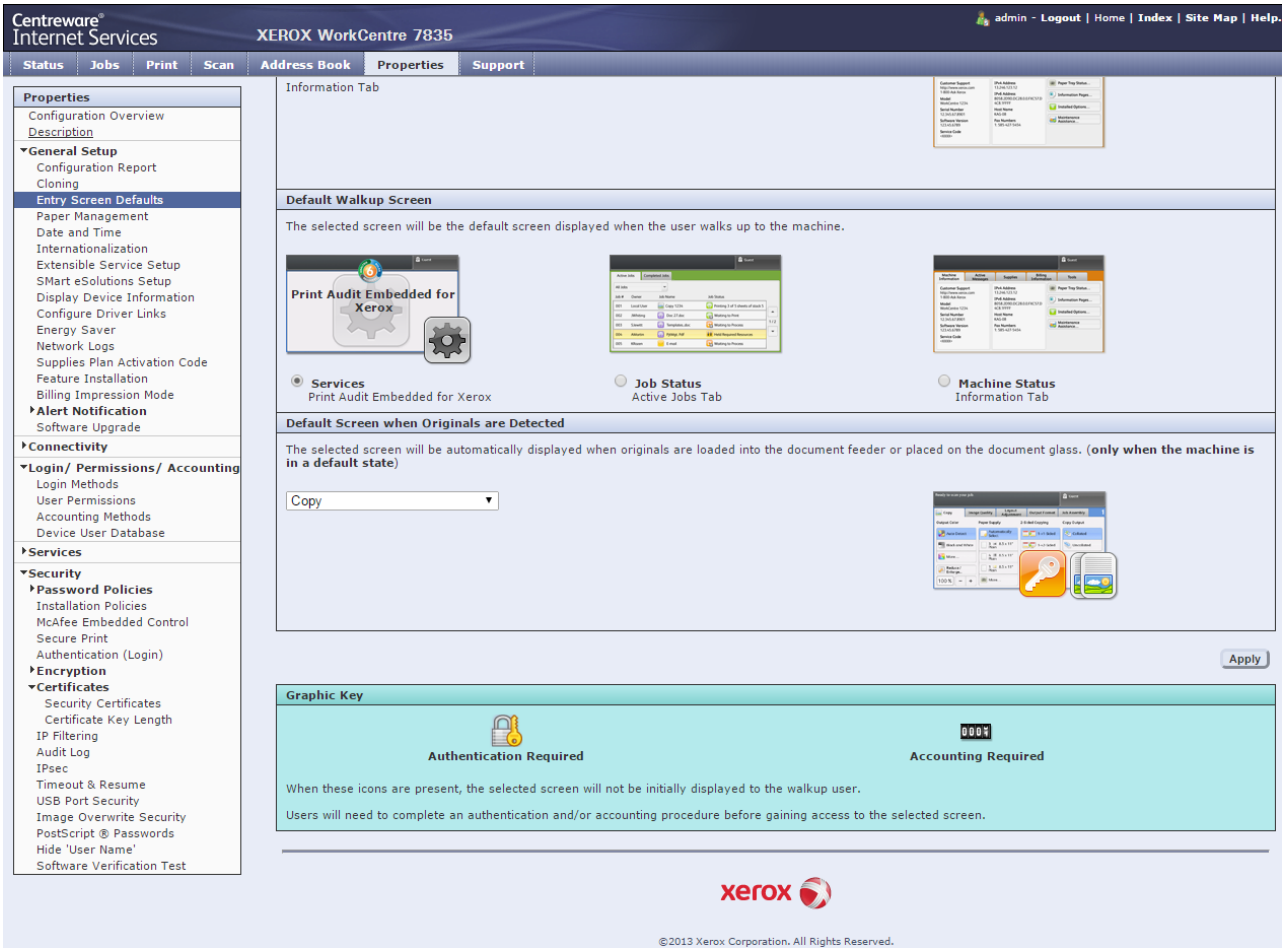
Selecting Entry Screen Defaults

1. Navigate to "Properties" from the top menu, then expand “General Setup” on the menu to the left and select “Entry Screen Defaults”

(Note: You may be prompted to enter admin credential)

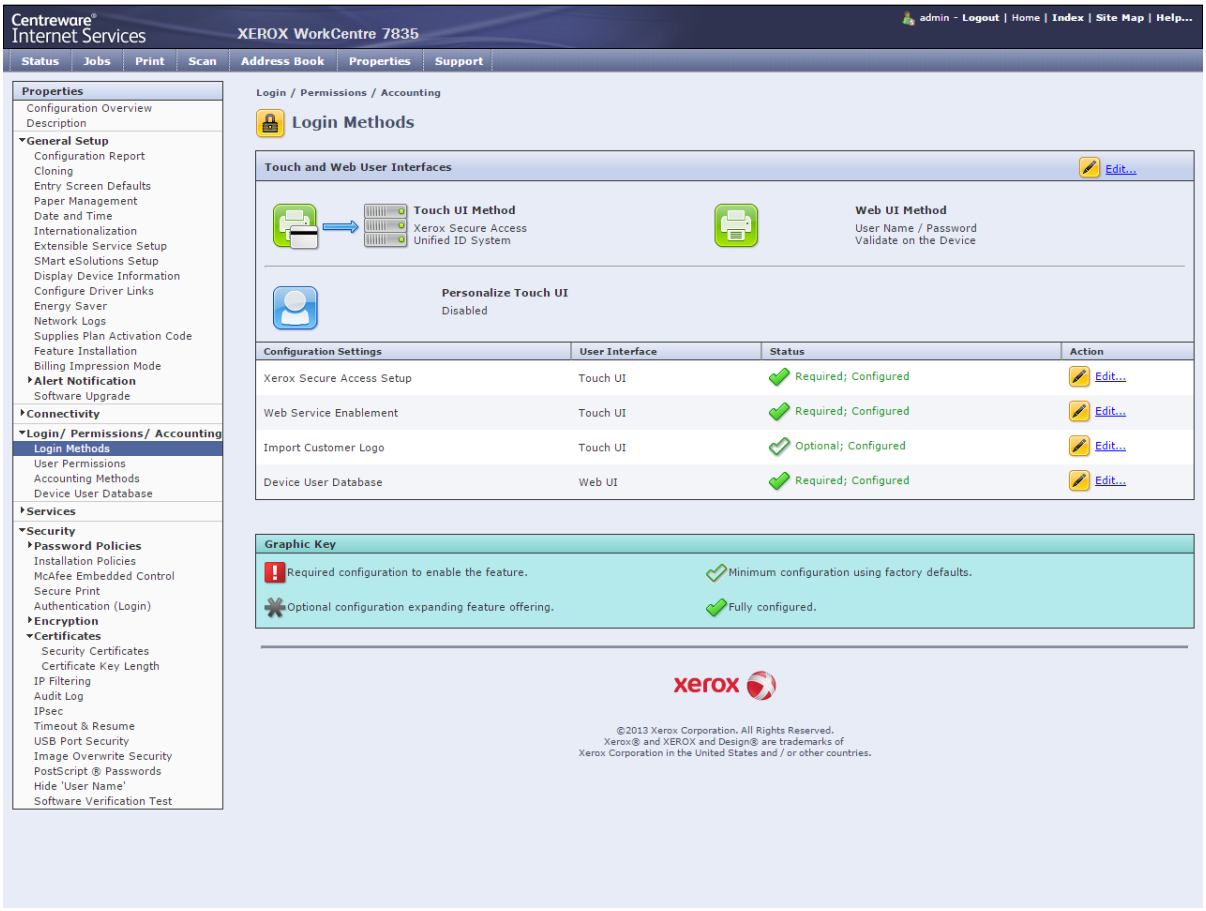


2. On the section labeled "Services", Select "Print Audit Embedded for Xerox" from the drop down list.

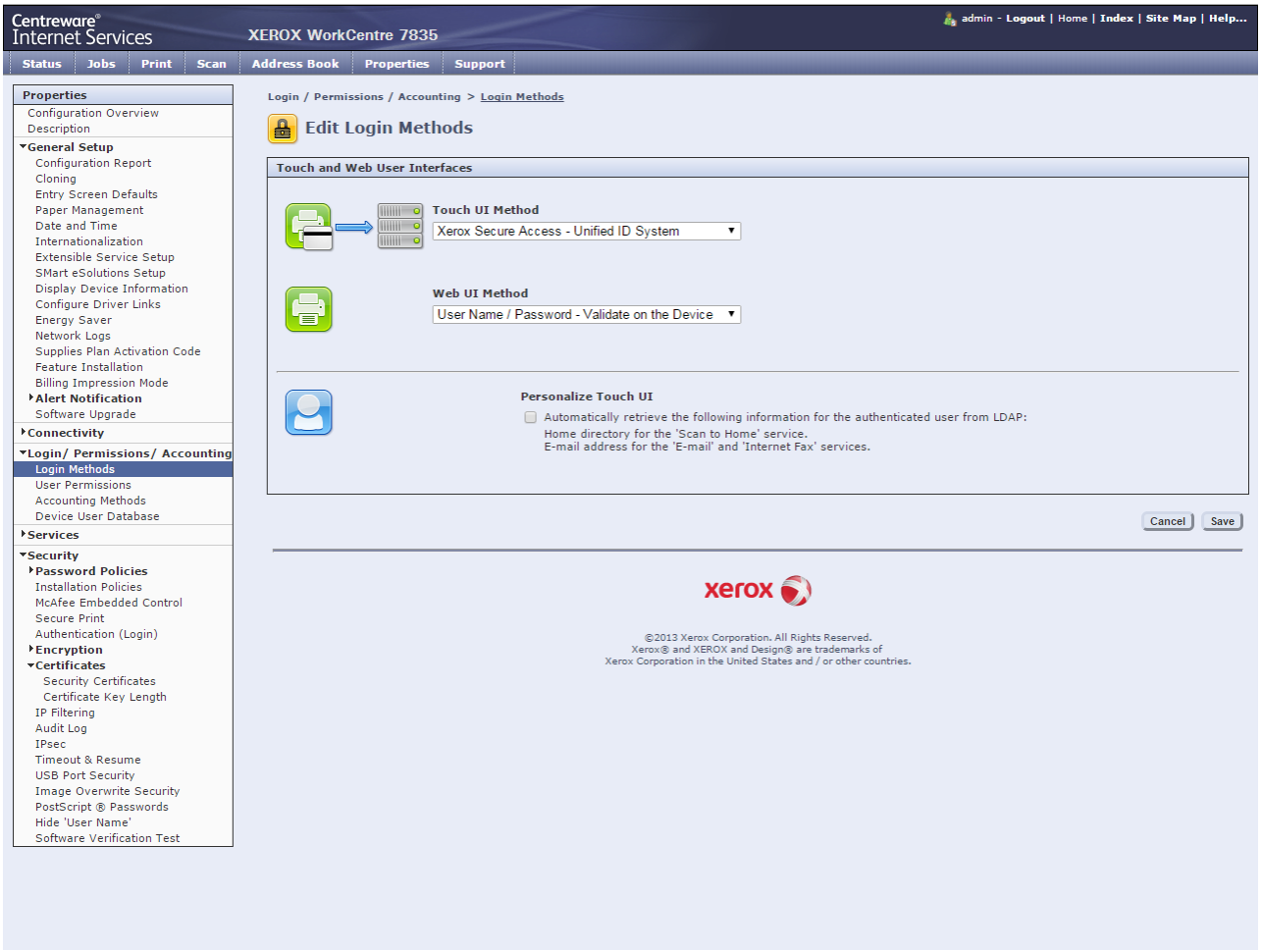


Configuring the authentication server details

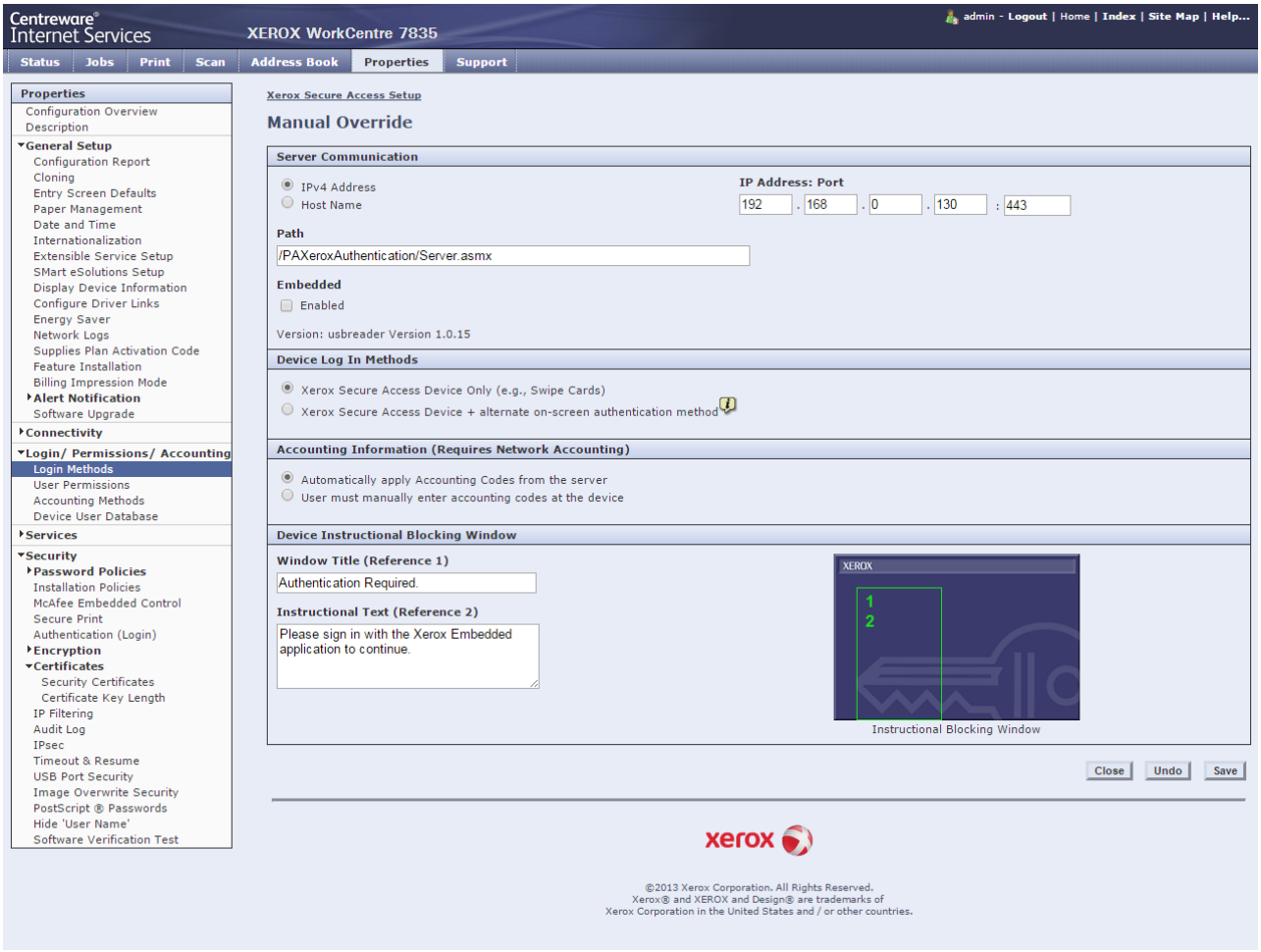
1. Navigate to "Properties" from the top menu, expand "Login / Permissions / Accounting" section on the left hand side menu and select "Login Methods".



2. Click the Edit icon in the "Touch and Web User Interfaces" section. 

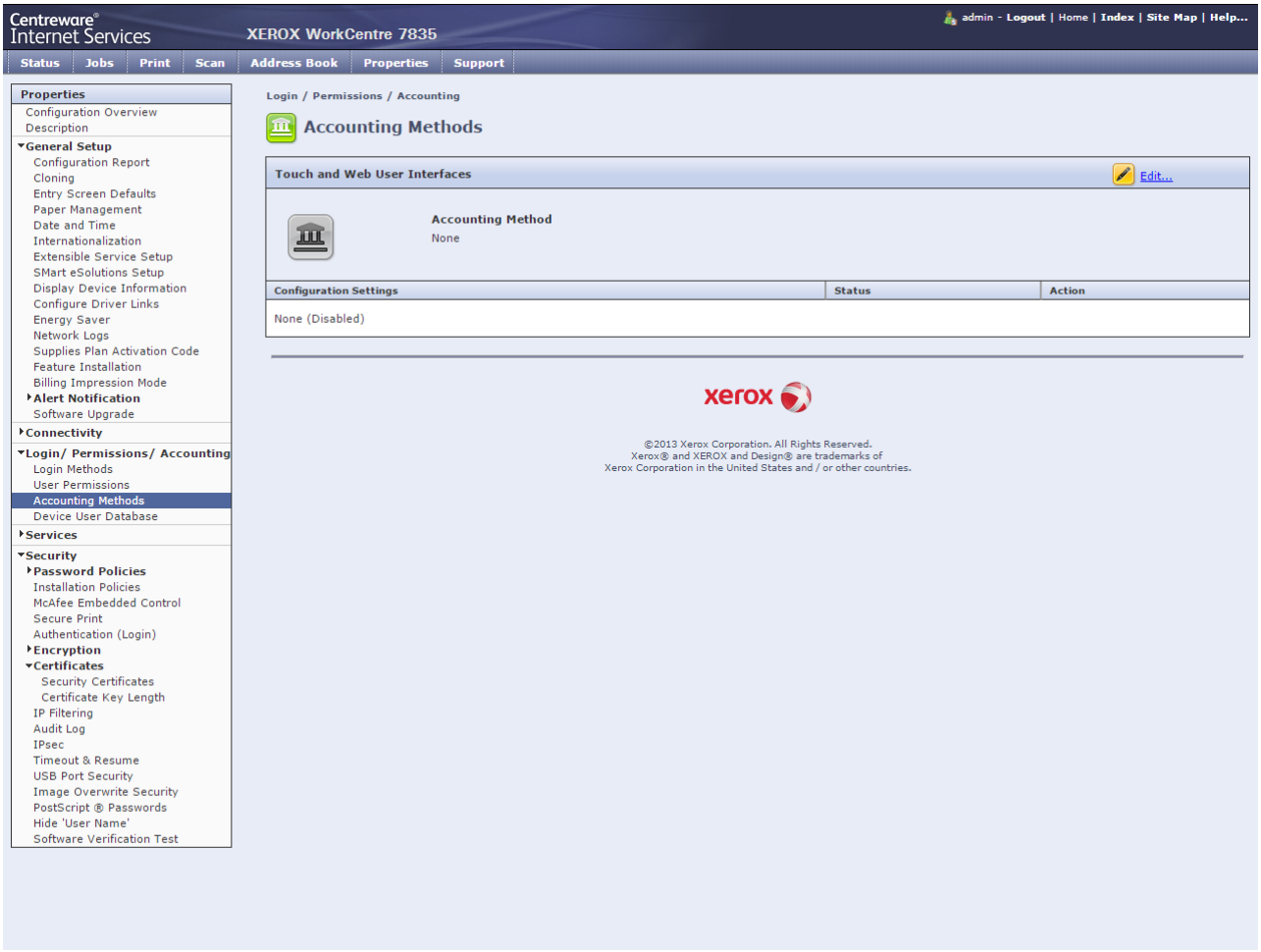


3. In the "Touch UI Method" dropdown select "Xerox Secure Access - Unified ID System".
4. In the "Web UI Method" dropdown select "User Name / Password - Validate on the Device".
5. Save and return to the previous screen.
6. Click the "Edit" button in the "Xerox Secure Access Setup" configuration settings section.
7. Click the "Manually Override Settings" button.
8. When presented with the "Manual Override" page, enter the following information.

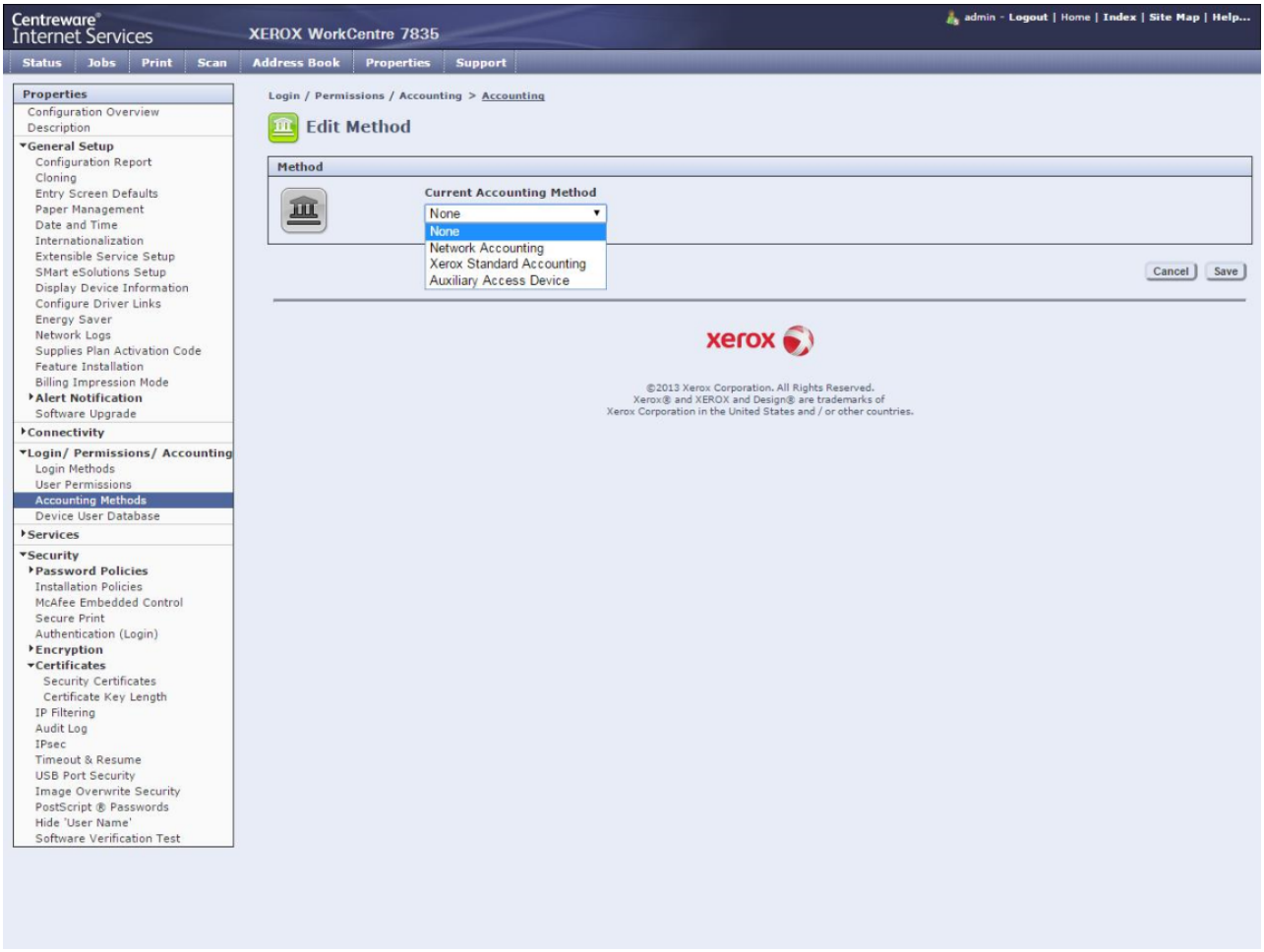


- In the Server Communication section select "IPv4 Address" radio button.
- Enter the "IP Address: Port". The IP will be the location of the Xerox Embedded hosted installation. Enter 443 for the port number as the authentication server uses SSL.
- Enter "/PAXeroxAuthentication/Server.asmx" as the Path.
- Uncheck the "Embedded" check box, as this might disable some proxy cards.
- From the "Device Log In Methods" section select "Xerox Secure Access Device Only (e.g., Swipe Cards)".
- Under the "Accounting Information (Requires Network Accounting)" section select " Automatically apply Accounting Codes from the server".

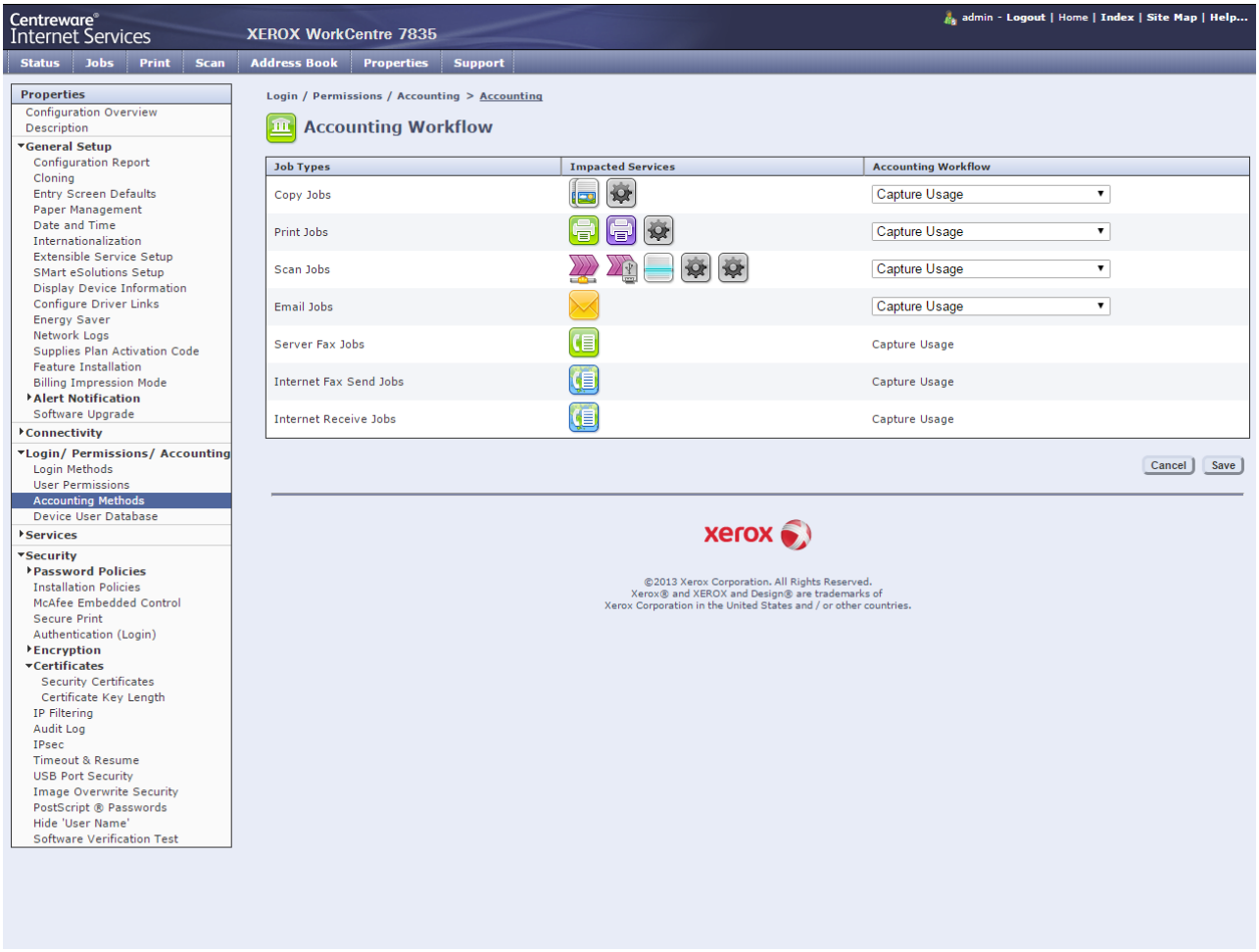
9. Click "Save" to continue. Navigate to "Login / Permissions / Accounting" and then "Accounting Methods". Click Edit next to Touch and Web User Interface.



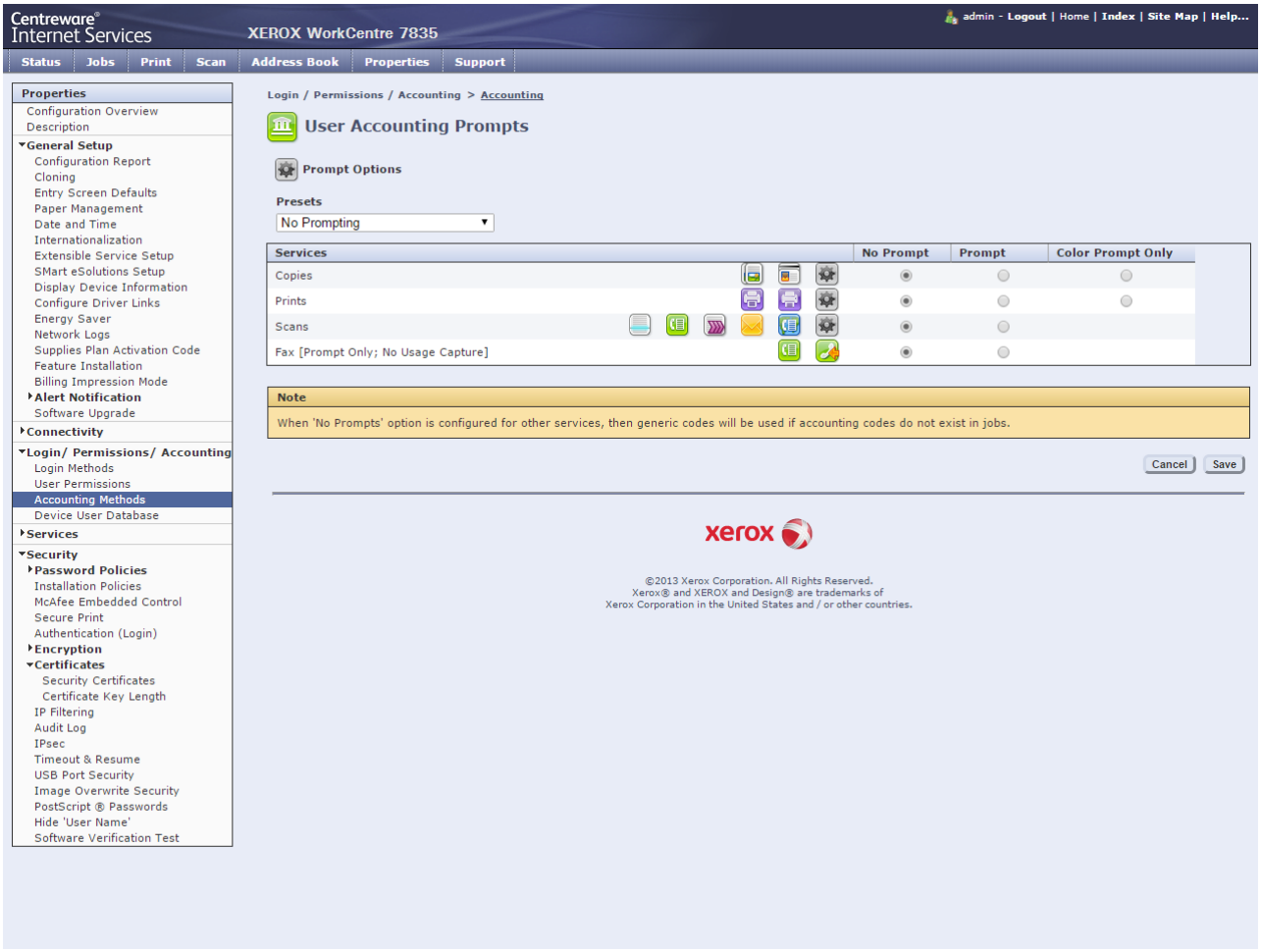
10. Set the Accounting Method to “Network Accounting”. Click on ‘Save’ to return to previous screen. (Select Accounting Methods)



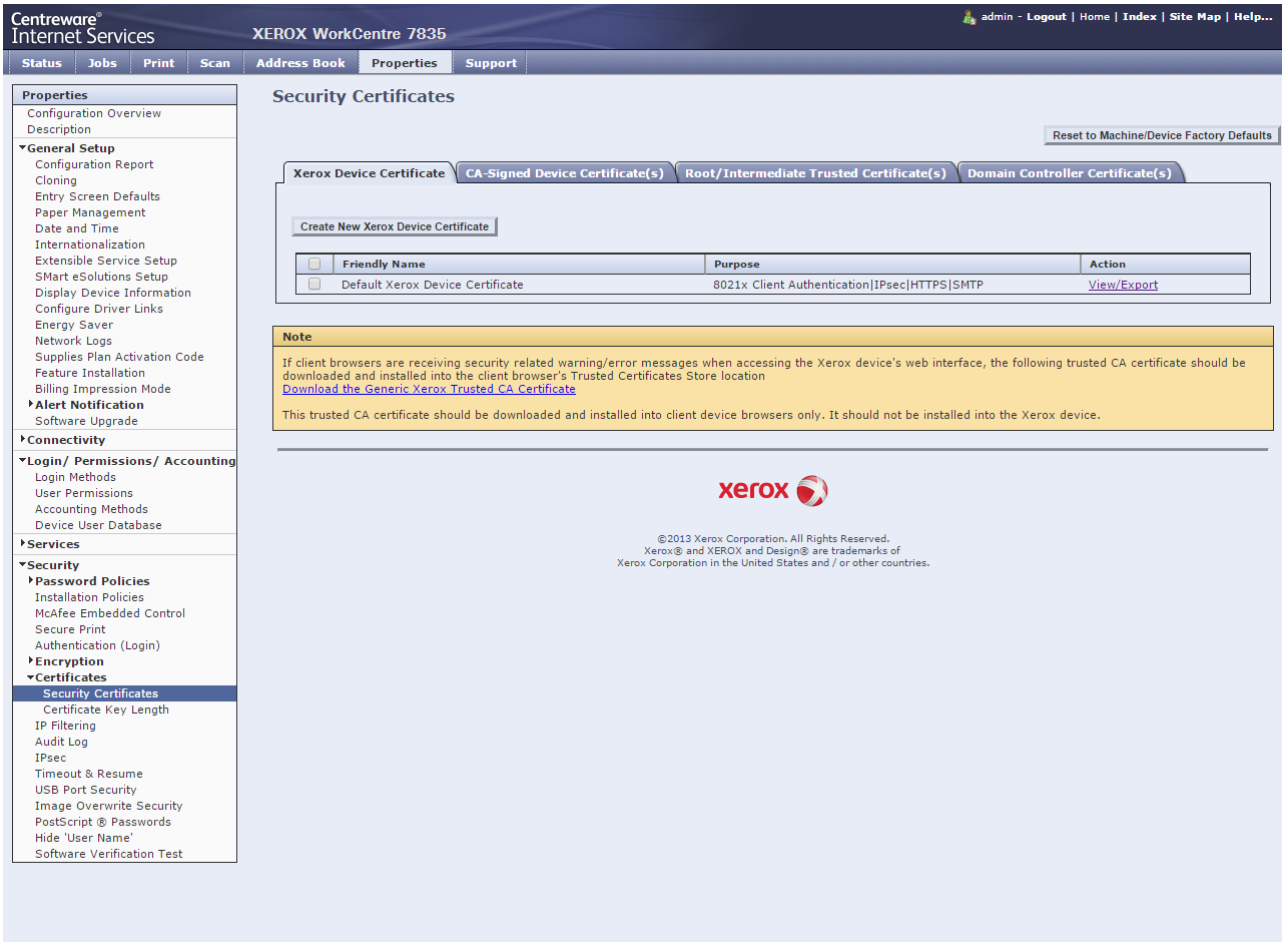
11. Click Edit next to the ‘Accounting Workflow’. All Job Types must be set to ‘Capture Usage’. Click Save.



12. Click Edit next to the ‘User Accounting Prompts’. Select ‘No Prompting’ from the Presets dropdown. Click Save.



13. Navigate to "Properties" from the top menu and select "Security" then "Certificates " and " Security Certificates" section on the left hand side menu.

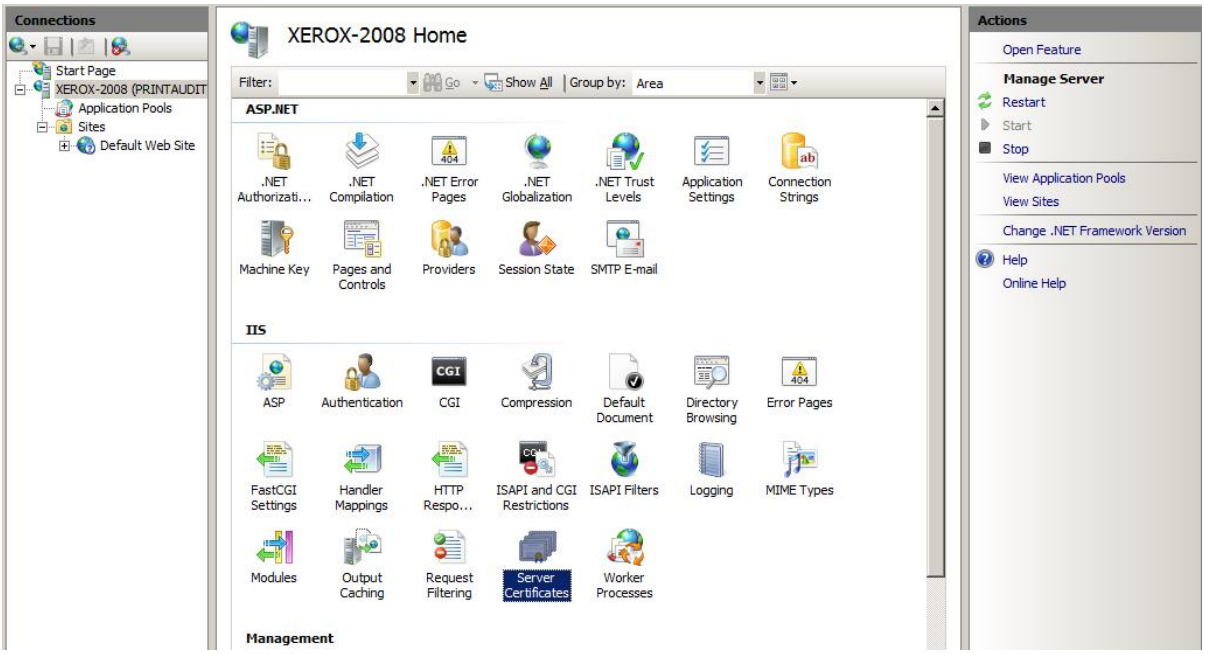


14. Ensure that there is a certificate installed on the Xerox device. If there is no certificate listed, please create a new Xerox device certificate

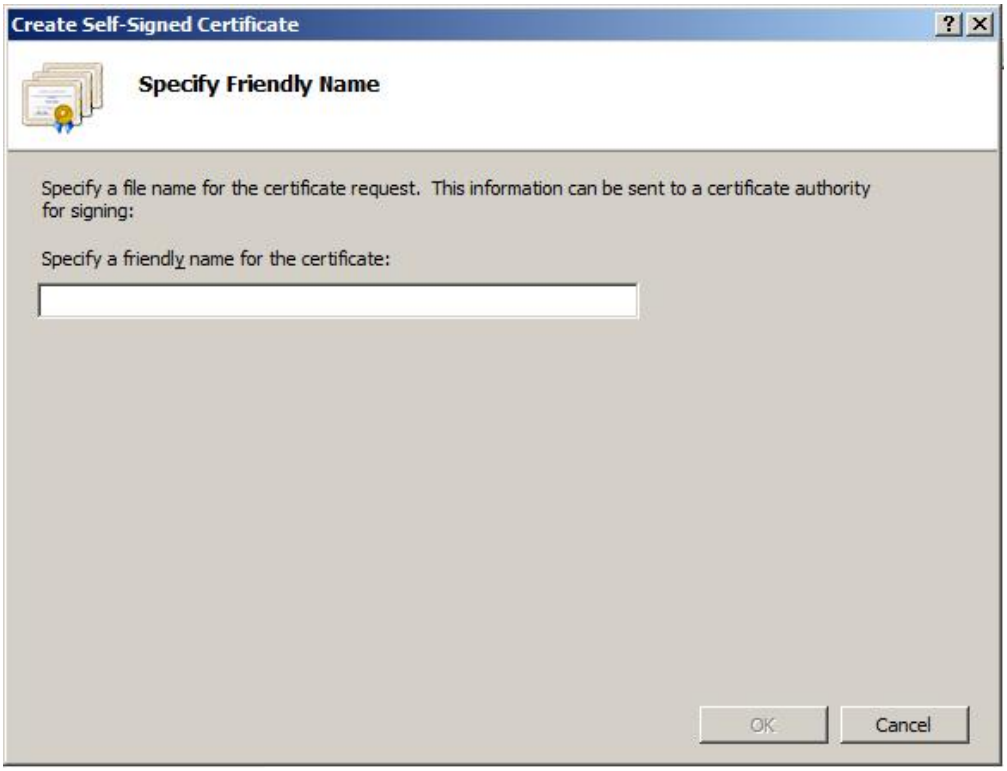
Installing\Verifying the Print Audit Embedded for Xerox Certificate

The Print Audit Embedded for Xerox requires that an SSL certificate be installed on the IIS web server to provide secure authentication (via HTTPS) on the Xerox device. If this certificate is not installed or is not properly bound to the web application, the user will encounter communication errors on the Xerox device. The SSL certificate can be an existing one or a self-signed certificate can be created if an SSL certificate is not already installed.

1. Open the Internet Information Services (IIS) Manager.

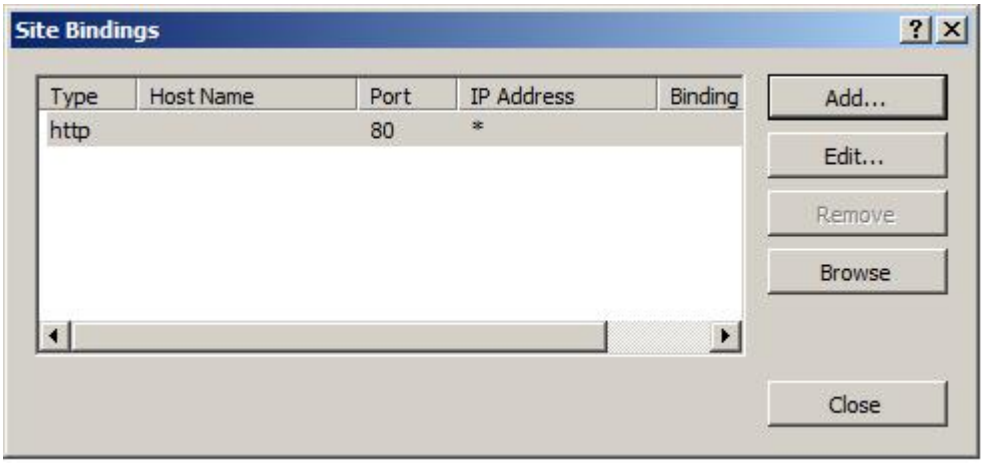


2. Double click on "Server Certificates" to bring up a list of installed certificates on the IIS Server .
3. If no certificates exist, create a new Self-signed certificate by clicking on "Create Self-Signed Certificate..." under Actions.

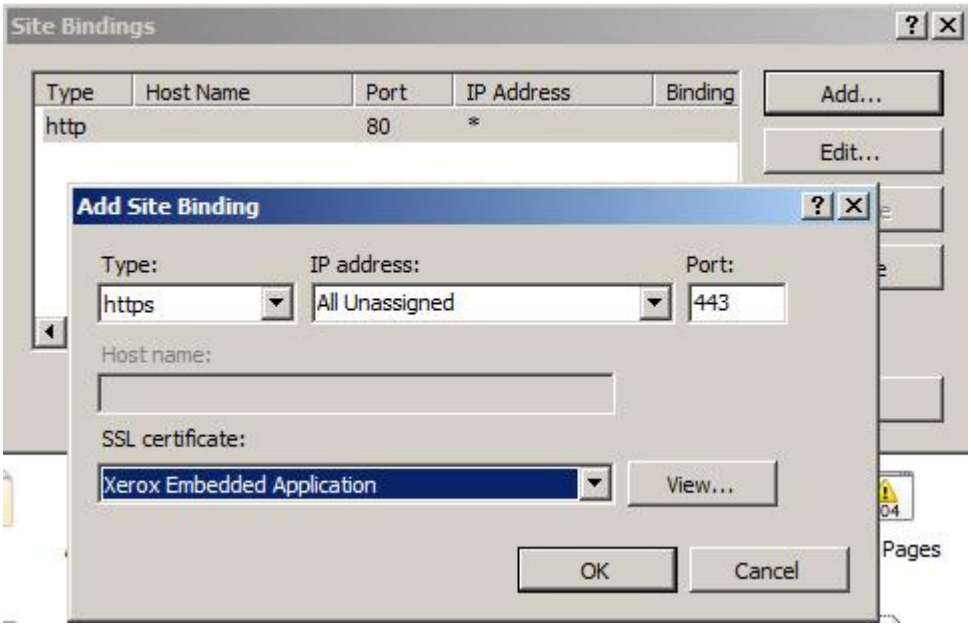


4. Enter a Friendly Name for the Self-signed certificate ie: "Xerox Embedded Application".

5. New versions of IIS may prompt for a certificate store to place the certificate. Select " Personal" or "Web Hosting" from the drop down.
6. Click OK.
7. Locate the web site containing the Print Audit Embedded for Xerox sites. By default, they are located under "Default Web Site".
8. Under "Actions --> Edit Site" (located on the right hand side of the IIS Manager), click on " Bindings..."



9. Locate the Site Bindings for type "https". If one does not exist, click on "Add".



10. Select "https" from the Type dropdown. Select the Self-signed certificate created in Steps 3-6 .
11. Click "OK and then "Close".

Configuring Print Audit Embedded for Xerox for use with a Card Reader

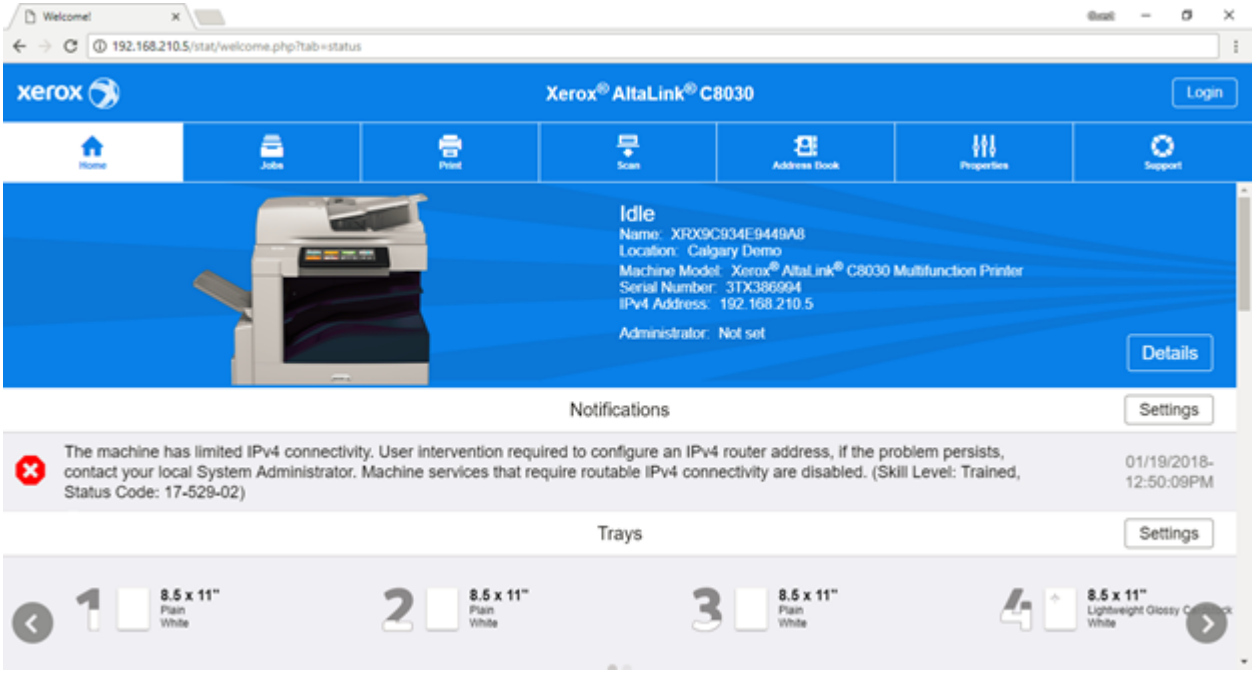
In order for authentication via Swipe/Prox card reader to work, the Print Audit Embedded for Xerox application must be configured to point to the IP address of the IIS server that the Embedded Xerox application is installed on. To configure this value:

1. Open the ...\Print Audit Embedded for Xerox\Main\AppSettings.config file for editing. This can be done by running Notepad as Administrator or copying the file to the desktop, editing it and then copying it back.
2. For the parameter "<add key="ServerIpAddress" value="IPADDRESS"/> , change the value to the IP Address of the IIS server that Print Audit Embedded for Xerox is installed on.
3. In IIS, restart the Application Pool "PAXEAuthAppPool" for the change to take effect.

2a. Altalink Configuration

Configuring the Panel Interface

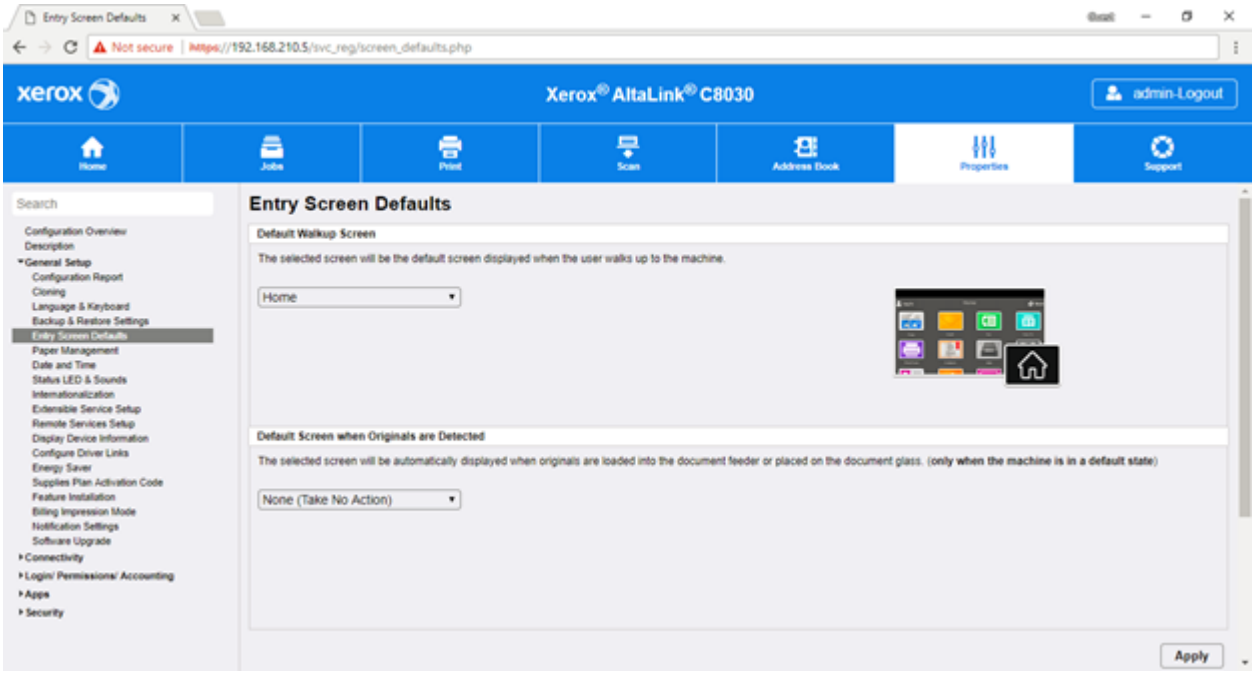
Please Note: These instructions are modeled after the XEROX AltaLink C8030 and may be slightly different depending on the device in question.



Selecting Entry Screen Defaults

1. Navigate to "Properties" from the top menu, then expand “General Setup” on the menu to the left and select “Entry Screen Defaults”

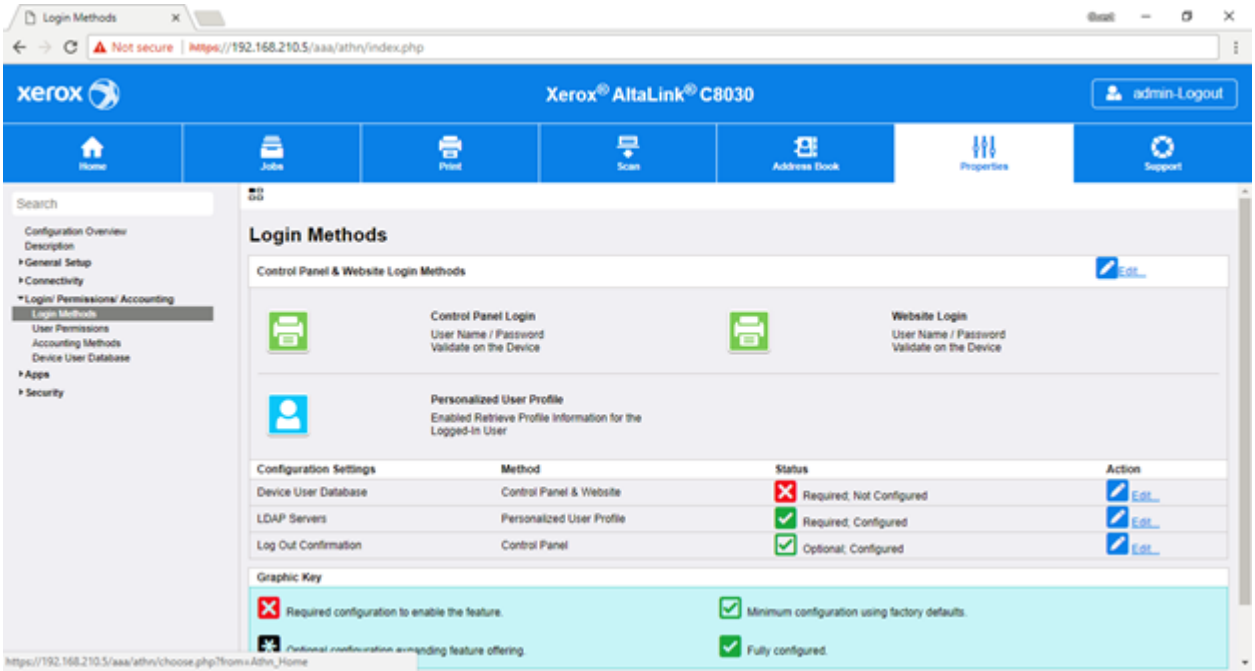
(Note: You may be prompted to enter admin credential)



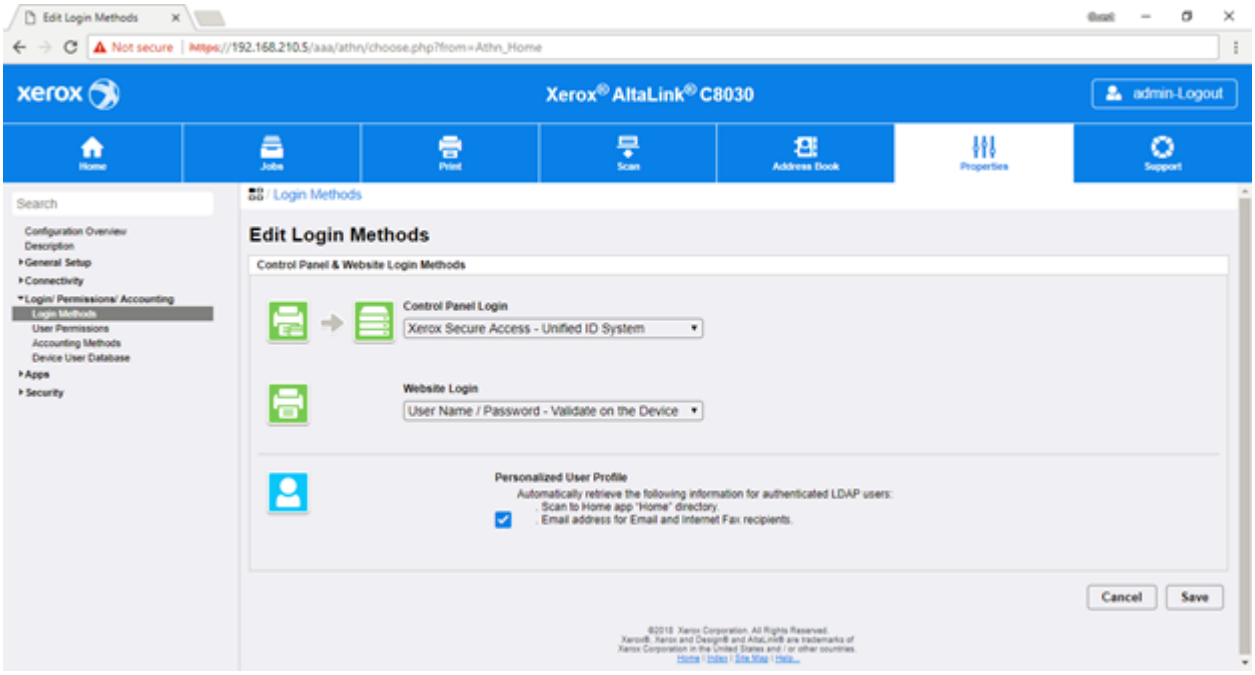
2. On the section labeled "Services", Select "Print Audit Embedded for Xerox" from the drop down list.

Configuring the authentication server details

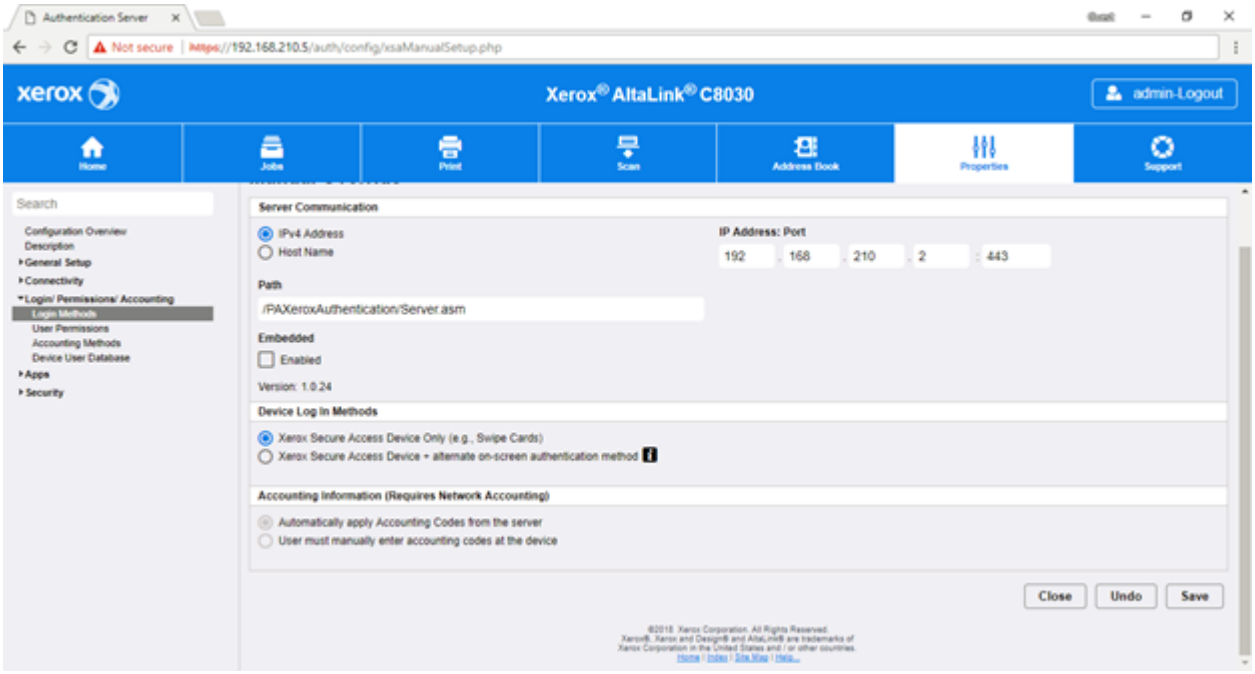
1. Navigate to "Properties" from the top menu, expand "Login / Permissions / Accounting" section on the left hand side menu and select "Login Methods".



2. Click the Edit icon in the "Control Panel & Website Login Methods" section. 



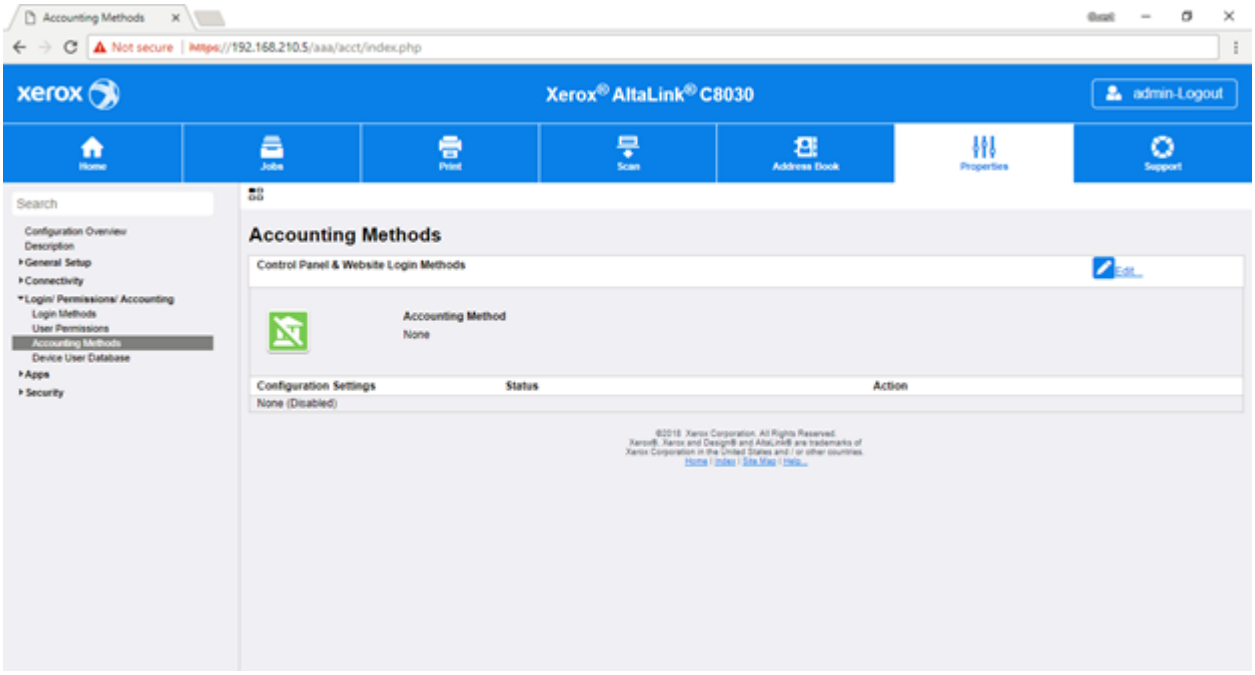
3. In the "Control Panel Login" dropdown select "Xerox Secure Access - Unified ID System".
4. In the "Website Login" dropdown select "User Name / Password - Validate on the Device".
5. Save and return to the previous screen.
6. Click the "Edit" button in the "Xerox Secure Access Setup" configuration settings section.
7. Click the "Manually Override Settings" button.
8. When presented with the "Manual Override" page, enter the following information.



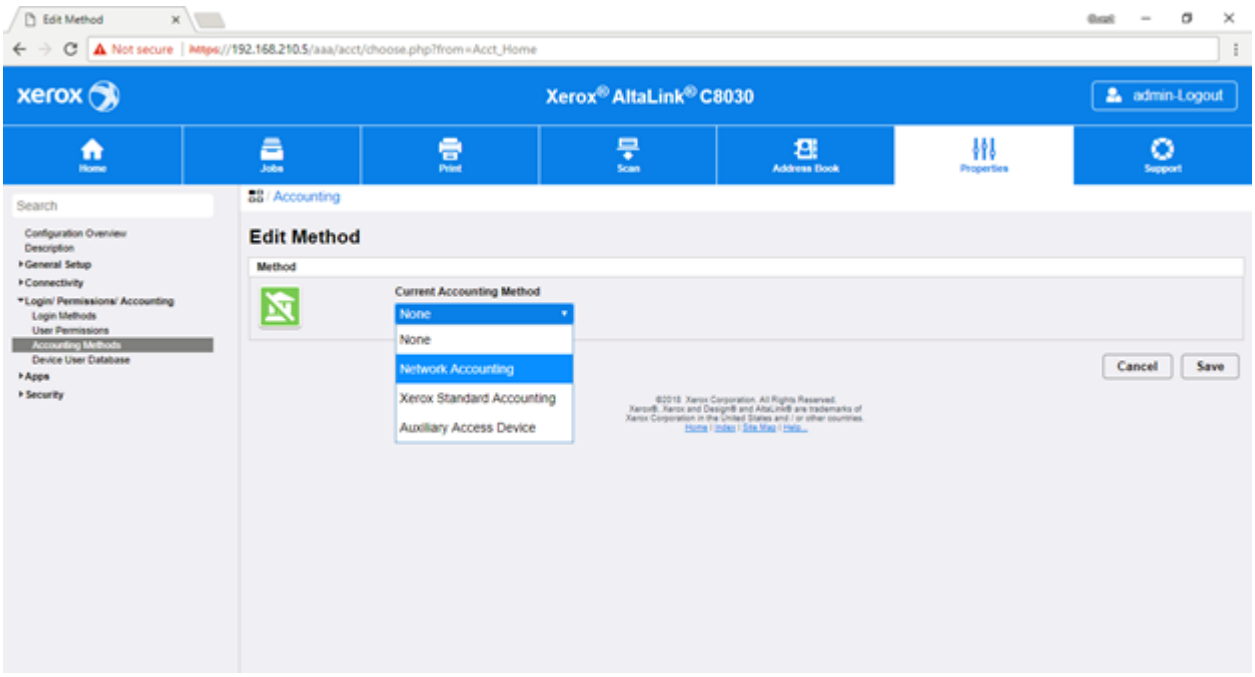
- In the Server Communication section select "IPv4 Address" radio button.

- Enter the "IP Address: Port". The IP will be the location of the Xerox Embedded hosted installation. Enter 443 for the port number as the authentication server uses SSL.
- Enter "/PAXeroxAuthentication/Server.asmx" as the Path.
- Uncheck the "Embedded" check box, as this might disable some proxy cards.
- From the "Device Log In Methods" section select "Xerox Secure Access Device Only (e.g., Swipe Cards)".
- Under the "Accounting Information (Requires Network Accounting)" section select " Automatically apply Accounting Codes from the server".

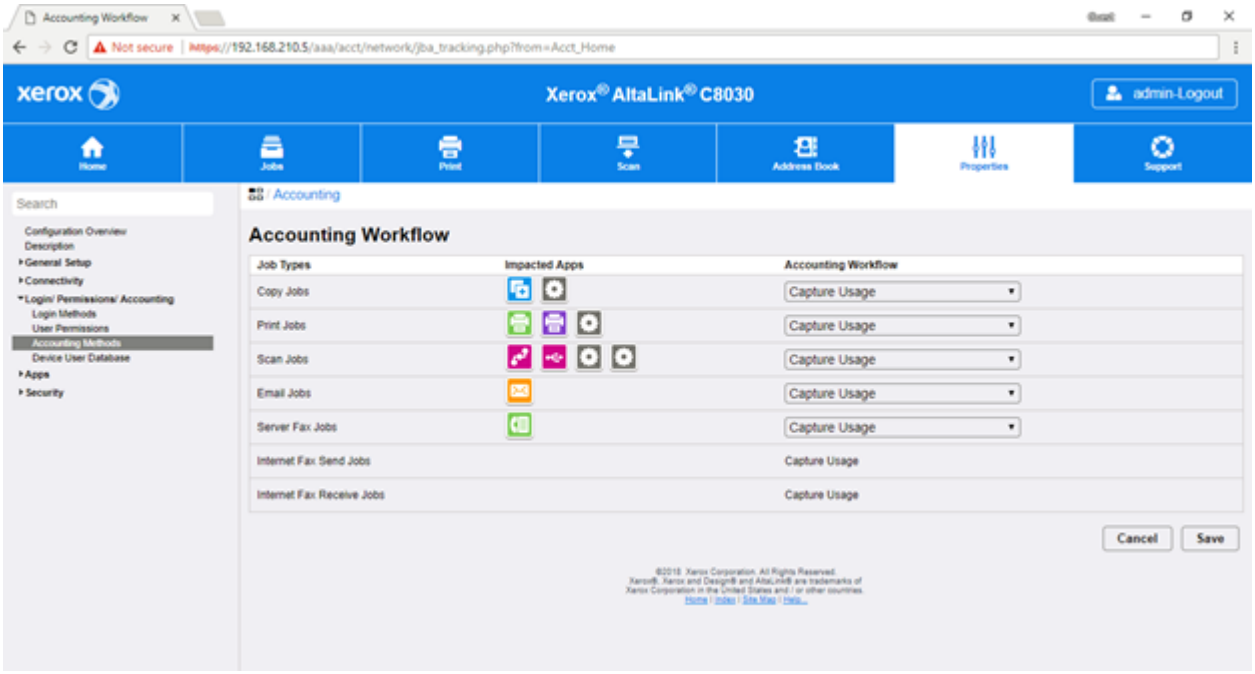
9. Click "Save" to continue. Navigate to "Login / Permissions / Accounting" and then "Accounting Methods". Click Edit next to Touch and Web User Interface.



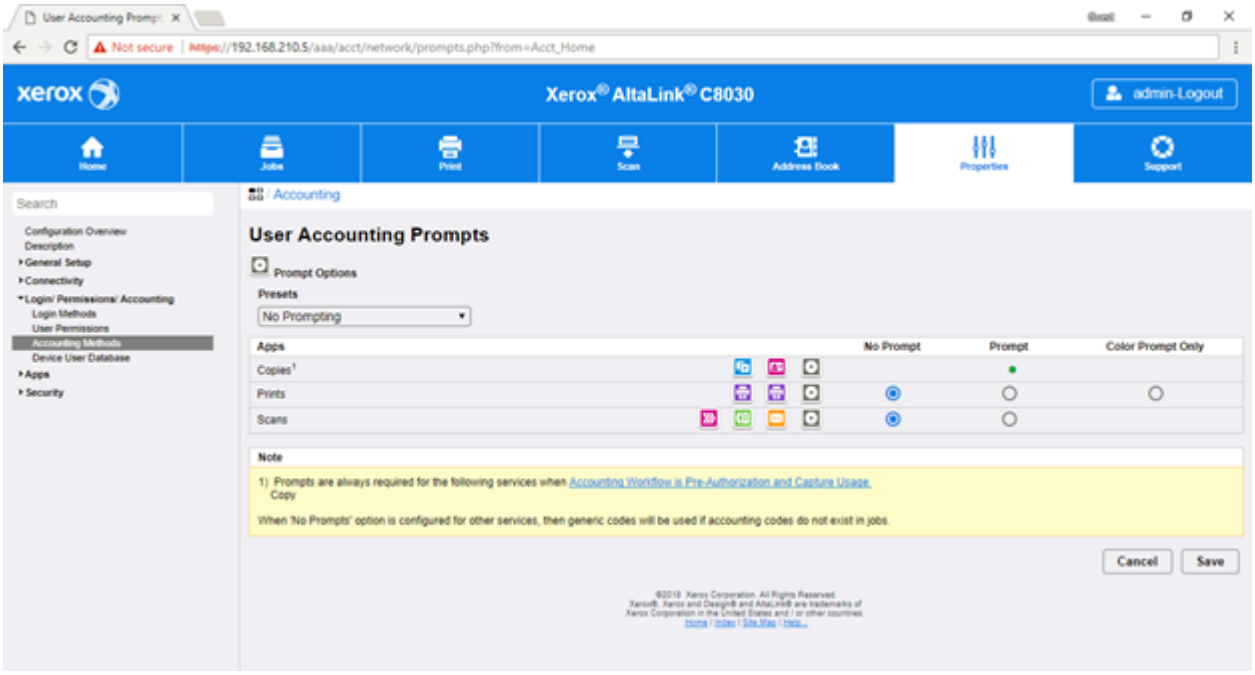
10. Set the Accounting Method to “Network Accounting”. Click on ‘Save’ to return to previous screen. (Select Accounting Methods)



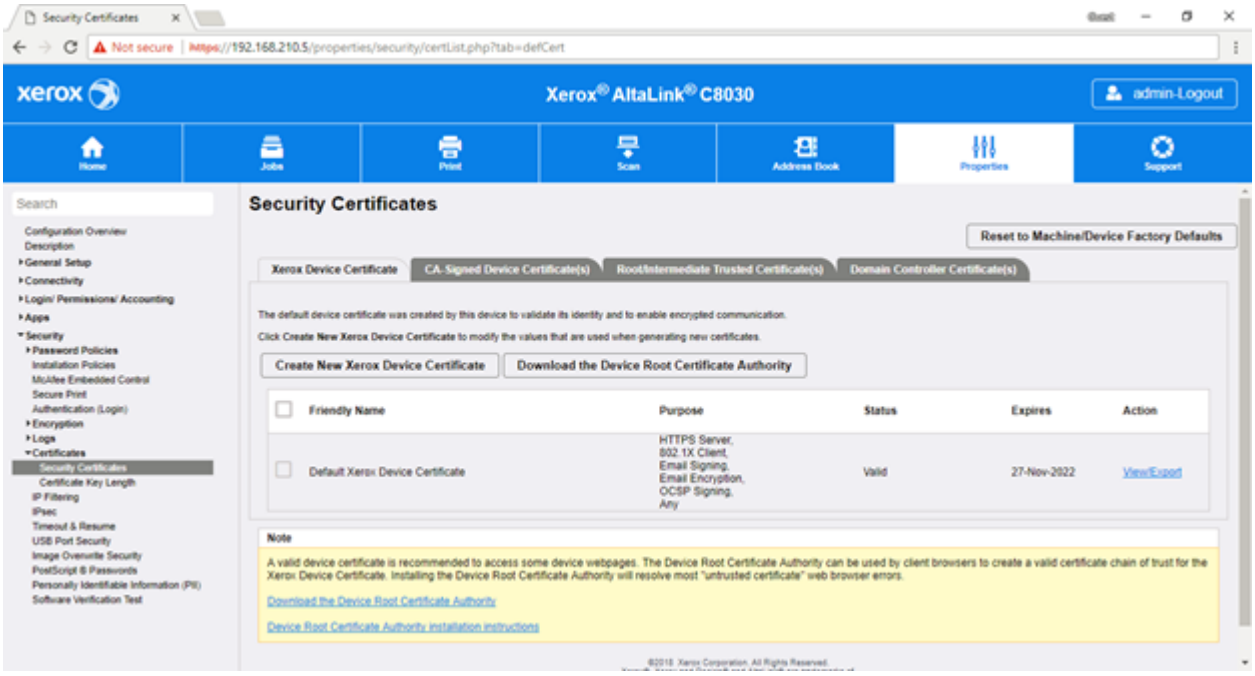
11. Click Edit next to the ‘Accounting Workflow’. All Job Types must be set to ‘Capture Usage’. Click Save.



12. Click Edit next to the ‘User Accounting Prompts’. Select ‘No Prompting’ from the Presets dropdown. Click Save.



13. Navigate to "Properties" from the top menu and select "Security" then "Certificates " and " Security Certificates" section on the left hand side menu.



14. Ensure that there is a certificate installed on the Xerox device. If there is no certificate listed, please create a new Xerox device certificate

Configuring Print Audit Embedded for Xerox for use with a Card Reader

In order for authentication via Swipe/Prox card reader to work, the Print Audit Embedded for Xerox application must be configured to point to the IP address of the IIS server that the Embedded Xerox application is installed on. To configure this value:

1. Open the ...\Print Audit Embedded for Xerox\Main\AppSettings.config file for editing. This can be done by running Notepad as Administrator or copying the file to the desktop, editing it and then copying it back.
2. For the parameter "<add key="ServerIpAddress" value="IPADDRESS"/> , change the value to the IP Address of the IIS server that Print Audit Embedded for Xerox is installed on.
3. In IIS, restart the Application Pool "PAXEAuthAppPool" for the change to take effect.

2b. Versalink Configuration

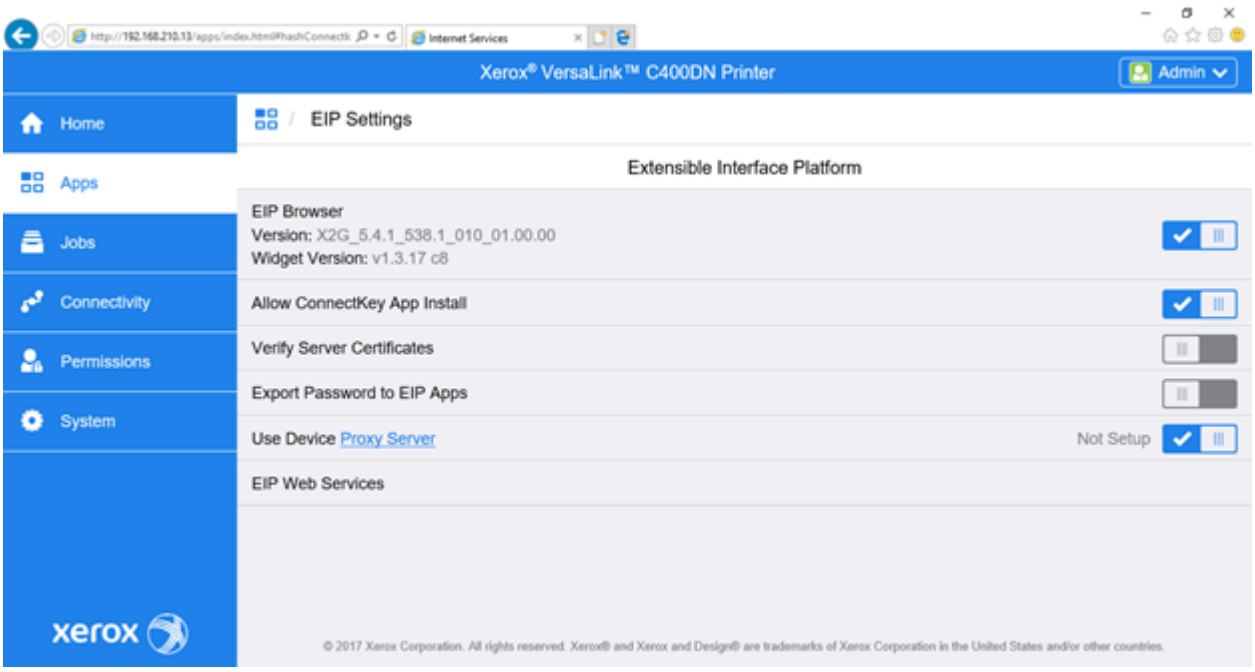
Configuring the Panel Interface

Please Note: These instructions are modeled after the XEROX Versalink C400DN and may be slightly different depending on the device in question.

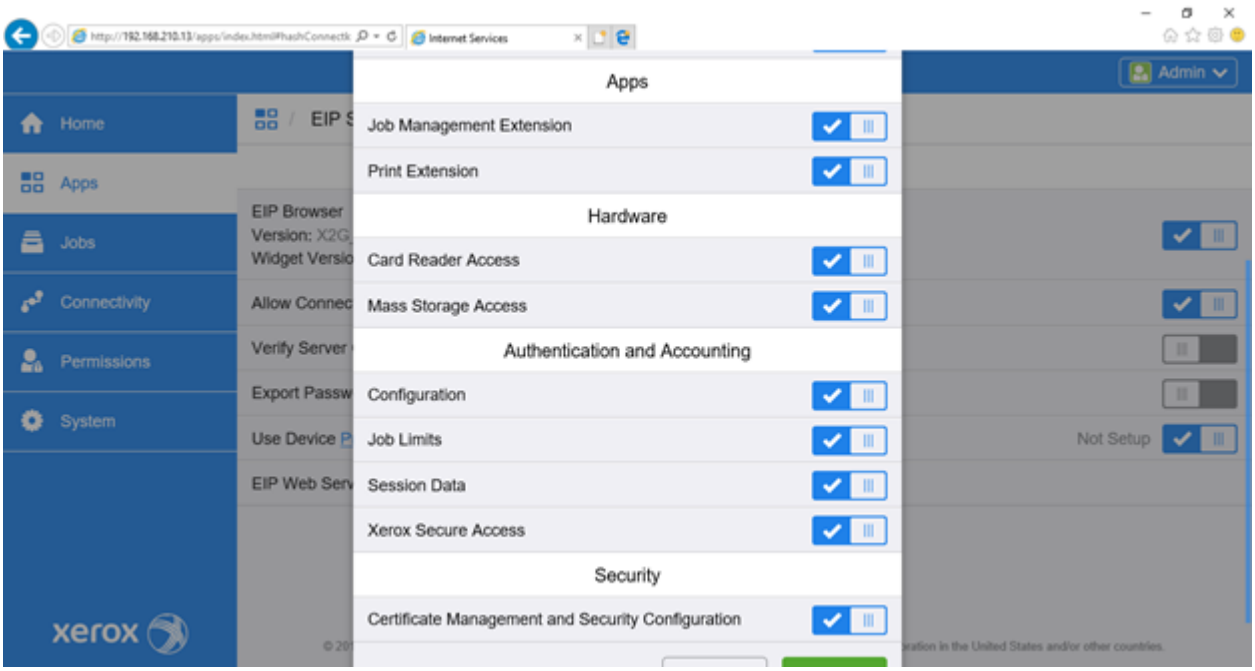
Enabling EIP Applications

1. Select "Apps" from the side menu. click on "EIP Settings"

- Ensure "Allow ConnectKey App" Install is enabled
- Set the "Verify Server Certificates" is set to disabled



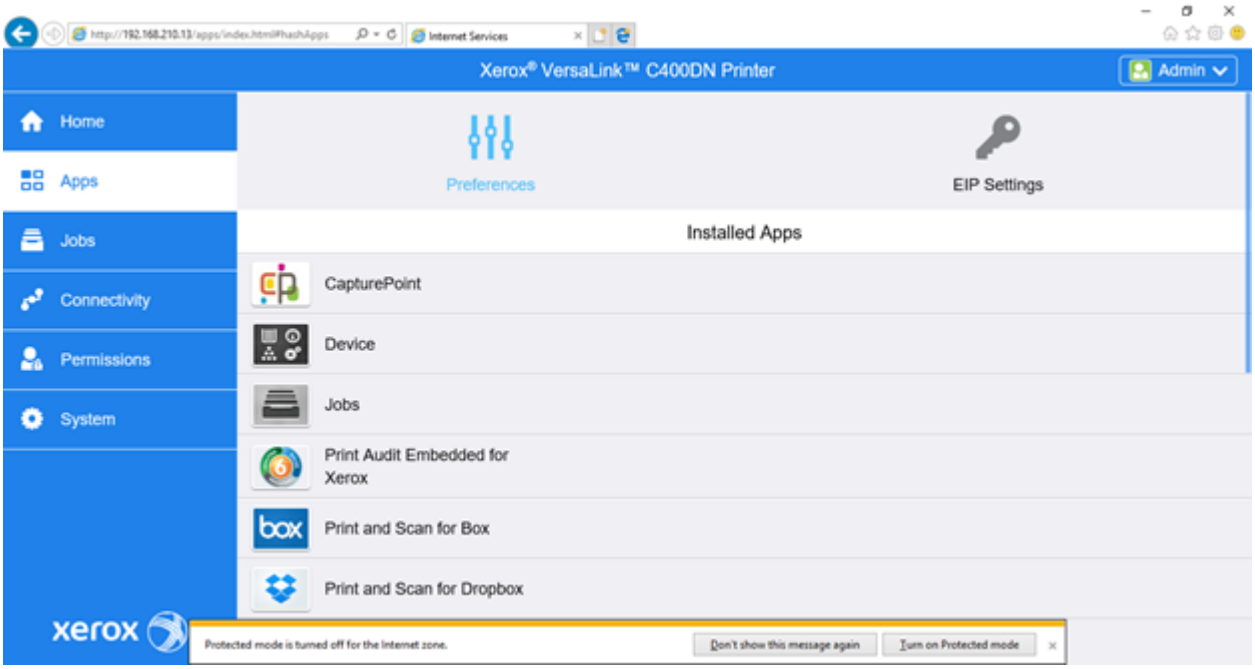
2. Click on "EIP Web Services". Under "Authentication and Accounting" ensure "Xerox Secure Access" is enabled



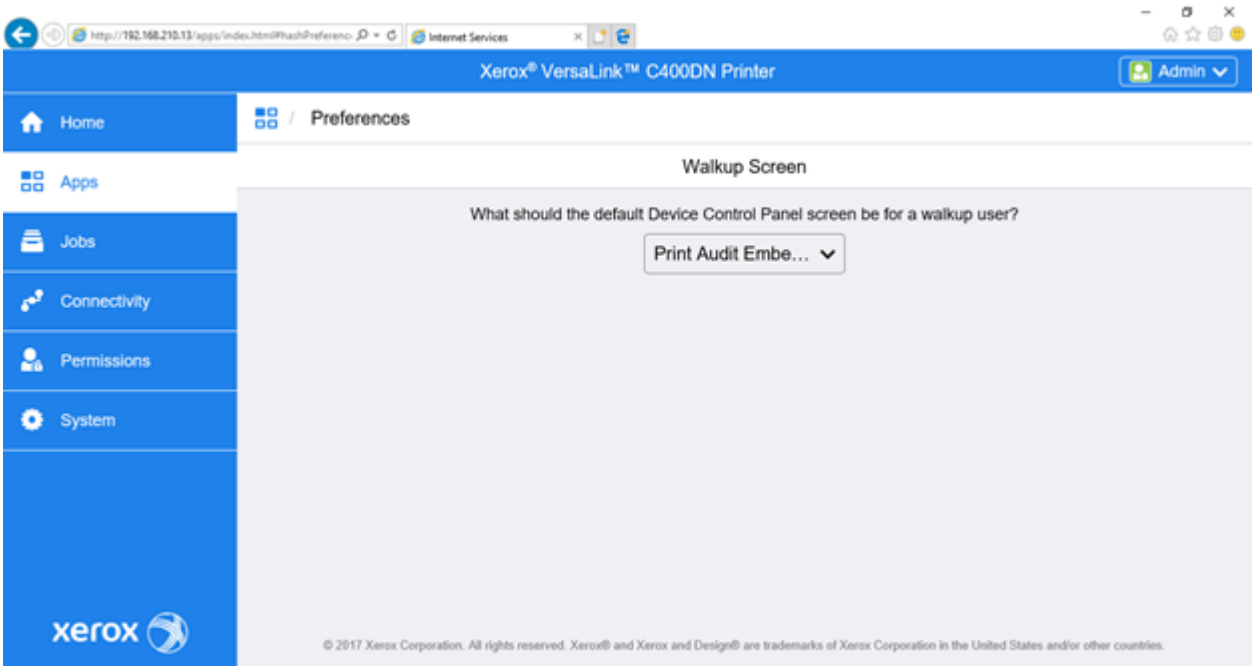
Configuring Default Walkup Screen

1. Navigate to "Apps" from the side menu, then click “Preferences” on the top menu

(Note: You may be prompted to enter admin credential)

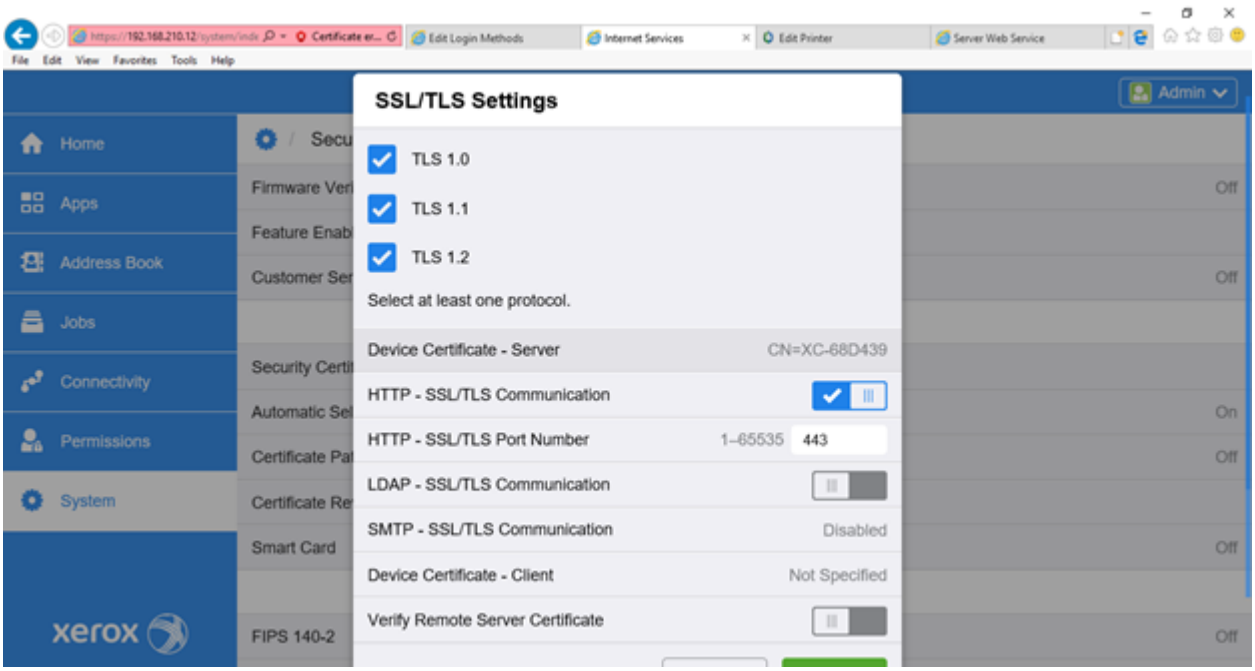


2. Under the "Walkup Screen" section select "Print Audit Embedded for Xerox" from the dropdown

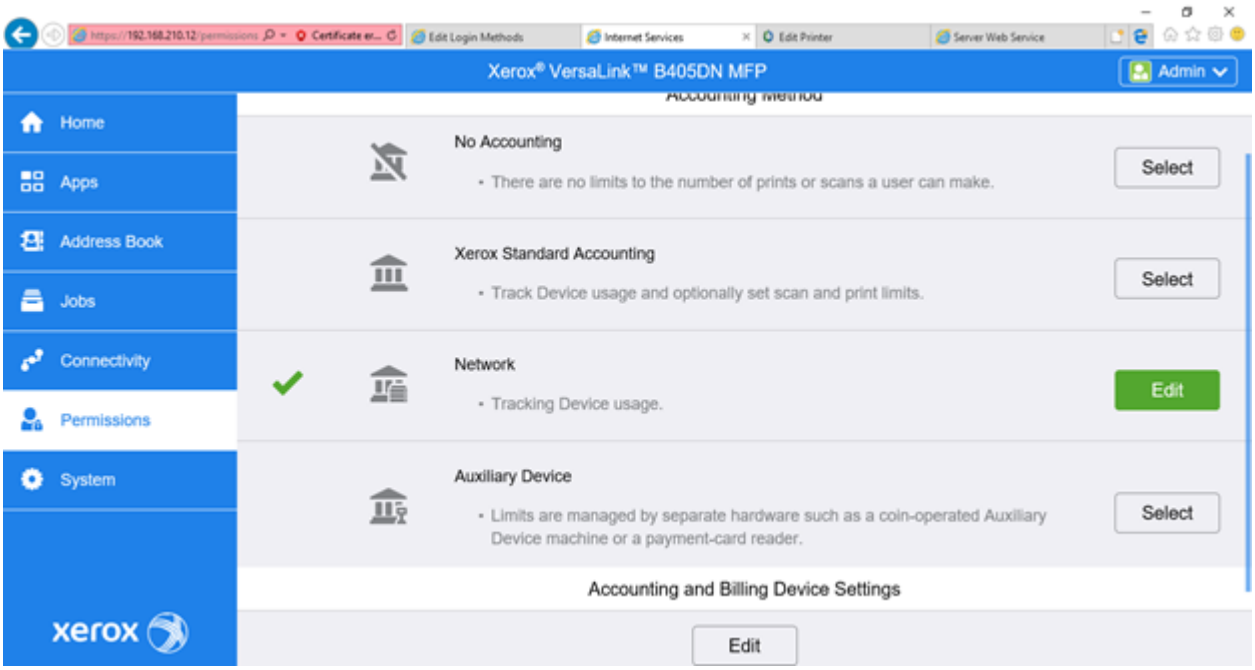


3. Click on System from the left Menu. Under the Security Section click on "SSL/TLS Settings".

- Ensure the appropriate TLS protocols are enabled
- Set the "HTTP - SSL/TLS Communication" to enabled
- Verify the "HTTP - SSL/TLS Port Number" is set to 443

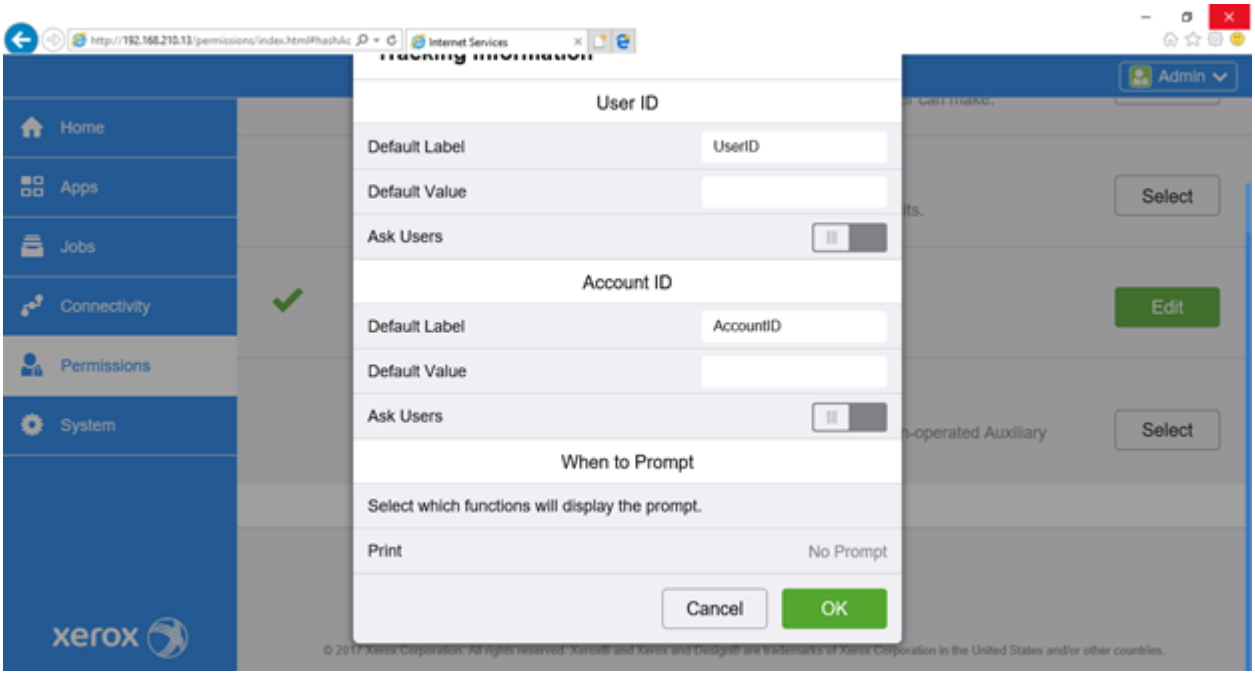


4. Click on Permissions from the left Menu. Select "Accounting Method" and click Edit next to " Network"

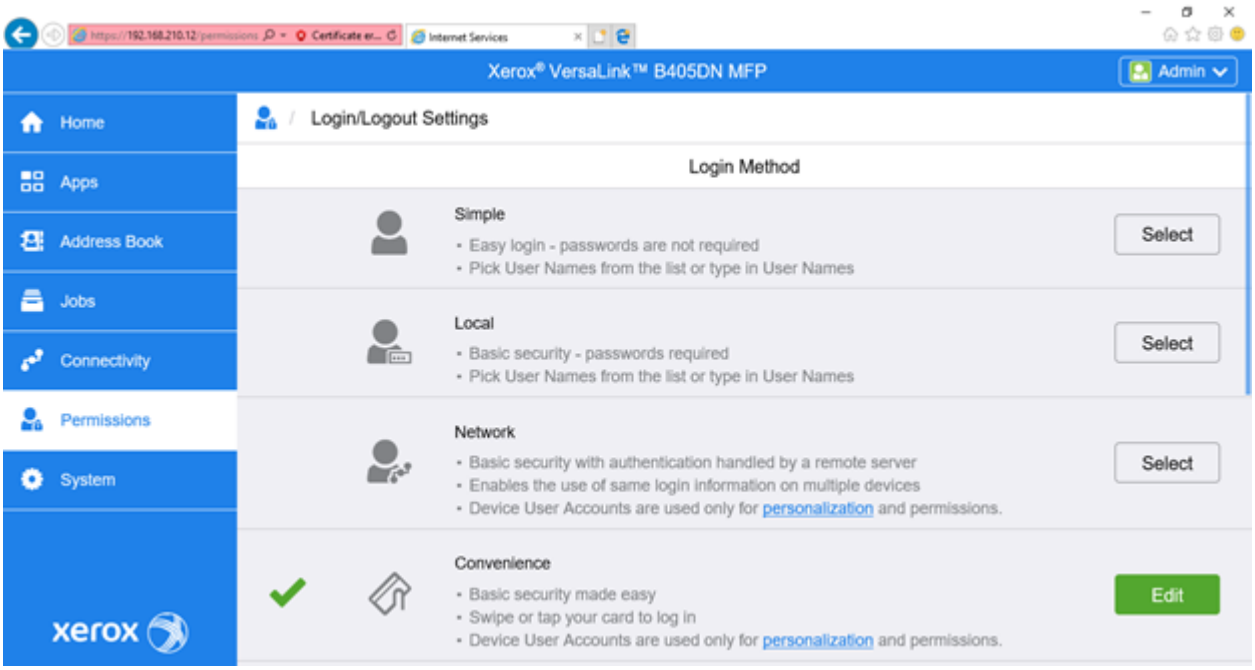


5. Under the "Tracking Information" Section Click Edit

- Under the "User ID" section ensure the "As Users" Setting is disabled
- Under the "Account ID" section ensure the "As Users" Setting is disabled
- Under "When to Prompt" section ensure all functions are set to "No Prompt"



6. Select "Permissions" from the left Menu. Click on the "Login/Logout Settings".



7. Click Edit next to the "Convinence" Login Method

- Configure the IP Address and Port of the system hosting the Xerox Embedded software
- Configure the Path as /PAXeroxAuthentication/Server.asmx
- Set the "Alternate Login" Setting to "Yes"
- Set the "Accounting Codes" section to "Get codes automatically from server

3. Using Xerox Embedded with Print Audit 6

The Embedded for Xerox Client is very easy to use. It will first prompt for required identification or billing information, before enabling the device for copy, scan, fax, or print functionality. Once the desired function is complete, return to the panel and complete the session, otherwise the MFP will timeout the session. When the session ends, the copy, scan, fax, or print transaction is sent to the Print Audit 6 database, and the Embedded Client resets to be ready for the next user.

Printing from the document server

When a print job is generated through Print Audit 6 it is automatically tracked in the Print Audit 6 database. Additionally, if a print job is released from the document server, it is tracked in the Print Audit 6 database. Therefore, jobs that are printed through Print Audit 6 and then released from the document server, are tracked twice in the Print Audit 6 database.

To ensure accurate print tracking with secure release capabilities, it is recommended to use only Print Audit Secure for secure document release functionality.

The standard set of steps to using Embedded for Xerox to track job information is as follows:

1. **Start the Transaction -** Press the Start button on the screen. The Embedded Client retrieves its configuration and proceeds to prompt for the required information. The Cancel button can be used at any time to return to the Start screen.
2. **Authenticate -** If configured to ask for a PIN Code, the Embedded Client displays a login screen. To login:
    a. Press the PIN Code button. An input form displays.
    b. Enter a PIN Code using the MFP's keyboard or touch screen.
    c. Press the OK button to accept the input.
    d. Press the OK button on the Login screen to validate the PIN Code.
3. **Enter Custom Field Information -** If configured to ask for Custom Field information, the Embedded Client will prompt for on or more values from the user. To enter values for a searchable field:
    a. Press the button on the touch screen that corresponds to the Custom Field Name.
    b. Enter a full or partial code on the screen and click OK.
    c. If only one match is found for the field, the Embedded Client asks for the next Custom Field value if any is configured.
    d. If Print Audit finds more than one match, a list of values will display. Use the touch screen to navigate through the values.
    e. When the desired value is found, press the button corresponding to the value. It appears highlighted.
    f. Press the OK button to accept the value.
    g. Press the OK button again to move to the next screen.
4. **To enter values for a non-searchable field:**
    a. Press the button that corresponds to the desired value. It appears highlighted.
    b. Use the arrows on the touch screen to navigate through the choices.
    c. Press the OK button to accept the value. The Embedded Client will request the next Custom Field value if any is configured.
5. **Enter any Comments -** If configured, the Embedded Client will request any Comments for the job. Press OK if to proceed without entering comments. To enter comments:
    a. Press the Comments button on the touch screen. An input form appears.
    b. Use the input form to enter comments.
    c. Press the OK button to close the input form.

d. Press the OK button on the Comments screen to accept the comments.

6. **Verify Selections -** After all information has been input, a summary screen appears showing the current balance if any, along with the custom values selected. Press the OK button to accept the selections and begin the job.

Account balance restrictions

If declining balances are enabled for the current user each copy/fax/scan operation will debit the account balance in real-time. Once the balance of the current user reaches zero all MFP copy/fax/scan functions will be locked for that user until such time that the user logs in again with a positive balance.

4. Using Xerox Embedded with Print Audit Secure

The Print Audit Secure Embedded for Xerox Client is very easy to use. It will first prompt for required information. The prompts which appear are dependent on how the Secure Embedded Client is configured. Once the prompted information is provided, the device will release the secure job(s). Then the Secure Embedded Client resets to be ready for the next user. If the session is not manually finished, the Xerox MFP will timeout.

Following, are the standard set of steps to using Secure Embedded for Xerox to release a print job.

1. Authenticate

1. **PIN Code authentication -** If configured to request a PIN Code, the Secure Embedded Client displays a login screen. To login:
   a. Click on the Pin Code Field
   b. Enter a PIN Code using the Sharp keyboard or the touch screen.
   c. Press the Login button to accept the input.
2. **Authenticate with a Username -** If configured to ask for a Username, the Secure Embedded Client displays a login screen. To login:
   a. Click on the Username Field
   b. Enter a Username
   c. Click on the Password Field
   d. Enter a Password
   e. Press the Login button to accept the input.

3. **Authenticate with a swipe card -** If configured to ask for a swipe card, the Secure Embedded Client displays a login screen. To login:
    a. Swipe a card in a card reader attached to the MFP.

2. Release Print Jobs

1. To release all the compatible print jobs, click the Release All button.
2. To release only certain jobs, press the checkbox next to the jobs to be released.
3. Click the Release button. The selected job(s) will now print.

3. Delete Print Jobs

To delete print jobs, press the checkbox next to the jobs to be remove and press the Delete button.

4. Complete the Job

When finished releasing print jobs, press the Logout button on the Xerox MFP screen. This will notify Print Audit Secure that the transaction is complete. If this step is not completed, the MFP will eventually reset back to the Start screen.

5. Troubleshooting - Embedded for Xerox

Please refer to this section if issues are encountered with the operation of Embedded for Xerox. If a resolution is not found in this section, please contact Print Audit technical support.

Error: Communication Problem - Unknown problem with the authentication system was detected. Unable to login.

This could indicate that the ASP.NET application pool in the IIS configuration is set to the wrong version. PA Xerox Authentication server requires the .NET 2.0 runtime to be configured in IIS.

Verify IIS is using a correct application pool.

1. Open the Windows Internet Information Services interface.
2. Click Application Pools and verify PAXEAuthAppPool has been installed and set to v2.0
3. Expand the website where PAXeroxAuthentication is installed.
4. Click on the PAXeroxAuthentication website and go to the Advanced Settings
5. Ensure the Application Pool in the General section is set to PAXEAuthAppPool.
6. If not, change it to reflect this Application Pool.
7. Click the Ok button.

Verify the self signed certificate has been installed and bound to the correct website.

1. Open the Windows Internet Information Services interface.
2. Click on the IIS server.
3. Click Server Certificates icon within the IIS section.
4. Ensure the XeroxAuthenticatioCeritifcate has been installed.
5. Click on the website where PAXeroxAuthentication is installed.
6. Click Bindings under the Actions section on the right hand menu
7. When the Site Bindings page is presented ensure the https type with Port 443 is visible.

Error: Unable to connect to Database Communicator

This error occurs if the MFP cannot connect to the Database Communicator. Please check the following:

1. The Database Communicator is running.
2. The correct host name and port are set for the Database Communicator. To change the host and port, edit the Embedded.config file installed with the Xerox Embedded for PA6 package.

Error: Print Audit License is not Valid

If for some reason the Xerox MFP cannot validate the Print Audit license, or if there are not enough Embedded for Xerox licenses for the MFPs, this error displays. Please contact Print Audit or an authorized dealer to purchase or update the Print Audit license.

Error: Unable to save file: C:\\Windows\Downloaded Installations\PrintAudit 6 Embedded – Xerox.msi
Access is denied

The installer must be executed with administrator privileges. Right-click PA6Xerox6xxR.exe and select 'Run as Administrator'. Enter username & password if necessary.

6. IIS Configuration/Setup for Print Audit Embedded for Xerox

Please Note: The Print Audit Embedded for Xerox Setup Wizard is designed to configure most settings in IIS when it is run. However, depending the environment, it may be necessary to verify or modify those settings. The examples presented in this guide are based on the default installation options. Please contact your System Administrator for additional details should changes to these defaults be required in your environment.

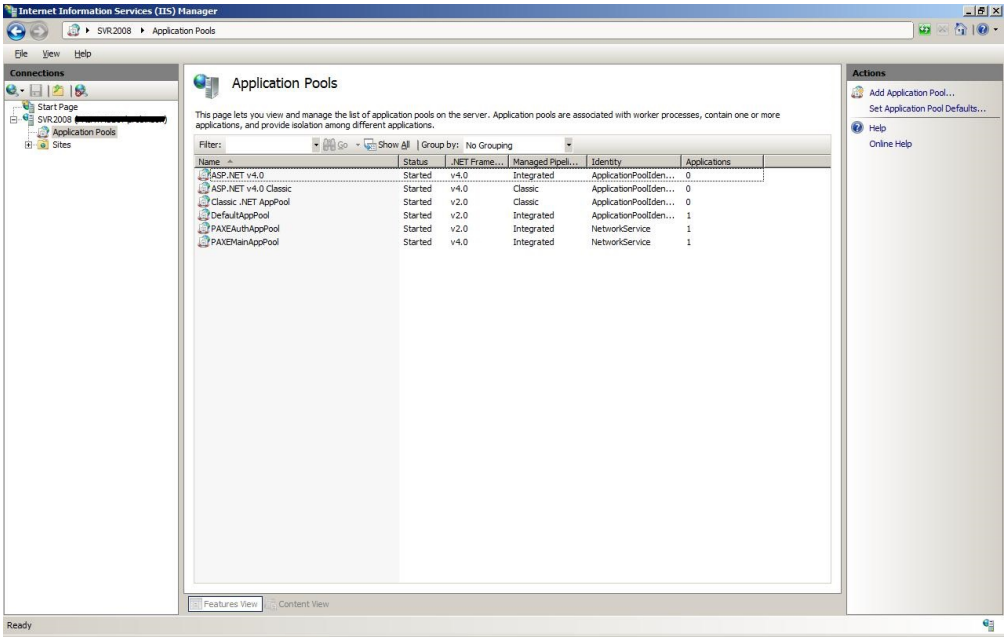
Verifying Application Pools

Application Pools in IIS allow different ASP.NET applications running on the web server to be isolated from each other. Errors in one application pool will not affect other applications running in other application pools. Print Audit Embedded for Xerox installs two separate application pools:

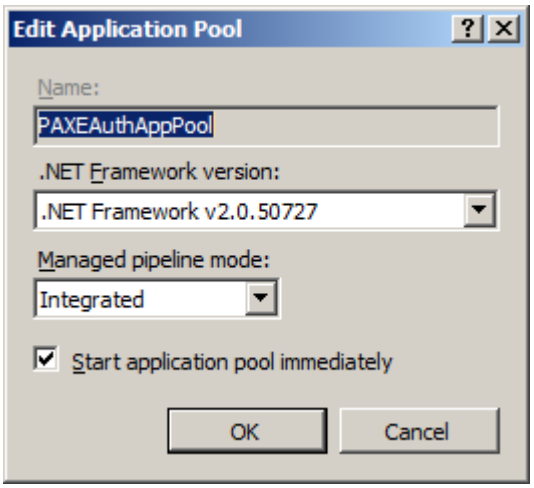
- PAXEAuthAppPool - runs under .NET Framework v2.0.50727
- PAXEMainAppPool - runs under .NET Framework v4.0.30319

To verify the .NET Framework version for the application pool:

1. Open the Internet Information Services (IIS) Manager.



2. Under the IIS server name, select "Application Pools".
3. Double click on the Application Pool Name.



4. Use the dropdown ".NET Framework version" to select the appropriate version.

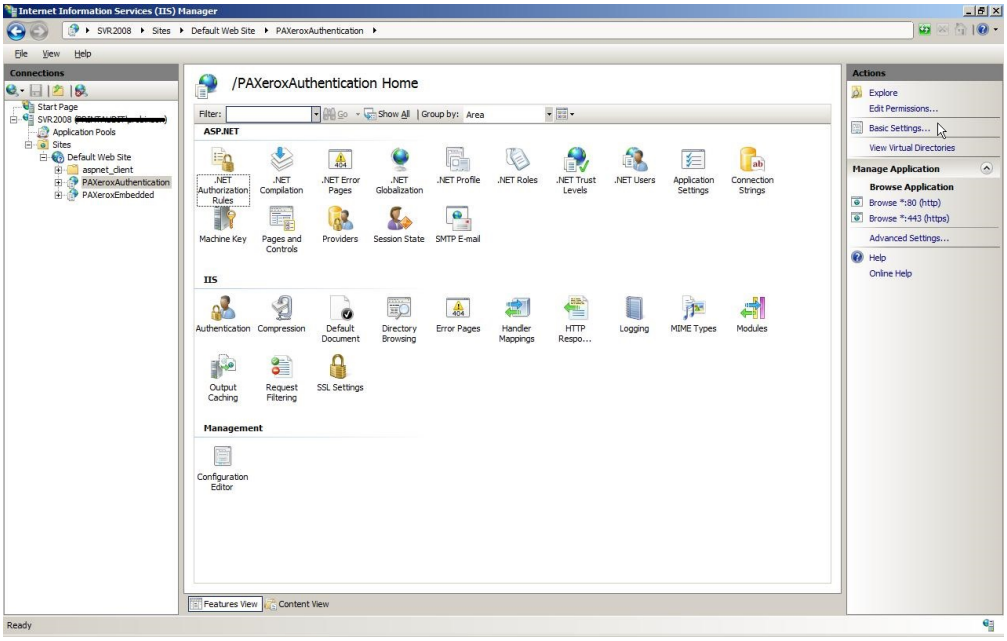
Verifying Application Pools used by Print Audit Embedded for Xerox sites

The Print Audit Embedded for Xerox creates two web sites under "Default Web Site" by default:

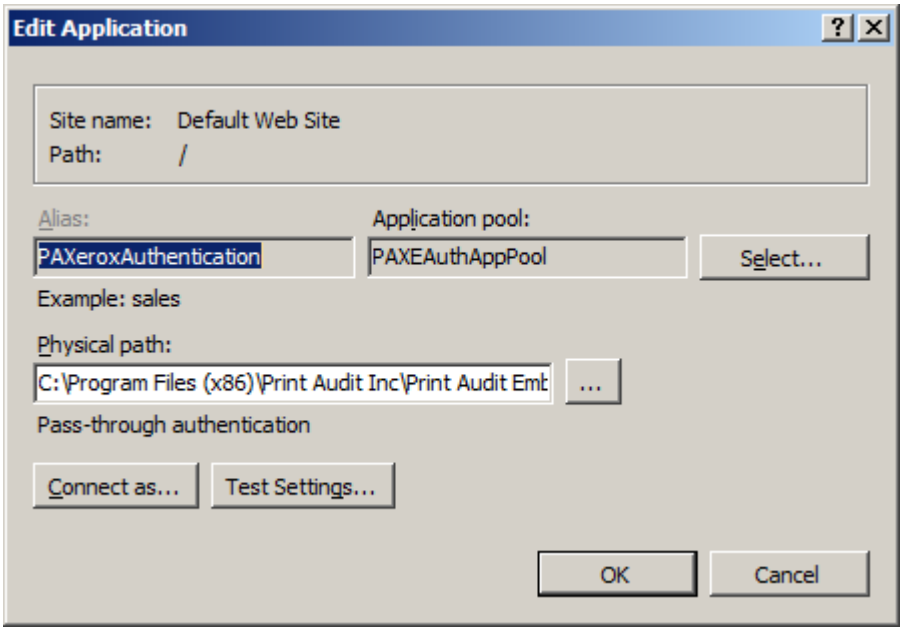
- PAXeroxAuthentication - uses the PAXEAuthAppPool application pool.
- PAXeroxEmbedded - uses the PAXEMainAppPool application pool.

To verify the Application pool used by a site:

1. Open the Internet Information Services (IIS) Manager.



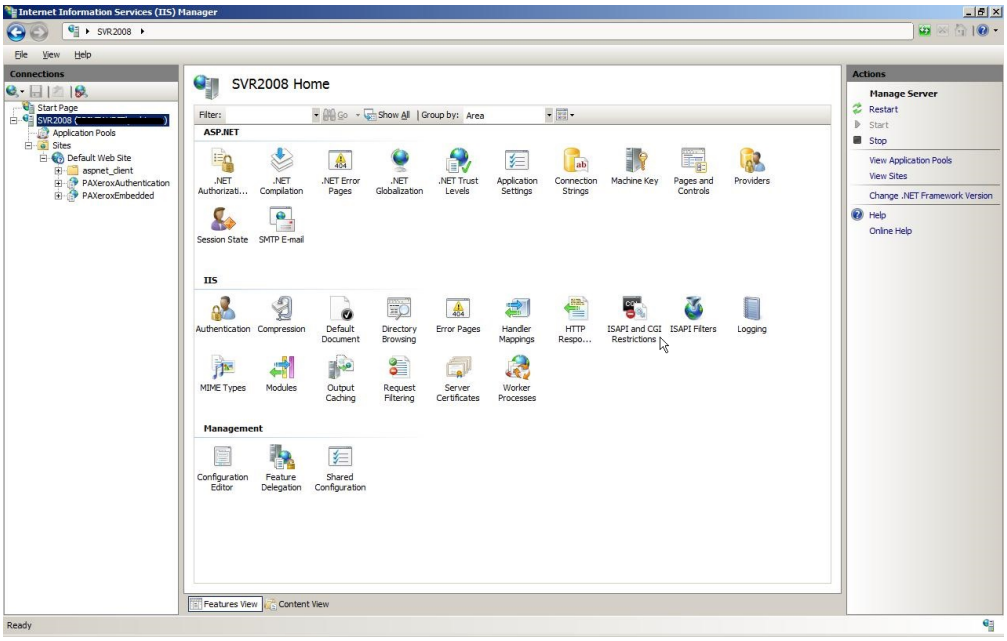
2. Locate the web site under "Sites" and highlight it. By default, the Print Audit Embedded for Xerox sites are under "Default Web Site".
3. Under "Actions" (located on the right hand side of the IIS Manager), click on "Basic Settings... "



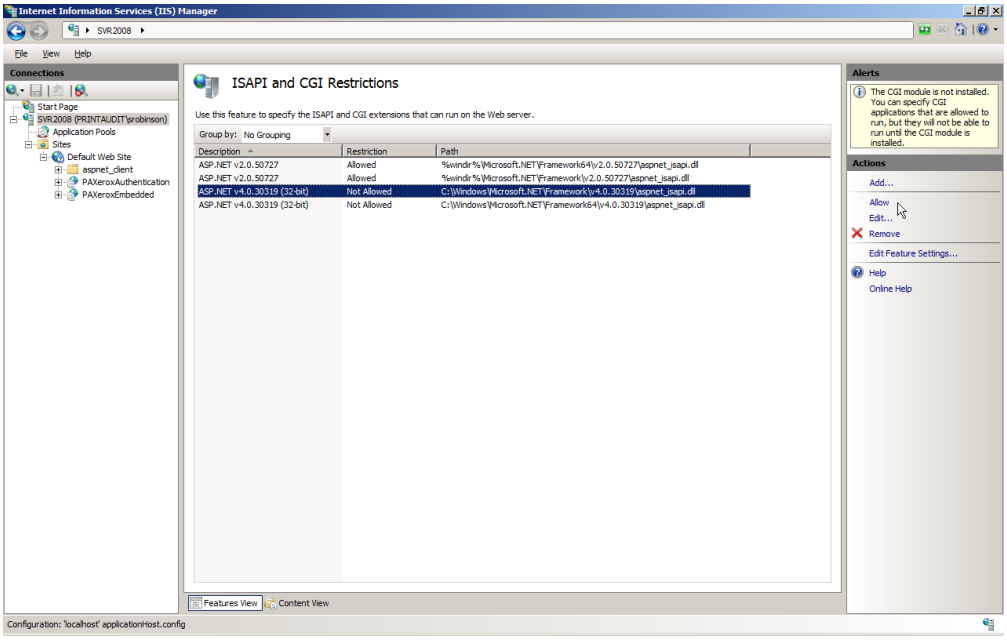
Verifying ASP.NET Restriction

The Print Audit Embedded for Xerox requires .NET Framework version 2 and version 4. The .NET Framework versions may need to be enabled to work with IIS.

1. Open the Internet Information Services (IIS) Manager.



2. Click on the icon "ISAPI and CGI Restrictions"



3. Highlight the .NET versions that are set to "Not Allowed" and click on the "Allow" link under " Actions".