Print Audit Embedded for Kyocera:

Installation and Setup Guide

Version: 19
Date: 21-Apr-2014 17:52

Table of Contents

Table of Contents

Components 4

1. Print Audit 6 - Embedded for Kyocera Configuration: 5

2. Embedded Client: 5

Print Audit 6 5

Print Audit Secure 6

Authentication Devices 7

Licensing 8

Limitations 9

1. Installation 11

Before you Install 12

Steps to install 12

Kyocera Embedded Application Installation to MFP 12

Configuring the Kyocera Embedded Application 14

Authentication Types 16

Using the Embedded for Kyocera Client 16

Detailed Panel Walkthrough 16

"None" Type of Authentication 16

PIN or Card Reader Authentication 16

Custom Fields 17

Comments 17

Declining Balances 17

2. Configuration 18

Pre-configuration checklist **19**

Overview **19**

Adding, Editing and Deleting Copiers in Print Audit 6 . . . . . **19**

Configuring the Kyocera MFP in Print Audit 6 . . . . . **22**
General 22
Pricing tab 23
Restrictions tab (only with Print Audit 6 Rules) 25
Prompts tab (only with Print Audit 6 Recovery) 25
Limits tab (only with Print Audit 6 Rules) 26
Advanced tab 26
Edit Configuration 27
Communicator Settings 28

3. Using Card Readers 29

Configuring Card IDs in the Print Audit Administrator **30**

4. Using Embedded for Kyocera with Print Audit 6 30

5. Using Embedded for Kyocera with Print Audit Secure 32

1. Authenticate **33**

2. Release Print Jobs **33**

3. Delete Print Jobs **34**

4. Refresh Job List **34**

5. Complete the Job **34**

6. Troubleshooting 34

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 6.8.1 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.

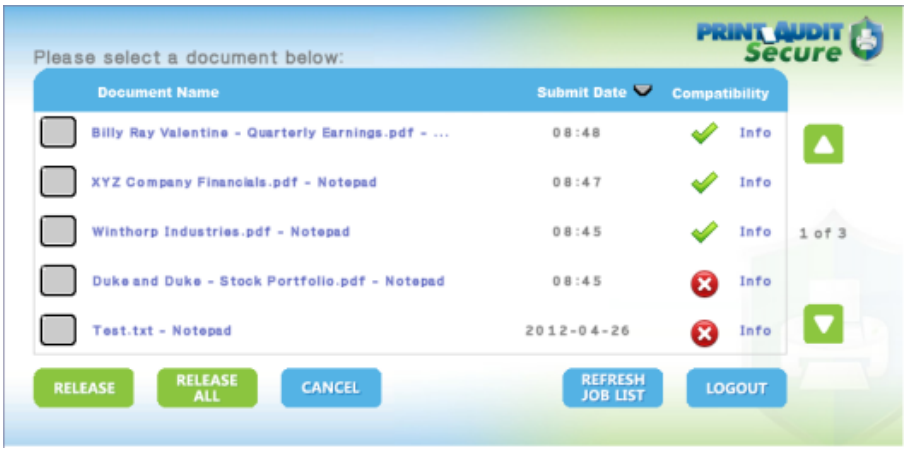
Print Audit 6

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 an 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

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 they are reached. User-based configuration of account limits behavior are also not possible. Print Audit Embedded controls page-type limits of a user, but that limit is controlled cannot be fine-grained to an individual limit. How all limits are treated is controlled via a system setting - Warn, Stop, or Ignore.
4. **Cancel Job:** The cancel job command is not available.
5. **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

Before you Install

- Print Audit Embedded for Kyocera will run on Kyocera HYPAS MFPs which support the HyPAS API version 2.0, with a 8.5" screen.
- 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. Download the Kyocera Embedded Application from the Print Audit web site
4. Download and install the Kyocera NetViewer – instructions below
5. Create the record for the MFP in the Print Audit Administrator Embedded section
6. Install the Embedded Application using NetViewer and configure
7. Verify operation and tracking of the MFP

Kyocera Embedded Application Installation to MFP

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

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

Deployment via Kyocera Net Viewer

1. You will need to download the latest version of Kyocera NetViewer from the Kyocera website.
2. 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
3. Run the NetViewer application

1. if this is the first time it is run, choose the location for your Workspace

2. Add Devices Wizard
    - Select Express or Custom to begin search for devices on the network

    a. 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
3. When device discovery has completed, you will be taken to the General view and your device(s) will be shown
4. Right click on the Kyocera device you wish to install to
5. Select 'Communication Settings'
6. 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'
7. Select 'OK' to close Communication Settings window
8. Right click on the Kyocera device again and select "Advanced"
9. select "Manage Applications"
10. select "Install application"
11. check the box for "Activate application after installation" and click "Next"
12. use the Browse button to go to the location where the Kyocera Embedded Application was saved
13. select the "PAE_Kyocera_Embedded_x.x.x.pkg" file and click Open
14. 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
15. 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
16. click on "Close" and you will be taken back to the main NetViewer window
17. 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 user name 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 Configuration 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 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

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

Device Configuration

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 - edit the configuration settings to be sent to the device.

Communicator Settings

1. Enable PA Communicator - enable communication on the Kyocera device with the Print Audit Database Communicator
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

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

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

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 Print Audit PIN.

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

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.

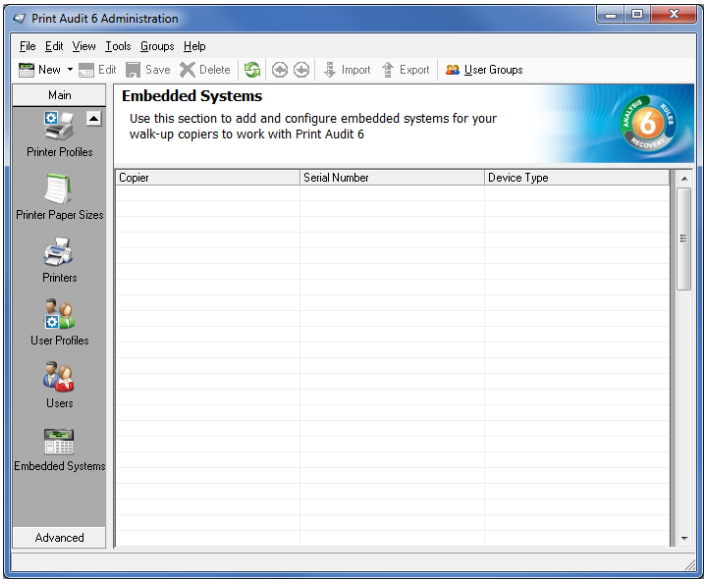
Overview

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

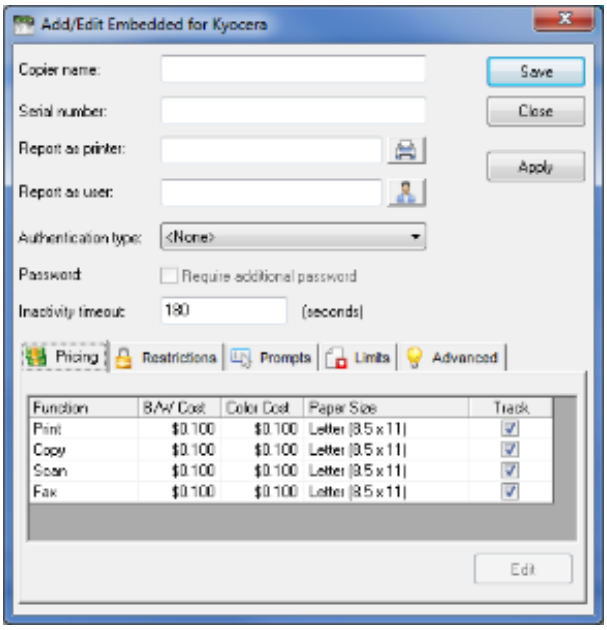
Use the Embedded Systems section of the Administration tool to add, edit and delete Embedded for Kyocera copiers. A copier in the Administration tool represents a physical copier in the network.



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.

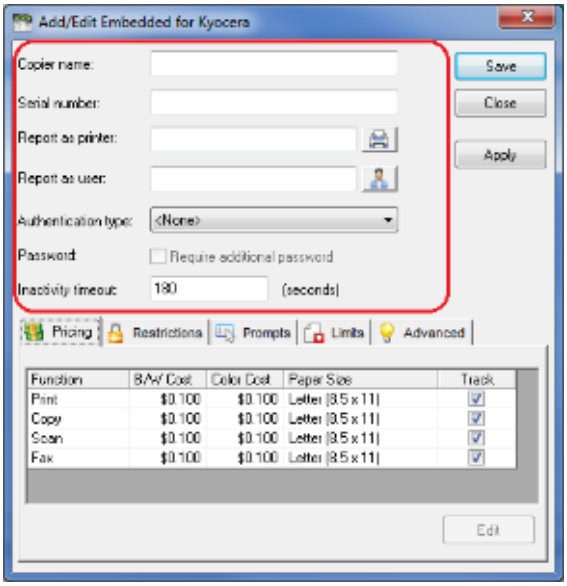
To delete a copier:

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.

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:

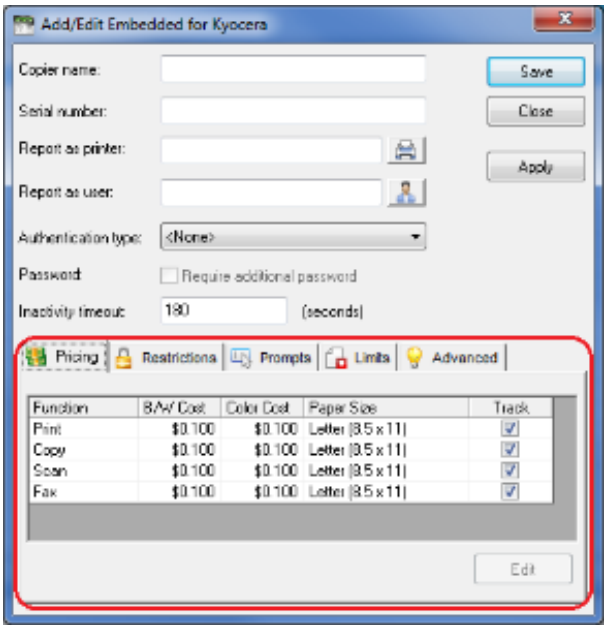
- None - Users do not have to authenticate before using the copier. All transactions are recorded to the generic Kyocera_Embedded user.
- PIN code - Users must enter their Print Audit PIN to access the copier.

- 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.

NOTE: Check the 'Require additional password' box on the Embedded for Kyocera 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.

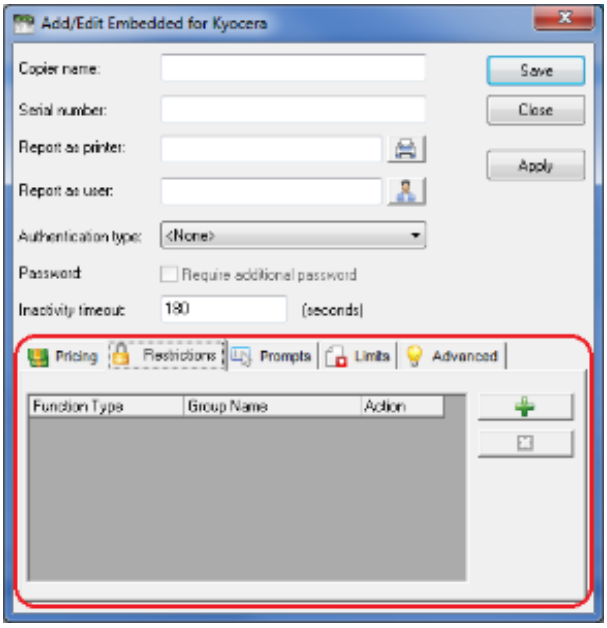
Pricing tab



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.


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

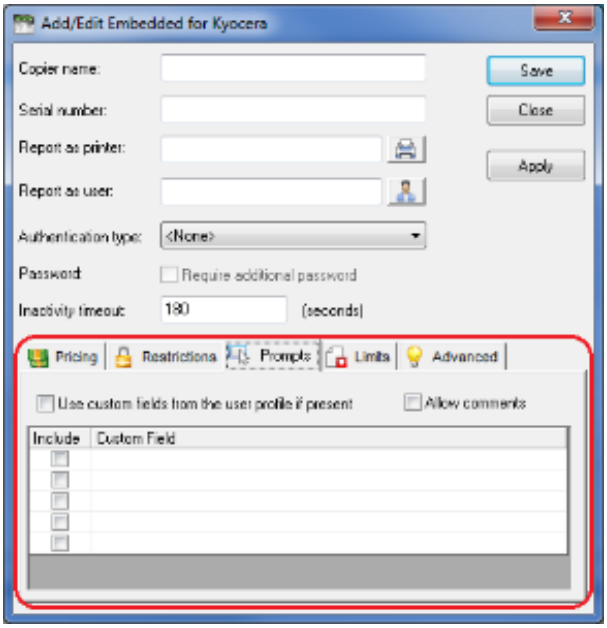
Restrictions tab (only with Print Audit 6 Rules)

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.

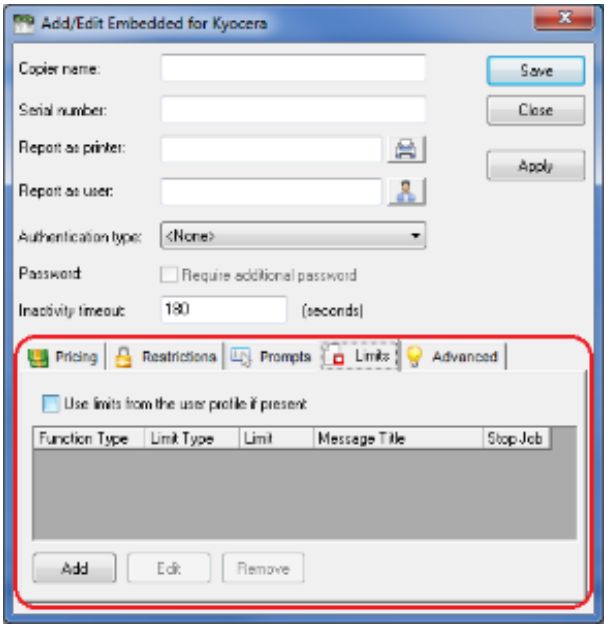
Prompts tab (only with Print Audit 6 Recovery)



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.

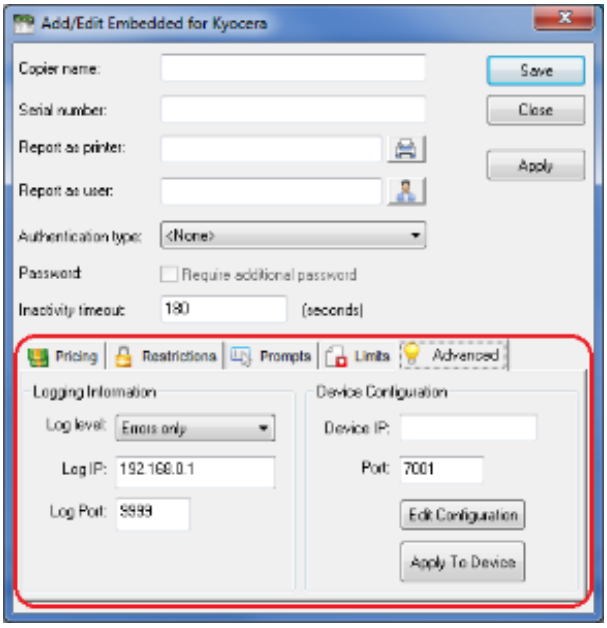
Use limits from the user profile - Check this to use limits defined in a user's profile instead of the limits defined here.

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

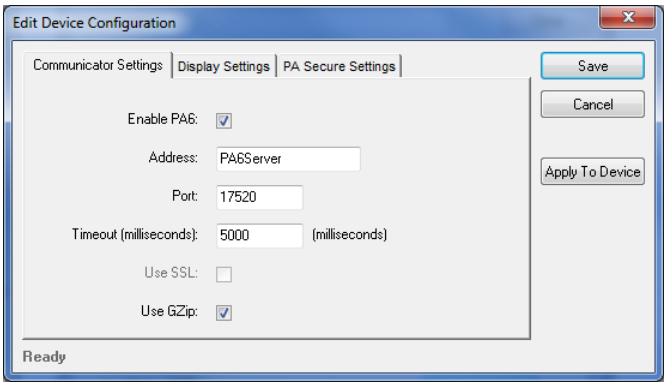
Use this feature to remotely configure a device for use with Print Audit 6 and Print Audit Secure.

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

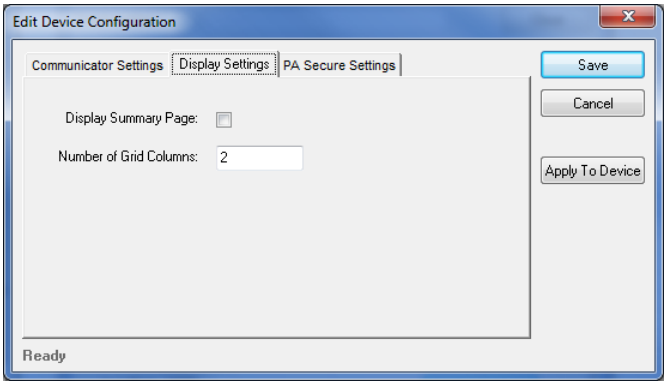


Enable PA6 - Check this box to enable device to use Print Audit 6

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.

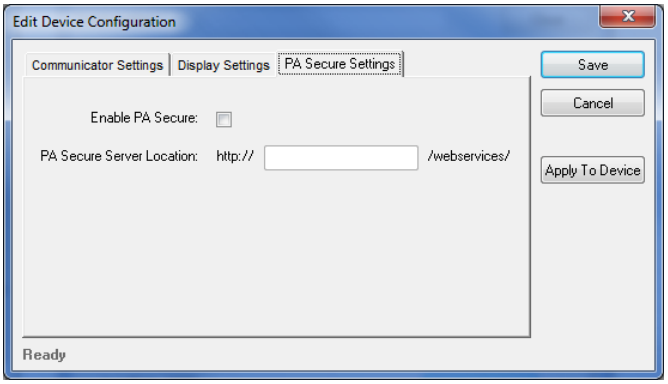


Display Settings

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 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

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. Susan Scurry Explain the negative balance situation better.

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

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

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 Kycoera 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 properly formatted, the Kyocera may emit a warning beep or display an error "The removable memory is not formatted - Cannot recognize the removable memory".