Print Audit 6 Print Audit Embedded for Print Audit 6

Version: 2 Date: 03-Dec-2018 17:21

Table of Contents

Browse Documents:
Browse Other Product Documentation: 11
Embedded for HP Documentation 11
Browse Documents:
Browse Other Product Documentation: 12
Embedded for HP-Install and Setup 12
Components
1. Print Audit 6 - Embedded for HP Configuration:
2. Embedded Client:
Print Audit 6
Print Audit Secure
Authentication Devices
Licensing
Limitations
1. Installation - Embedded for HP
System Requirements
Optional
Before you Install
Steps to Install
Installing the Print Audit Embedded for HP installation package on the server
Deploying the Print Audit Embedded for HP application to MFPs
Using the Print Audit Embedded for HP client 25
Detailed Panel Walkthrough
"None" Type of Authentication 26
PIN or Card Reader Authentication 26
Custom Fields
Comments
2. Configuration - Embedded for HP 27
Pre-configuration checklist
Overview
Adding, Editing and Deleting Copiers in Print Audit 6 28
Configuring the HP MFP in Print Audit 6 29
Pricing tab

Promots tab (only with Print Audit 6 Recovery)	31
Advanced tab	33
3 Using HP Embedded with Print Audit 6	33
4 Using Embedded for HP with Print Audit Secure	35
1 Authenticate	35
2 Release Print Jobs	36
3. Delete Print Jobs	36
3. Refresh Job List	36
4. Complete the Job	36
5. Troubleshooting - Embedded for HP	36
6. IIS Configuration/Setup for Print Audit Embedded for HP	38
Verifying Application Pools	39
Verifying Application Pools used by Print Audit Embedded for HP sites	40
Verifying ASP.NET Restriction	41
Embedded for Konica Minolta Documentation	41
Browse Documents:	42
Browse Other Product Documentation:	42
Embedded for Konica Minolta Install and Setup	42
Components	43
1. Print Audit 6 - Embedded for Konica Minolta Configuration:	43
2. Embedded Client:	43
Print Audit 6	43
Print Audit Secure	44
Authentication Devices	44
Supported Card Readers	44
	44
1. Installation - Embedded for Konica Minolta	45
System Requirements	45
Device Requirements	46
Optional	46
Before you Install	46
Steps to Install	46
Installation Walkthrough	47
Configuring the Konica Minolta device using the Web Interface*	47
	52
Installing the Print Audit Embedded for Konica Minolta installation package on the server	52
Deploying the Print Audit Embedded for Konica Minolta application to MFPs.	59
2. Configuration - Embedded for Konica Minolta	62
Pre-configuration checklist	62

Overview	62
Adding, Editing and Deleting Copiers in Print Audit 6	63
Configuring the Konica Minolta MFP in Print Audit 6	64
Pricing tab	66
	67
•••••••••••••••••••••••••••••••••••••••	67
	67
	67
Prompts tab (only with Print Audit 6 Recovery)	67
Advanced tab	67
3. Using Embedded for Konica Minolta with Print Audit 6	68
4. Using Embedded for Konica Minolta with Print Audit Secure	69
1. Authenticate	70
2. Release Print Jobs	70
3. Delete Print Jobs	70
3. Refresh Job List	71
4. Complete the Job	71
5. Troubleshooting Print Audit Embedded for Konica Minolta	71
6. IIS Configuration/Setup for Print Audit Embedded for Konica Minolta	71
Installing IIS Components for Print Audit Embedded for Konica Minolta	72
Server 2008/IIS 7	72
Windows 2012/IIS8 and up	72
	73
Verifying Application Pools	73
Verifying Application Pools used by Print Audit Embedded for Konica Minolta sites	74
Verifying ASP.NET Restriction	75
Embedded for Kyocera Documentation	76
Browse Documents:	77
Browse Other Product Documentation:	77
Embedded for Kyocera Installation and Setup Guide	77
	78
1 Print Audit 6 - Embedded for Kyocera Configuration:	78
2 Embedded Client:	78
Print Audit 6	78
	70
	70
	79
	79
Limitations	80
1. Installation - Embedded for Kyocera	82
System Requirements	82

	Before you Install	82
	Steps to install	82
	Deploying the Print Audit Embedded for Kyocera application Installation to MFP	82
	Configuring the Kyocera Embedded Application	84
	Authentication Types	88
	Using the Embedded for Kyocera Client	88
	Detailed Panel Walkthrough	89
	"None" Type of Authentication	89
	PIN or Card Reader Authentication	89
	Custom Fields	89
	Comments	89
	Declining Balances	90
2.	Configuration - Embedded for Kyocera	91
	Pre-configuration checklist	91
	Overview	91
	Adding, Editing and Deleting Copiers in Print Audit 6	91
	Configuring the Kyocera MFP in Print Audit 6	94
	General	94
	Pricing tab	95
	Restrictions tab (only with Print Audit 6 Rules)	97
	Prompts tab (only with Print Audit 6 Recovery)	97
	Limits tab (only with Print Audit 6 Rules)	98
	Advanced tab	98
	Edit Configuration	99
	Communicator Settings	100
3.	Using Card Readers - Embedded for Kyocera	102
	Configuring Card IDs in the Print Audit Administrator	102
4.	Using Embedded for Kyocera with Print Audit 6	103
5.	Using Embedded for Kyocera with Print Audit Secure	105
	1. Authenticate	105
	2. Release Print Jobs	105
	3. Delete Print Jobs	106
	4. Refresh Job List	106
	5. Complete the Job	106
6.	Troubleshooting - Embedded for Kyocera	107

Embedded for Lexmark Documentation	108
Browse Documents:	109
Browse Other Product Documentation:	109
Embedded for Lexmark-Install and Setup	109
Components	110
1. Print Audit 6 - Embedded for Lexmark Configuration:	. 110

2. Embedded Client:		110
Print Audit 6		110
Print Audit Secure		111
Authentication Devices		111
		111
		112
1 Installation - Lexmark		112
Refore you Install		112
System Requirements		113
Pre-Installation Steps		113
Steps to install		113
Install the Embedded Solution to MEP		113
Create the Security Template		116
Set the Access Controls		121
Configure the Print Audit and Print Audit Secure Settings		124
Communicator Settings		124
Secure Server Settings		125
2 Configuration - Embedded for Lexmark		125
Pre-configuration checklist		125
Overview		125
Adding Editing and Deleting Copiers in Print Audit 6		126
Configuring the Lexmark MEP in Print Audit 6		127
General		128
Pricing tab		129
Restrictions tab (only with Print Audit 6 Rules)		130
P romots tab (only with Print Audit 6 Recovery)		131
· · · · · · · · · · · · · · · · · · ·		131
		131
Limits tab (only with Print Audit 6 Rules)		132
Advanced tab		133
		133
		133
		133
		133
Edit Configuration		134
Communicator Settings		134
PA Secure Settings		134
Repeat the above steps for each Lexmark MFP on which Embedded for Lex	mark will be)
used.		135
3. Using Lexmark Embedded with Print Audit 6		135
4. Using Lexmark Embedded with Print Audit Secure		137
1. Authenticate		137
2. Release Print Jobs		137
3. Delete Print Jobs		137

4. Complete the Job	
5. Troubleshooting - Embedded for Lexmark	

Embedded For Sharp Documentation 13	;9
Browse Documents:	10
Browse Other Product Documentation:	10
Embedded for Sharp-Install and Setup 14	10
Components	11
1. Print Audit 6 - Embedded for Sharp Configuration:	41
2. Embedded Client:	41
Print Audit 6	11
Print Audit Secure	12
Authentication Devices	12
Licensing	12
1. Installation	13
System Requirements	43
Optional	44
Installation Walkthrough	44
2. Configuration	18
Pre-configuration checklist	48
Overview	49
Configuring the Sharp MFP in Print Audit 6 15	50
General	51
Pricing tab	52
Restrictions tab (only with Print Audit 6 Rules) 15	52
Prompts tab (only with Print Audit 6 Recovery) 15	53
Advanced tab	53
Extended Configuration Settings 15	54
5. Configuring Sharp MFPs with the Embedded Client for Sharp	55
3. Using Sharp Embedded with Print Audit 6	56
4. Using Sharp Embedded with Print Audit Secure	58
1. Authenticate	58
2. Release Print Jobs	58
3. Delete Print Jobs	58
4. Complete the Job	<u>9</u> פנ
5. I roubleshooting	»9
6. IIS Configuration/Setup for Print Audit Embedded for Sharp	30
Installing .NET version 4	30
IIS 6 (Server 2008) 16 IIO 7 and bit loss (One on 2010 and bit loss) 16	50 20
IIS / or higher (Server 2012 and higher)	50 24
Instailing no components	21

Allowing the ASP.NET Version 4 Extension	162
Creating Application Pools in IIS for Print Audit Embedded	163

Browse Documents: 165 Browse Other Product Documentation: 165 Embedded for Xerox Installation and Setup Guide 165 Components 166 1. Print Audit 6 - Embedded for Xerox Configuration: 166 2. Embedded Client: 166 Print Audit 6 166 Print Audit 6 167 Authentication Devices 167 Licensing 167 Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 176 Notes on Print Audit Embedded for Xerox 176 Pre-configuration Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox MFP 176 Overview 176 Overview 176 Overview 178 General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended c	Embedded for Xerox Documentation
Browse Other Product Documentation: 165 Embedded for Xerox Installation and Setup Guide 165 Components 166 1. Print Audit 6 - Embedded for Xerox Configuration: 166 2. Embedded Client: 166 Print Audit 6 166 Print Audit 6 166 Print Audit Secure 167 Licensing 167 Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 P rompts tab (only with Print Audit 6 Recovery)	Browse Documents:
Embedded for Xerox Installation and Setup Guide 165 Components 166 1. Print Audit 6 - Embedded for Xerox Configuration: 166 2. Embedded Client: 166 Print Audit 6 166 Print Audit 6 166 Print Audit 8 166 Print Audit Secure 167 Authentication Devices 167 Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuration checklist 177 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit Ewbedded for Xerox Certificate 199 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring Print Audit Embedded fo	Browse Other Product Documentation:
Components 166 1. Print Audit 6 - Embedded for Xerox Configuration: 166 2. Embedded Client: 166 Print Audit 6 166 Print Audit 6 166 Print Audit Secure 167 Authentication Devices 167 Licensing 167 Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox 176 Overview 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit & with the Xerox MFP 178 General 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 P configuring Print Audit Embedded for Xerox for use with a Card Reader <td< td=""><td>Embedded for Xerox Installation and Setup Guide</td></td<>	Embedded for Xerox Installation and Setup Guide
1. Print Audit 6 - Embedded for Xerox Configuration: 166 2. Embedded Client: 166 Print Audit 6 166 Print Audit Secure 167 Authentication Devices 167 Licensing 167 Linstallation - Embedded for Xerox 167 Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox 176 Pre-configuration Embedded for Xerox 176 Overview 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 177 Adding, Editing and Deleting Copiers in Print Audit 6 178 General 178 Pricing tab 179 P roting tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring Print Audit Embedded for Xerox Cortificate 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Attalink Configuration </td <td>Components</td>	Components
2. Embedded Client: 166 Print Audit 6 166 Print Audit Secure 167 Authentication Devices 167 Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 177 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring Print Audit Embedded for Xerox Certificate 198 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2. Altalink Configuration 199 2. Altalink Configuration 205 2. Using Xerox Embedded with Print Audit 6	1. Print Audit 6 - Embedded for Xerox Configuration:
Print Audit 6 166 Print Audit Secure 167 Authentication Devices 167 Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 177 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Attalink Configuration 199 2a. Attalink Configuration 199 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 5 205 4. Using Xerox Emb	2. Embedded Client:
Print Audit Secure 167 Authentication Devices 167 Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 179 Pricing tab 179 Priompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing/Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Attalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink	Print Audit 6
Authentication Devices 167 Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 177 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing/Verifying the Print Audit Embedded for Xerox Certificate 199 2a. Altalink Configuration 199 2b. Versalink Configuration 205 3b. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 201	Print Audit Secure
Licensing 167 Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 1779 Pricing tab 179 Princing tab 179 Princing tab 179 Pring tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing/Verifying the Print Audit Embedded for Xerox Certificate 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 2b. Versalink Configuration 205 2b. Versalink Configuration 205	Authentication Devices
Limitations 168 1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 177 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing/Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211 1 Authenticate 211 <td>Licensing</td>	Licensing
1. Installation - Embedded for Xerox 169 Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing/Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altaling Verifying the Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211 1. Authenticate 211	Limitations
Before you Install 169 System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing/Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	1. Installation - Embedded for Xerox 169
System Requirements 169 Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 177 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit Secure 211 1. Authenticate 211	Before you Install
Installation Walkthrough 170 Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	System Requirements
Notes on Print Audit Embedded for Xerox Logging 175 2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox Certificate 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211 1. Authenticate 211	Installation Walkthrough
2. Configuration Embedded for Xerox 176 Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing/Verifying the Print Audit Embedded for Xerox Certificate 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211 1. Authenticate 211	Notes on Print Audit Embedded for Xerox Logging 175
Pre-configuration checklist 176 Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	2. Configuration Embedded for Xerox 176
Overview 176 Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing/Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Pre-configuration checklist 176
Adding, Editing and Deleting Copiers in Print Audit 6 176 Configuring Print Audit 6 with the Xerox MFP 178 General 179 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Overview
Configuring Print Audit 6 with the Xerox MFP 178 General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Adding, Editing and Deleting Copiers in Print Audit 6 176
General 178 Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Configuring Print Audit 6 with the Xerox MFP 178
Pricing tab 179 P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	General
P rompts tab (only with Print Audit 6 Recovery) 180 Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Pricing tab
Extended configuration settings 181 Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	P rompts tab (only with Print Audit 6 Recovery) 180
Configuring the Xerox MFPs with the Embedded Client for Xerox 183 Installing\Verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Extended configuration settings
Installing/verifying the Print Audit Embedded for Xerox Certificate 196 Configuring Print Audit Embedded for Xerox for use with a Card Reader 199 2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Configuring the Xerox MEPs with the Embedded Client for Xerox
2a. Altalink Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Installing/Verifying the Print Audit Embedded for Xerox Certificate
2a. Attaining Configuration 199 Configuring Print Audit Embedded for Xerox for use with a Card Reader 205 2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211 1. Authenticate 211	Configuring Print Audit Embedded for Xerox for use with a Card Reader
2b. Versalink Configuration 205 3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211	Za. Altallink Configuration
3. Using Xerox Embedded with Print Audit 6 209 4. Using Xerox Embedded with Print Audit Secure 211 1. Authenticate 211	205 2b Versalink Configuration
4. Using Xerox Embedded with Print Audit Secure	3 Using Xerox Embedded with Print Audit 6
1. Authenticate 211	4 Using Xerox Embedded with Print Audit Secure 211
	4. Osing Acros Embedded with Finit Addit Secure
2 Release Print Jobs 212	2 Release Print Johs 211
3 Delete Print Jobs	3 Delete Print Jobs
4. Complete the Job	4. Complete the Job

5.	Troubleshooting - Embedded for Xerox	212
6.	IIS Configuration/Setup for Print Audit Embedded for Xerox	213
	Verifying Application Pools	214
	Verifying Application Pools used by Print Audit Embedded for Xerox sites	215
	Verifying ASP.NET Restriction	216



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

Billy Ray Valentine - Quarterly Earnings.pdf	08:48	🧹 Info	
XYZ Company Financials.pdf - Notepad	08:47	🖌 Info	
Winthorp Industries.pdf - Notepad	08:45	🖌 Info	1 of 3
Duke and Duke - Stock Portfolio.pdf - Notepad	08:45	🔀 Info	
Test.txt - Notepad	2012-04-26	🔀 Info	
	REFRESH	LOGOUT	-

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.

- 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.

Print Audit Embedded for	HP Setup	×
	Welcome to the Print Audit Embedded for HP Setup Wizard	
	The Setup Wizard will allow you to change the way Print Audit Embedded for HP features are installed on your computer or even to remove Print Audit Embedded for HP from your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.	
	< <u>B</u> ack Cancel	

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



Print Audit Embedded for HP Setup
End-User License Agreement Please read the following license agreement carefully
SOFTWARE LICENSE AGREEMENT OF PJLM SOFTWARE INC. OPERATING AS PRINT AUDIT ("VENDOR") SOFTWARE LICENSE AGREEMENT accompanying Software to you only upon the condition that you accept all of the terms contained in this License Agreement and any supplementary license terms included herewith ("Agreement"). READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE SELECTING "Continue" AT THE BOTTOM OF THIS PAGE. YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT.
 I accept the terms in the License Agreement I do not accept the terms in the License Agreement
< <u>B</u> ack <u>N</u> ext > Cancel

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

Print Audit Embedded for HP Setup	
Select Installation Folder This is the folder where Print Audit Embedded for HP will be installed.	Þ
To install in this folder, click "Next". To install to a different folder, enter it below or c "Browse".	lick
Eolder: C:\Program Files (x86)\Print Audit Inc\Print Audit Embedded for HP\ Browse	
< <u>B</u> ack <u>N</u> ext > Ca	incel

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.



Print Audit Embedded for HP Setup Embedded application web site Please select the web site to install to.		×
Web Site Name SITE: "Default Web Site" WEBAPP		
	< <u>B</u> ack <u>N</u> ext > Cancel	

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

Print Audit Embedded for HP Setup	×
Print Audit 6 Please enter your Print Audit server configuration.	le j
Print Audit 6	
Print Audit 6	
IP Address/Host Name	Connection Timeout
Communicator Port 17520	Response Timeout
< <u>B</u> ack	Next > Cancel

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.

O Print Audit Embedded for HP Setup	×
Print Audit Secure Please enter your Print Audit Secure server configuration.	¢
Print Audit Secure	
Enabled	•
Print Audit Secure IP Address/Host Name Virtual Directory pasecure	
< <u>B</u> ack <u>Next</u> >	Cancel

- **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.



🟮 Print Audit Embedded for HP Setup	×
MSI Package Address Please enter the IP Address of the server where this installation package is being installed.	¢
IP Address/Host Name	
< <u>B</u> ack	Cancel

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

Print Audit Embedded for HP Setup	×
HP Embedded Configuration Portal Credentials	c
Please enter credentials to use to access the HP embedded configuration portal.	
Username	
admin	
Password	
•••••	,
Advanced Installer	
< <u>B</u> ack <u>Next</u> >	Cancel



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.

Print Audit Embedded for	HP Setup	×
	Completing the Print Audit Embedded for HP Setup Wizard Click the "Finish" button to exit the Setup Wizard.	
	< <u>B</u> ack Finish Cancel	

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

 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

HP Embedded Adm	ninistrator Authentication
Username: Password:	
	Print Audit Embedded for HP v0.0.8.0

- 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.

Configuration Set	tings	
COMMUNICATOR	PA SECURE	REGISTRATION
Enable PA communicator:	-	
Address:	10.0.1.222	
Port:	17520	
Connection timeout:	20	
Response timeout:	15	
	GOUT	

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

	Embedded	5
Configuration Set	tings	
COMMUNICATOR	PA SECURE REGISTRATION	
Enable PA secure:	✓	
Address:	10.0.1.222	
Virtual directory:	pasecure	
Secure server location:	http://10.0.1.222/pasecure/webservices/	
UPDATE	GOUT	



- **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.

Print Audit Embedded for HP v0.0.18.0 - Inter	net Explorer	Print Audit Embedded for HP.	×	
		P		0
Configuration Set	tings			
COMMUNICATOR	PA SECURE	REGISTRATION	_	
MFP IP address:	10.0.1.220]	
MFP password:	••••]	
Card reader vendor ID:	1008]	
Card reader product ID:	69			
Lo	GOUT		SISTER IS REGISTE	RED v0.0.18.0

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.

Print Audit 6 A	dministration		
<u>F</u> ile <u>E</u> dit ⊻iew <u>T</u>	ools <u>G</u> roups <u>H</u> elp		
🔚 New 👻 📷 Ed	it 🔚 Save 💢 Delete 🏼	🚡 🕐 🕢 🐺 Import 🔮 Export 🛛 🚨 🛛 Ser Groups	
Main	Embedded System	IS	0
e	Use this section to ad- walk-up copiers to wo	d and configure embedded systems for your rk with Print Audit 6	Contraction of the second
System Settings			
	Copier	Serial Number	Device T 🔺
Client Settings			
Client Custom Fields			
0 47			
Printer Profiles			
Thinker Tronies			
Printer Paper Sizes			
2			
S			
Printers			
<u>20</u>			
Advanced			<u> </u>
			1.

To add a new copier:

- 1. Run the Print Audit Administration program.
- 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.
- 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.
- 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.
- 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.



erial number: erial number: eport as printer: eport as user: ethentication type: None> Image: Require additional password Image: Pricing Image: Prompts Advanced Function B/W Cost Color Cost Paper Size Track Fint \$0.100 \$0.100 Letter (8.5 x 11) Copy \$0.100 \$0.100 Letter (8.5 x 11) Scan \$0.100 \$0.100 Letter (8.5 x 11) Fax	erial number: erial number: eport as printer: eport as user: uthentication type: None> I Require additional password Pricing Prompts Advanced Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Copy \$0.100 \$0.100 Letter (8.5 x 11) Scan \$0.100 \$0.100 Letter (8.5 x 11) Fax \$0.100 \$0.100 Letter (8.5 x 11)	pier name:				C Sauce
erial number: eport as printer: eport as user: uthentication type: <none> state additional password Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Copy \$0.100 \$0.100 Letter (8.5 x 11) Scan \$0.100 \$0.100 Letter (8.5 x 11) Fax \$0.100 \$0.100 Letter (8.5 x 11)</none>	erial number: eport as printer: eport as user: uthentication type: None> assword: Require additional password Pricing Require additional password Print S0.100 \$0.100 Letter (8.5 x 11) Copy \$0.100 \$0.100 Letter (8.5 x 11) Scan \$0.100 \$0.100 Letter (8.5 x 11) Fax \$0.100 \$0.100 Letter (8.5 x 11) 	opier name.	1			Save
eport as printer: eport as user: wthentication type: <none> assword: Pricing Pricing Prompts Advanced Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Copy \$0.100 \$0.100 Letter (8.5 x 11) \$ Track Print Scan \$0.100 \$0.100 Letter (8.5 x 11) \$ Track Print Scan \$0.100 \$0.100 Letter (8.5 x 11) \$ Track Print Scan \$0.100 \$0.100 Letter (8.5 x 11) \$ Track Print Scan \$0.100 \$0.100 Letter (8.5 x 11) \$ Track Print Scan \$0.100 \$ Track Print \$ Track Pr</none>	eport as printer:	erial number:				Close
eport as user: uthentication type: <none> assword:</none>	eport as user: uthentication type: <none> assword: Require additional password Pricing Require additional password Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Copy \$0.100 \$0.100 Letter (8.5 x 11) Scan \$0.100 \$0.100 Letter (8.5 x 11) Fax \$0.100 \$0.100 Letter \$0.100 \$0.100 Letter \$0.100 \$0.10</none>	eport as printe	er:		2	
uthentication type: <none> assword: Image: Require additional password Image: Pricing Image: Prompts Advanced Function B/W Cost Color Cost Paper Size Print \$0.100 \$0.100 \$0.100 Letter (8.5 x 11) Image: Print Scan \$0.100 \$0.100 Fax \$0.100 \$0.100</none>	uthentication type: <none> assword: Image: Require additional password Image: Pricing Image: Prompts Advanced Function BAW Cost Color Cost Print \$0.100 \$0.100 Letter (8.5 x 11) Copy \$0.100 \$0.100 Letter (8.5 x 11) Scan \$0.100 \$0.100 Letter (8.5 x 11) Fax \$0.100 \$0.100 Letter (8.5 x 11)</none>	eport as user:			2	
Advanced Function BAW Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Copy \$0.100 \$0.100 Letter (8.5 x 11) Scan \$0.100 \$0.100 Letter (8.5 x 11) Fax \$0.100 \$0.100 Letter (8.5 x 11)	assword:	uthentication (vpe: <none></none>		.	
Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Copy \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Scan \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Fax \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost	Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Image: Color Cost Cost Color Cost Color Cost Color Cost	and the three where the				
Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Copy \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Scan \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Fax \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost	Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Copy \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Scan \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost Fax \$0.100 \$0.100 Letter (8.5 x 11) Image: Color Cost		E Bequi	ire additional i	nassword	
Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) ✓ Copy \$0.100 \$0.100 Letter (8.5 x 11) ✓ Scan \$0.100 \$0.100 Letter (8.5 x 11) ✓ Fay \$0.100 \$0.100 Letter (8.5 x 11) ✓	Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) ✓ Copy \$0.100 \$0.100 Letter (8.5 x 11) ✓ Scan \$0.100 \$0.100 Letter (8.5 x 11) ✓ Fax \$0.100 \$0.100 Letter (8.5 x 11) ✓	assword:	r Requi	ire additional (password	
Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) ✔ Copy \$0.100 \$0.100 Letter (8.5 x 11) ✔ Scan \$0.100 \$0.100 Letter (8.5 x 11) ✔ Fax \$0.100 \$0.100 Letter (8.5 x 11) ✔	Function B/W Cost Color Cost Paper Size Track Print \$0.100 \$0.100 Letter (8.5 x 11) ✔ Copy \$0.100 \$0.100 Letter (8.5 x 11) ✔ Scan \$0.100 \$0.100 Letter (8.5 x 11) ✔ Fax \$0.100 \$0.100 Letter (8.5 x 11) ✔	assword: 🛃 Pricing 🛙	☐ Requi	ire additional dvanced	password	
Print \$0.100 \$0.100 Letter (8.5 x 11) ✔ Copy \$0.100 \$0.100 Letter (8.5 x 11) ✔ Scan \$0.100 \$0.100 Letter (8.5 x 11) ✔ Fax \$0.100 \$0.100 Letter (8.5 x 11) ✔	Print \$0.100 \$0.100 Letter (8.5 x 11) ✔ Copy \$0.100 \$0.100 Letter (8.5 x 11) ✔ Scan \$0.100 \$0.100 Letter (8.5 x 11) ✔ Fax \$0.100 \$0.100 Letter (8.5 x 11) ✔	assword: B Pricing	☐ Requi	ire additional dvanced	password	
Copy \$0.100 \$0.100 Letter (8.5 x 11) ✔ Scan \$0.100 \$0.100 Letter (8.5 x 11) ✔ Fax \$0.100 \$0.100 Letter (8.5 x 11) ✔	Copy \$0.100 \$0.100 Letter (8.5 x 11) ✓ Scan \$0.100 \$0.100 Letter (8.5 x 11) ✓ Fax \$0.100 \$0.100 Letter (8.5 x 11) ✓	essword: Pricing	☐ Requi	ire additional dvanced Color Cost	Paper Size	Track
Scan \$0.100 \$0.100 Letter (8.5 x 11) ♥ Fax \$0.100 \$0.100 Letter (8.5 x 11) ♥	Scan \$0.100 \$0.100 Letter (8.5 x 11) ✔ Fax \$0.100 \$0.100 Letter (8.5 x 11) ✔	assword: Pricing	Requi	ire additional dvanced Color Cost \$0.100	Paper Size Letter (8.5 x 11)	Track
Eav \$0,100 \$0,100 Letter (8.5 v 11)	Fax \$0.100 \$0.100 Letter (8.5 x 11)	essword: Pricing		ire additional (dvanced Color Cost \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11)	Track V
40.100 40.100 Ecker(0.0 x 11)		Assword: Pricing Function Print Copy Scan	Requi Prompts A B/W Cost \$0.100 \$0.10	ire additional (dvanced Color Cost \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track V V

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.

pier name:	-	iewiett rat	ckard	
				Save
erial number:				Close
eport as printer	r. [
eport as user:				
uthentication ty	vpe: <none></none>		•	
assword:	🗖 Begu	ire additional i	password	
Function	BAV Cost	Color Cost	Paper Size	Track
Print	\$0.100	\$0,100	Letter (8.5 x 11)	
0	\$0,100	\$0,100	Letter (8.5 x 11)	
LODY	\$0,100	\$0,100	Letter (8.5 x 11)	
Scan	φ0.100 ·	40.400	Lotter (9 E 11)	10 10 10 10 10 10 10 10 10 10 10 10 10 1
Copy Scan Fax	\$0.100	\$0.100	Letter (0.5 X 11)	

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.

Copier name: Serial number: Report as printer:	Save Close
Serial number:	Close
Report as printer:	
-	
Heport as user:	
Authentication type: <a>None>	•
Password: 🔽 Require additional passv	word
Pricing Rompts Advanced Use custom fields from the user profile if pre- Disable Exact Matching	isent 🗖 Allow comments
Include Custom Field	

- 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

🖀 Add/Edit Embed	ded for Hew	ett-Packard		×
Copier name:				Save
Serial number:				Close
Report as printer:	[
Report as user:			-	
Authentication type:	<none></none>		•	
Password:	E Require ad	ditional password	d	
Pricing R Pr	ompts Advar	nced		
Display Settings -		Admin Cre	edentials	1
🗖 Display Summ	ary Page	Password	l: [******	
		 *USB Car	rd Reader Info	mation
		*Vendor	rID:	
		*Produc	t ID:	

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.

🕼 🔞 🐼 Start Copy	0 🖪 🖸 🕄
Sign In Ready	Copies: 1
HP JetAdvantage	Initial Setup
Connect to On Demand applications	Enable functions and customize the device
Сору	Fax

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.

						Actions
Application Pools	of application pools on the ferent applications.	he server. Application pools	are associated with worker pro	cesses, contain one	or more	Add Application Pool Set Application Pool Defai
Filter: • 🔐 😔 •	Show All Group by	y: No Grouping				▶ Start
ault Web Site Name A	Status .	NET Frame Managed P	peli Identity	Applications		Stop
ASP.NET v4.0	Started v	v4.0 Integrated	ApplicationPoolIden	0		👶 Recyde
HP Embedded App	Started	v4.0 Classic	ApplicationPoolIden	0		Edit Application Pool
PASecure Classic .NET AppPool	Started	2.0 Classic	ApplicationPoolIden	0		Pasis Cattings
DefaultAppPool	Started v	2.0 Integrated	ApplicationPoolIden	1		basic secongs
IP Embedded Agent AppPool	Started v	v4.0 Integrated	NetworkService	0		Recyaing
P Embedded App AppPool	Started	v4.0 Integrated	NetworkService	1		Advanced Settings
PASAppPool	Started v	v4.0 Integrated	NetworkService	1		Rename
						X Remove
						View Applications
						🔞 Help
						Online Help
						Grane nep

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

Edit Application Pool	? ×
Name:	
HP Embedded Agent AppPool	
.NET Framework version:	
.NET Framework v4.0.30319	┓
Managed pipeline mode:	
Start application pool immediately	
OK Cancel	

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..."



Edit Application	<u>? ×</u>
Site name: Default Web Site Path: /	
Alias: Application pool:	
HP.Embedded.Agent HP Embedded Agent AppPool	S <u>e</u> lect
Example: sales	
Physical path:	
C:\Program Files (x86)\Print Audit Inc\Print Audit Emt	
Pass-through authentication	
Connect as Test Settings	
OK	Cancel

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"

Tob											
10	SVF	2008 Ho	me								Actions
188	-10										Manage Server
39e 38 ("011 (711 2071),	Filter:		• 00 00 - 0	Show All Gr	roup by: Area		• 📰 •				e Restart
plication Pools	ASP.NET										Stop
Default Web Site	iin	1			4.	1		i 😜	and the second s	1	View Application Pools
B Embedded Agent	NET	NET	NET Error	- NET	NET Trust	Application	Connection	Machine Key	Pages and	Providers	View Sites
HP.Embedded.App	Authorizati	Compilation	Pages	Globalization	Levels	Settings	Strings	(de line ney	Controls	TTO HOLED	Change .NET Framework \
PASecure	C.										Help
	Session State	SMTP E-mail									Online Help
	ocount otate	or m e mos									
	TIC										
		-		-	_			-	-	-	
	25	×2	0	Ξp	404	2		-	۷		
	Authentication	Compression	Default	Directory	Error Pages	Handler	HTTP	ISAPI and CGI	ISAPI Filters	Logging	
			(The	of Onling	-	(hoppinga	recaport	Read Redona			
	Jan .					1					
	MIME Types	Modules	Output	Request	Server	Worker					
			country	Thursday	Certificates	110003003					
	Manageme	nt									
		1	92	52	Fill 💆	4					
	Configuration	Feature	IIS Managar	TIS Manager	Macagement	Shared					
	Editor	Delegation	Permissions	Users	Service	Configuration					

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

Document Name	Submit Date 💙	Compatibility	
Billy Ray Valentine - Quarterly Earnings.pdf	08:48	🛷 Info	
XYZ Company Financials.pdf - Notepad	08:47	🛷 Info	-
Winthorp Industries.pdf - Notepad	08:45	🖌 Info	1 of 3
Duke and Duke - Stock Portfolio.pdf - Notepad	08:45	🙁 Info	
Test.txt - Notepad	2012-04-26	😢 Info	
	REFRESH	LOGOUT	1

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-update s.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.



Login	○ Registered User							
	Administrator							
Display Speed	Quick Mode Standard Mode							
	To speed up the display speed using the cache in quick mode.							
User Assist	Display dialog box in case of warning.							
Language	English (English)							
	Log							

2. Select Security --> PKI Settings.

	OLTA	ゐ Admin	Administrator							
Model Name:bizhub Co	nnection	Ready	/ to Scan nu (Admin Mode)					品	
Maintenance	System Sett	ings Se	ecurity	User Auth/Acc Tracl	ount «	Network	В	ox		
Print Sett	ing Store	Address	Wizard	с	ustomize		E .	To N Me	lain nu	
 PKI Settings Device Certification 	ate Setting	Device (Registration	ist						
 SSL Setting Protocol Settin 	a	Default	Issuer		Subject		Validity Period	Detail	Setting	
External Certifi	cate Setting	۲	KMC488D7-3	3.bmd. <mark>k</mark> o	KMC488D	7-3.bmd.ko	12/10/2025	Detail	Setting	
Certificate Verification Settings	ition	-						OK	Cancel	

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

▼ PKI Settings	Create Device Certificate	
Device Certificate Setting	Ocreate and install a self-signed Certificate.	
SSL Setting	O Request a Certificate	
Protocol Setting	O Import Certificate	
External Certificate Setting		OK Cancel

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

KONICA MING KONICA MING KONE Web Co Model Name:bizhub C	OLTA nnecti 2258	on e	Adm Rea Rea	inistrator dy to Scan dy to Print						Logout	? 品 〇
Maintenance	Syster	n Setting	s	Security	Us Auth/A Tra	er ccount ck	Netw	vork	Box		
Print Sett	ing	Store Ac	Idress	Fax Settin	ngs	Wizard		Customize		To Ma Ment	in u
 PKI Settings Device Certific SSL Setting Protocol Settin External Certification Certificate Verification Certificate Verification Address Reference Restrict User Acces Auto Logout Administrator Pass Setting 	ate Settin icate Se ition e Settin ess	ing tting g	Create Comr Organ Local State Coun Admi Validi Encry	and install non Name nization nizational Unit ity /Province try n. E-mail Add ty Start Date ty Period rption Key Typ	a self-sig ress	ined Cerl	tificate. 192.168.0 Organiza Unit Canada Alberta Ca km@myu 05/20/20 3650 RSA-10	0.21 tion domain.org 16 12:28:39 Day(s)(1-1 24_SHA-1	3650) ▼		
 TX Operation Log Security Details Quick Security Se USB Connection F setting FW Update (USB) Setting 	Setting tting Permiss Permiss	ion sion								OK C	ancel

5. Click OK again.

Certificate has been created and installed. SSL/TLS can now be used. (After OK is clicked, SSL Mode setting will be available.)

OK

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.

Mai	Maintenance System Setti		em Settin <mark>g</mark>	gs S	Security Auth/A Tr			Network	Вох			
	Print Sett	ing	Store A	ddress	Wizaro	d Ci	istomize		To Main Menu			
▼ PKI Se	ttings			SSL Se	tting							
► Dev	Device Certificate Setting				Mode using SSL/TLS				Admin. Mode and User Mode 🗸			
► SS	L Setting			Encryption Strength				AES-25	6, 3DES-168, RC4-128 🗸			
► Pro	otocol Settin	g		SSL/TLS Version Setting								
► Ext	ternal Certif	icate S	etting	SSLV3								
Certificate Verification Settings				•	TLSv1.1							
► Addre	ss Referenc	e Setti	ng	-	TLSv1.2							
► Restrie	ct User Acc	ess		(eq.					OK Cancel			

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

Maintenance	Syste	em Setting	5	Security	Aut	User h/Account Track	Networ	rk Box	
Print Set	ting	Store Ad	dress	Wizard		Customiz	:e	To Main Menu	
TCP/IP Setting			TCP Se	ocket Setting	g				
E-mail Setting			(Turn ti	ne main switch (OFF, a	nd then ON , wh	nen changing	TCP Socket.)	
LDAP Setting			⊡ T	CP Socket			50158	(1 65535)	
IPP Setting			V 1	Ise SSI /TLS			03100	(1-05050)	
FTP Setting			F	Port No.(SSL/T	(1-65535)				
SNMP Setting			TCP Socket(ASCII Mode)						
SMB Setting			F	Port No.(ASCII	Mode)	59160	(1-65535)	
DPWS Settings			-					OK OFFICI	
Bonjour Setting								OK Cancer	
► NetWare Setting									
AppleTalk Setting	AppleTalk Setting								
RebDAV Settings	;								
OpenAPI Setting									
TCP Socket Setting	ng								

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

Turn the main switch OFF, and then ON, when changing settings.

OK

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.

	Ма	intenance	Syste	em Settings)	Security	Au	User th/Account Track		Network	Box		
_		Print Sett	ing	Store Ad	dress	Wizard		Customiz	ze		.	To Main Menu	
•	TCP/I	P Setting			OpenA	PI			3				
×.	E-mai	il Setting			Use SSL/TLS			S	SSL Only				
LDAP Setting				Port Number			5	50001 (1-65535)					
IPP Setting				Port No.(SSL)			5	0003 (1-	65535)				
•	FTP Setting				Proxy Settings			Ē					
	SNMF	Setting				Toxy Oction A	uures	5	6		K to enter nos	st name.	
	SMB Setting				Proxy Server Port Number			8	8080 (1-65535)				
N	DPWS Settings				Proxy Server Port Number (HTTPS)			5) 8	080 (1-	65535)			
-	Bonjo	our Setting			Proxy Server Port Number (FTP)			2	1 (1-	65 <mark>5</mark> 35)			
	NetW	are Setting			User Name								
	Apple	Talk Setting			Password is changed.			_					
	Mahr	AV Cotting			Password								
1	webl	AV Settings			Certif	licate Verificati	on Le	vel Settings					
	Open.	API Setting			Client Certificates				Do not request				
•	TCP S	Socket Settin	g		Validity Period				Do Not Confirm V				
N 1	IEEE802.1X Authentication Setting			on	CN Key Usage				Do Not Confirm V				
	LLTD	Setting			C	Chain				o Not Confirn	1 🗸		
•	SSDP	Settings			E	Expiration Date	Conf	irmation		o Not Confirm	1 🗸		
Þ 1	Web I	Browser Sett	ing									OK Cancel]

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



Maintenance System Se	ttings	Security	User Auth/Account Track	Network	Box		
Print Setting Stor	e Address	Wizard	Custom	ize	To Main Menu		
► TCP/IP Setting	WebD	AV Server Se	ettings				
E-mail Setting	Web	WebDAV Settings ON V					
LDAP Setting	SSL	SSL Setting Non-SSL Only V					
IPP Setting	Acce	Access Rights Settings					
FTP Setting		New Password					
SNMP Setting		Retype New Password					
SMB Setting				Initial Passwo	ord		
DPWS Settings							
Bonjour Setting					OK Cancel		
► NetWare Setting							
AppleTalk Setting							
▼ WebDAV Settings							
WebDAV Client Settings							
WebDAV Server Settings							

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

	Ма	intenance	Syste	em Setting	s :	Security	Auti	User h/Account Track		Network	Box		
_		Print Sett	ing	Store Ad	ldress	Wizard		Customiz	ze			To M Mer	ain Iu
	TCP/I E-mai	P Setting il Setting			Web B	rowser Setti Browser	ing		En	able 🗸			
* *	LDAP	' Setting etting									[ок	ancel
* *	SNMF	Setting Setting											
× ×	SMB	Setting S Settings											
	NetW	are Setting											
	WebE Open	AV Settings											
•	TCP S	Socket Settin 302.1X Authe	ig inticati	on									
•	Settin	ig Setting											
•	SSDF Web I	' Settings Browser Sett	ing										

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



SCOPICA MINOLTA		Adm	in <mark>ist</mark> rator	Lo	gout		
		Read	dy to Scan				몲
Model Name:bizhub C	:454		enu (Admin Mode)				R
Maintenance	System Sett	ings s	Security	User Auth/Account Track	Network	Box	
Print Sett	ing Store	Address	Wizard	Customize		E	b Main Menu
General Settings		Print w	vithout Authe	entication			
User Authentication	on Setting	Print Authe	without	Full Color/Black	T		
Account Track Set	ttings	IF (F	P Filtering Permit Access)	Disable •			
Print without Auth	entication	(.	IP Address				
Simple Print Auth	entication		Range1	0.0.0	- 0.0.0.	0	
Setting			Range2	0.0.0	- 0.0.0.	0	
External Server Se	ettings	-	Range3	0.0.0	- 0.0.0.	0	
Public User Box S	etting		Range4	0.0.0	- 0.0.0.	0	
User/Account Con Setting	nmon		Range5	0.0.0	- 0.0.0.	0	
Scan to Home Set	tinas					OK	Cancel

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.

Print Audit Embedded for Konica Mino	olta Setup	
End-User License Agreement		
Please read the following license agreeme	ent carefully	5
SOFTWARE LICENSE AGREEMENT		•
OF PJLM SOFTWARE INC. OPERATING	AS PRINT AUDIT ("VENDOR")	
SOFTWARE LICENSE AGREEMENT Ven accompanying Software to you only of the terms contained in this Licens license terms included herewith ("A READ THE TERMS AND CONDITIONS O SELECTING "Continue" AT THE BOTTO	ndor is willing to license the y upon the condition that you accept all se Agreement and any supplementary greement"). OF THIS AGREEMENT CAREFULLY BEFORE DM OF THIS PAGE, YOU AGREE TO BE	
BOUND BY THE TERMS AND CONDITIO	ONS OF THIS AGREEMENT.	-
C I accept the terms in the License Agre	ement	
• I do not accept the terms in the Licens	se Agreement	
	< Back Next Cano	el

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



elect Installation Folder		-
This is the folder where Print Audit installed.	Embedded for Konica Minolta will be	5
To install in this folder, dick "Next". "Browse",	. To install to a different folder, enter	it below or click
<u>F</u> older:		
Files (x86)\Print Audit Inc\Print Aud	dit Embedded for Konica Minolta V	Browse

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.

Print Audit Embedded for Konica Mino	lta Setup		×
Embedded application web site Please select the web site to install to.			0
Web Site Name			
SITE: "Default Web Site" WEBAPP			•
	< <u>B</u> ack	Next >	Cancel

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



<u>•</u>
Connection Timeout
20
Response Timeout
15

- **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.



int Audit Secure		6
Please enter your Print Audit Se	cure server configuration.	
Print Audit Secure		
Enabled		•
IP Address/Host Name		
IP Address/Host Name		
IP Address/Host Name Virtual Directory pasecure		
IP Address/Host Name Virtual Directory pasecure		

- **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.



MSI Package Address		-
Please enter the IP Address of the being installed.	server where this installation package is	C
- IP Address/Host Name		

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

Print Audit Embedded for Konica Plin	olta Setup	
Konica Minolta Embedded Configurat Please enter credentials to use to acces configuration portal.	tion Portal Credentials is the Konica Minolta embedded	e
Username		
admin		
Password		
·····		



10. Select the appropriate Geographic region and click Next.

😔 Print Audit Embedded for Konica Minolta Setup	×
Geographic region Please select in which region the application is installed.	0
Region	
The Americas	•
< Back Next >	Cancel

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

Install p Wizard is ready to b on	egin the Print .	Audit Embec	lded for Konica I	Minolta
ip Wizard is ready to b	egin the Print .	Audit Embec	lded for Konica I	Minolta
tall" to begin the insta on settings, click "Back	llation,If you ".Click "Cance	want to rev I [®] to exit th	iew or change a e wizard.	ny of your
		< <u>B</u> ack	Install	Cancel
	on setungs, click back	on settings, click back . Click Cance	on settings, click back . Click Cancel to exit the	< Back

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.



PRINT AUD

Embedded Sembedded Administrator Authentication
Username: admin

Username:	admin	
Password:		
	LOGIN	CLEAR

- 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.

		PRINT_AUDIT Embedded
onfiguration Sett	ings	
COMMUNICATOR	PA SECURE REGISTRATION	
Enable PA communicator:	v	
Address:	192.168.0.124	
Port:	17520	
Connection timeout:	20	

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.

				PRINT_AUDIT Embedded	C
Configuration Set	tings				
COMMUNICATOR	PA SECURE	REGISTRATION			
Enable PA secure:					
Address:	192.168.0.124	ł			
Virtual directory:	pasecure				
Secure server location:	http://192.168	3.0.124/pasecure/we	bservices/		
UPDATE	OGOUT				v0.0

- **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.

			PRIN	
Configuration Se	ttings			
COMMUNICATOR	PA SECURE	REGISTRATION		
MFP IP address:				
MFP password:				
			GISTER IS REGISTERED	V0.3.0



• The Registration may take some time to complete.

Print Audit Embedded for		
← → C 🗋 localhost/KM.Embed	ded.App/	무 ☆] 〓
Configuration Set	tings	
COMMUNICATION		
MFP IP address:	Registering applicatio	n
MFP password:		

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.

🥞 Print Audit 6 A	Administration			
<u>F</u> ile <u>E</u> dit ⊻iew (<u>T</u> ools <u>G</u> roups <u>H</u> elp			
🎦 New 🔻 🎦 E	dit 📕 Save 💢 Delete	: 🚱 🕙 🕢 🐺 Import 🔮 Expo	t 🎒 User Groups	
Main	Embedded Syst Use this section to walk-up copiers to	tems o add and configure embedded syst o work with Print Audit 6	ems for your	
	Copier	Serial Number	Device Type	-
Printer Paper Sizes				
sinters 🖉				
2				
				_
mbedded Systems				
Advanced				-
	. р.	<u>k</u>		

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.

				Save
erial number:				Close
eport as printer	. [
eport as user:				
uthentication ty	vpe: <pre> </pre>		-	
uthentication ty assword:	vpe: <mark> <none></none></mark>	re additional (password	1
uthentication ty assword: Pricing	vpe: <a>None Require Restrictions B/W Cost 	re additional Prompt	Dassword	ced
uthentication ty assword: Pricing	vpe: <pre></pre> <pre></pre> <pre></pre> <pre> <pre> <pre> </pre> <pre> <pre> </pre> </pre> <pre> </pre> <pre> </pre> <pre> </pre> <pre> </pre> </pre> <pre> </pre> </pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>	re additional Prompt Color Cost \$0.100	Password Is Limits Advan Paper Size Letter (8.5 x 11)	ced Track
uthentication ty assword: Pricing	vpe: <a>None> Restrictions B/W Cost \$0.100 \$0.100 	re additional Color Cost \$0.100 \$0.100	Dassword Is Limits Advan Paper Size Letter (8.5 x 11) Letter (8.5 x 11)	ced Track V
uthentication ty assword: Pricing	vpe: <a>None> Restrictions B/W Cost \$0.100 \$0.100 \$0.100 	re additional p Color Cost \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	ced Track V V

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

opier name:				
	-			Save
erial number:				Close
eport as printer:	-			
eport as user:				
uthentication type	x <pre></pre>		•	
lacoword:	-	1.07	275 275	
	I Hequi	re additional	password	
Pricing	Restrictions	re additional	ts	ced
Function	Restrictions	Color Cost	Password	Track
Function	Restrictions	Color Cost \$0.100	Password Paper Size Letter (8.5 x 11)	Track
Function Print Copy	Restrictions B/W Cost \$0.100 \$0.100	Color Cost \$0.100 \$0.100	Password Paper Size Letter (8.5 x 11) Letter (8.5 x 11)	Track

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.

	Save
	Close
	2
	2
<none></none>	•
E Require additional password	
estrictions 43 Prompts 64 Limits	Advanced
te	None> Require additional password testrictions T Prompts Limits hary Page

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:


Select server rol	ES	DESTINATION SERVER
Before You Begin	Select one or more roles to install on the selected server.	PJLM-KONICA.printaudit.loca
Installation Type	Roles	Description
Server Selection Server Roles Features Confirmation Results	▲ Web Server (IIS) (18 of 43 installed) ▲ ■ Web Server (14 of 34 installed) ▷ ■ Common HTTP Features (4 of 6 installed) ▷ ■ Common HTTP Features (4 of 6 installed) ▷ ■ Health and Diagnostics (2 of 6 installed) ▷ ■ Performance (1 of 2 installed) ▷ ■ Security (2 of 9 installed) ▲ ■ Application Development (5 of 11 installed) ✓ .NET Extensibility 3.5 (Installed) ✓ .NET Extensibility 4.5 (Installed) △ ASP.NET 3.5 ✓ ASP.NET 4.5 (Installed) □ CGI ✓ ■	Application Development provides infrastructure for developing and hosting Web applications. Use these features to create Web content or extend the functionality of IIS. These technologies typically provide a way to perform dynamic operations that result in the creation of HTML output, which IIS then sends to fulfil client requests.

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"

Application Pools				
This page lets you view and manage the worker processes, contain one or more a	list of application p pplications, and pr	oools on the serve ovide isolation am	r. Application pools a ong different applica	are associated with ations.
Name *	Status	.NET Frame	Managed Pipeli	Identity
ASP.NET v4.0	Started	v4.0	Integrated	ApplicationPoolIden
ASP.NET v4.0 Classic	Started	v4.0	Classic	ApplicationPoolIden
Classic .NET AppPool	Started	v4.0	Classic	ApplicationPoolIden
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIden
KM Embedded App AppPool	Started	v4.0	Integrated	NetworkService

3. Double click on the Application Pool Name.



lit Application Pool	? ×
Name:	
KM Embedded App AppPool	
.NET <u>F</u> ramework version:	
.NET Framework v4.0.30319	•
Managed pipeline mode:	
Integrated 💌	

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...

Site name: I Path:	Default Web Sit /	te	
lias:		Application pool:	
M.Embedded.	Арр	KM Embedded App AppPool	S <u>e</u> lect
Example: sales Physical path: C:\Program File	es (x86)\Print A	udit Inc\Print Audit Emb	
ass-through a	uthentication		
	1000		

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.



Start Page Start Page Start Page Servez 200682 (PRINTALIDITIS Application Pools Start Default Web Site Construction Default Web Site	SERVER2008	R2 Home	Show All G Show All G NET Globalization Session State	NET Trust Levels SMTP E-mail	Application Settings	Connection Strings	Actions Hanage Server Restart Start Stop View Application Pools View Sites Change .NET Framewor Pielep Online Help
	IIS Authentication Compression ISAPI and CGI ISAPI Filters Restrictions	Default Document Logging	Directory Browsing MIME Types	Error Pages	Handler Mappings Output Caching	HTTP Respo Request Filtering	
	Server Worker Certificates Processes Management	\$2	52	80. <mark>7</mark>	¥=		

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

Thternet Information Services (11	5) Manager			
SERVER2008R2 SERVER208 SERVE	•			😐 🖂 🕼 •
Eile View Help				
Ele View Heb Connections Start Page Start Page Strict	Sector 2 April	rictions CGI extensions that can run of Allowed Not Allowed Not Allowed	n the Web server. Path %windf%VMcrosoft.NETVFramework64/v2 %windf%VMcrosoft.NETVFrameworkVv4. C:WindowsVMcrosoft.NETVFramework64/v	Alerts ① The CGI module is not installed. applications that are allowed to run, but they will not be able to run until the CGI module is installed. Add Edit Feature Settings ② Help Online Help
Configuration: 'localhost' applicationHost.c	onfig			G
and a second				

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

lease select a document below:	Secure		
Document Name	Submit Date 💙	Compatibility	
Billy Ray Valentine - Quarterly Earnings.pdf	08:48	💉 Info	
XYZ Company Financials.pdf - Notepad	08:47	🖌 Info	
Winthorp Industries.pdf - Notepad	08:45	🖌 Info	1 of 3
Duke and Duke - Stock Portfolio.pdf - Notepad	08:45	🔀 Info	
Test.txt - Notepad	2012-04-26	😣 Info	
RELEASE CANCEL	REFRESH JOB LIST	LOGOUT	-

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:

 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"
 - I. 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)
- 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

Copier name:				Save
Serial runder:				Close
Report as primer:		8		Analy
Report as use				нрру
Autheni ation ya	e: (None)		-	
Passward	Require addit	onal password		
Inactivity.timec.#	180	(seconds)		
	Restrictions 23 P	rompts 🔓 Limits 💡	Advanced	
Logging Informa	tion	Device Configur	ation	
Log levet	rrors only	Device IP:		
Log IP: 1	32.168.0.1	Port 70	001	
Log Port 9	999	E	dit Configuratio	n

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	Configu	uration
--------	---------	---------

Copier name:			Save
Serial number:			Close
Report as printer:		8	Ansh
Report as user:		8	Арру
Authentication type:	(None)	ہا لے 💴	
Password	Require additio	nal password	
Inactivity timeout:	180	(seconds)	
🏭 Pricing 🔒 R	estrictions 23 Pro	ompts 🔒 Limits 🦉 A	dvanced
Logging Information		Device Configuration	n
Log level: Erron	only •	Device IP:	
Log IP: 192.1	68.0.1	Port 7001	
Log Port 9999		Edit	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
- Port the port used to communicate with the Kyocera device. This setting defaults to port " 7001"

Edit Configuration



Copier name:				Save
Serial number:				Close
Report as printer:		1	8	Analy
Report as user:			а П	Adda
Authentication type:	<none></none>		•	
Password:	Require additions	/ password	- 11	
Inactivity timeout:	180	(seconds)	- 11	
👯 Pricing 🔒 R	lestrictions	pts 🔂 Linits	💡 Rdva	ced
Logging Informatio	n	Device Confi	guration	
Log levet Eno	ts only 🔻	Device IP:	-17	
Log IP: 192	168.0.1	Port	7001	
Log Port 9995)		Edit Confi	guration

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
- 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

Edit Device Configuration ECOSYS M6526cidn		×
Communicator Settings Display Settings PA Secure Settings Enable PA Secure: PA Secure Server Location: http://	/webservices/	Save Cancel Apply To Device
Ready		

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.

Print Audit 6 Au	dministration			
Eile Edit View I	ools <u>G</u> roups <u>H</u> elp it JR Save 🗶 Delete	😘 🛞 🛞 🌲 Import 🔮 Exp	ort 🏻 🚨 User Groups	
Main Main Printer Profiles	Embedded Syste Use this section to a walk-up copiers to v	ms Idd and configure embedded sys vork with Print Audit 6	stems for your	(
Printer Paper Sizes	Copier	Serial Number	Device Type	
S Printers				E
User Profiles				
Carlos Users				
Embedded Systems				
Advanced				-
				//.



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:

Add/Edit Emb	edded for K	yocera		×
Copier name:				Save
Serial number:				Close
Report as printer:				Apply
Report as user:				
Authentication type	: <none></none>		•	
Password:	🔄 Requi	re additional p	assword	
Inactivity timeout:	180		(seconds)	
🔡 Pricing 🔒	Restrictions	Prompt	s 🔓 Limits 🖓 .	Advanced
Function	B/W Cost	Color Cost	Paper Size	Track
	40.100	#0.100	Letter (9.5 v 11)	177
Print	\$0.100	\$0.100	Letter (0.5 X 11)	v
Print Copy	\$0.100	\$0.100	Letter (8.5 x 11)	
Print Copy Scan	\$0.100 \$0.100 \$0.100	\$0.100	Letter (8.5 x 11) Letter (8.5 x 11)	
Print Copy Scan Fax	\$0.100 \$0.100 \$0.100 \$0.100	\$0.100 \$0.100 \$0.100 \$0.100	Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	
Print Copy Scan Fax	\$0.100 \$0.100 \$0.100 \$0.100	\$0.100 \$0.100 \$0.100 \$0.100	Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	V V V
Print Copy Scan Fax	\$0.100 \$0.100 \$0.100 \$0.100	\$0.100 \$0.100 \$0.100 \$0.100	Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	
Print Copy Scan Fax	\$0.100 \$0.100 \$0.100 \$0.100	\$0.100 \$0.100 \$0.100 \$0.100	Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	▼ ▼ ▼ E dit
Print Copy Scan Fax	\$0.100 \$0.100 \$0.100 \$0.100	\$0.100 \$0.100 \$0.100 \$0.100	Letter (8.5 × 11) Letter (8.5 × 11) Letter (8.5 × 11)	V V V Edit

- 1. Run the Print Audit Administration program.
- 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.
- 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

ipier name:				Save
rial number:				Close
eport as printer:				Applu
eport as user:				Apply
thentication typ	e: <none></none>		•	
issword:	Requir	re additional p	password	
activity timeout:	180		(seconds)	
,			(00001100)	
Pricing	Restrictions	Promp	ts 🔓 Limits 🖓 Ac	dvanced
Pricing	Restrictions B/W Cost	Color Cost	ts 🔂 Limits 💡 Ac	dvanced
Pricing	Restrictions B/W Cost \$0.100	Color Cost \$0.100	research, Limits 💡 Ac	dvanced
Pricing	B/W Cost \$0.100 \$0.100	Color Cost \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11)	tvanced
Pricing	Restrictions B/W Cost \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100	Imits Imits	dvanced
Pricing Function Print Copy Scan Fax	Restrictions B/W Cost \$0.100 \$0.100 \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	dvanced
Pricing Function Print Copy Scan Fax	B/W/ Cost \$0.100 \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Jvanced

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

- they cont critic	edded for K	iyocera		X
Copier name:				Save
Serial number:				Close
Report as printer:			8	Applu
Report as user:				
Authentication type	e: </td <td></td> <td>•</td> <td></td>		•	
Password:	🔄 Requi	re additional p	assword	
inactivity timeout:	180		(seconds)	
强 Pricing 🔒	Restrictions	Prompt	s 🔁 Limits 🖓 A	dvanced
Function	B/W Cost	Color Cost	Paper Size	Track
Function Print	B/W Cost \$0.100	Color Cost \$0.100	Paper Size Letter (8.5 x 11)	Track
Function Print Copy	B/W Cost \$0.100 \$0.100	Color Cost \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11)	Track
Function Print Copy Scan	B/W Cost \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track
Function Print Copy Scan Fax	B/W Cost \$0.100 \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track
Function Print Copy Scan Fax	B/W Cost \$0.100 \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track V V
Function Print Copy Scan Fax	B/W Cost \$0.100 \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track V V V
Function Print Copy Scan Fax	B/W Cost \$0.100 \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track V V Edit
Function Print Copy Scan Fax	BAW Cost \$0.100 \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track V V Edit

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 Embed	Ided for Kyocera	
Copier name:	Save	
Serial number:	Close	
Report as printer:	Apply	1
Report as user:		
Authentication type:	<none></none>	
Password:	Require additional password	
Inactivity timeout:	180 (seconds)	
强 Pricing 🍐 R	estrictions 🖳 Prompts 🔂 Limits 💡 Advanced	
Function Type	Group Name Action	
		2



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)

😁 Add/Edit Embed	Ided for Kyocera	X
Copier name:		Save
Serial number:		Close
Report as printer:	8	Apply
Report as user:		
Authentication type:	<none></none>	
Password:	Require additional password	
Inactivity timeout:	180 (seconds)	
🐫 Pricing 🔒 R	estrictions 🖳 Prompts 🔒 Limits 💡 A	dvanced
🔲 Use custom fie	lds from the user profile if present	ow comments
Include Custom F	ïeld	

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)

Add/Edit Embe	edded for Ky	ocera			×
Copier name:					Save
Serial number:					Close
Report as printer:			8		Apply
Report as user:					
Authentication type:	<none></none>		•]	
Password:	🗌 Require	e additional p	assword		
Inactivity timeout:	180	(seconds)		
🐫 Pricing 🔒	Restrictions	Prompts	s 🚹 Limits 💡	Advanced	
Pricing 🔒	Restrictions	Frompts	Limits 💡	Advanced	
Pricing A	Restrictions	File if present	Message Title	Advanced	op Job
Pricing A	Restrictions	File if present	Message Title	Advanced	dol qe
Pricing A	Restrictions	File if present	Message Title	Advanced	pJob
Pricing A Use limits fro Function Type Add	Restrictions	Prompts file if present Limit Remove	Message Title	Advanced	dof de

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



Copier name:	Save
Serial number:	Close
Report as printer:	
Report as user:	
Authentication type: <pre></pre>	•
Password: Require additiona	l password
Inactivity timeout: 180	(seconds)
🐫 Pricing 🔒 Restrictions 🖳 Prom	pts 🔓 Limits 💡 Advanced
Logging Information	Device Configuration
Log level: Errors only 💌	Device IP:
Log IP: 192.168.0.1	Port: 7001
Log Port: 9999	Edit Configuration

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

Communicator Settings Displ	ay Settings PA Secure Settings	Save
Enable PA6:		Cancel
Address:	PA6Server	
Port	17520	
Timeout (milliseconds):	5000 (milliseconds)	
Use SSL:		
Use GZip:		

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.

Save
Cancel
Apply To Device

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



Communicator Settings Display Settings PA Secure Settings		Save
Enable PA Secure: 🕅		Cancel
PA Secure Server Location: http://	/webservices/	Apply To Device

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.

(i) 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

Document Name	Submit Date 💙	Compatibility	
Billy Ray Valentine - Quarterly Earnings.pdf	08:48	🖌 Info	
XYZ Company Financials.pdf - Notepad	08:47	🖌 Info	_
Winthorp Industries.pdf - Notepad	08:45	🖌 Info	1 of 3
Duke and Duke - Stock Portfolio.pdf - Notepad	08:45	🛞 Info	
Test.txt - Notepad	2012-04-26	😢 Info	
RELEASE CANCEL	REFRESH	LOGOUT	

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

	Solutions	System Network License					
Device Status	Install Uninstall Start Stop						
Scan Profile		Installed Solutions	Version	State	License		
Copy Printer Settings	• 🚳	BETA - Debug Application	4.0.0.080911	Running	None Required		
Settings							
Reports	- 🚸	Remote Operator Panel	2.1.0	Running	None Required		
Links & Index Applications	• 🚳	USB My MFP Application	2.1.0	Running	None Required		
Order Supplies							

Click the Install button



	Solutions System Network License			
Device Status	Install A New Solution			
Scan Profile	Solution Install File	Choose File No file chosen		
Copy Printer Settings			Start Install	Return
Settings	Status			
Reports				
Links & Index				
Applications				
Order Supplies				

Click the Choose File button

	Solutions System Network License
Device Status	Install A New Solution
Scan Profile	Solution Install File Choose File No file chosen
Copy Printer Settings	Onen Start Install Return
Settings	COC Vice Local Disk (C:) > LES-sdk-ESS.43.041 > target > jars > lexmarkembedded + 4 Search lexmarkembedded P
Reports	Organize ▼ New folder 🔠 ▼ 🗍 😧
Links & Index	Becent Places Name Date modified Type Size
Applications Order Supplies	Image: Concept Image: Concent Image: Concept Imag
	File name: All Files

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

	Solutions System Network License	
Device Status	Install A New Solution	
Scan Profile	Solution Install File Choose File lexmarkembedded fis	
Copy Printer Settings		Start Install Return
Settings	Status	
Reports		
Links & Index		
Applications		
Order Supplies		

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



Menus		
Supplies Menu		\bigcirc
Paper Menu		
Reports		
Network/Ports		
Security		
Settings		\bigtriangledown
2	Back	

Select Security

<u>Menus</u> -> Security	
Edit Security Setups	
Miscellaneous Security Settings	
Confidential Print	
Disk Wiping	
Security Audit Log	
Set Date and Time	
	Back

Select Edit Security Setups



<u>Menus</u> -> <u>Security</u> -> Edit Security Setups	
Edit Backup Password	
Edit Building Blocks	
Edit Security Templates	
Edit Access Controls	
	Back

Select Edit Security Templates

Menus ->> <u>Edit Security Setups</u> -> Edit Security Te	mplates
	Add Entry
	Open Entry
	Delete Entry
	Delete List
Displaying 0 - 0 / 0	k

Click the Add Entry button



	_{Name} PrintAudit				
	abc 123	âáä¥	Ююźó	한글	
image: mail of the second	2 3 e r s d z x \ /	4 5 6 t y u f g h c v b Space	78i0jknmClear	9 0 9 0 1 ; ; ; ; ; ; ; ; ; ; ; ; ;	Backspace
			1	Cancel	

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

Authentication Setup			
Internal_Accounts_Building_Block	0		
PAM Example - AuthN and AuthZ	0		
PAM Example - AuthN Only	0		
PAM Example - Group AuthZ	0		
PrintAudit Authorization Service			
Displaying 1 - 5 / 5		Cancel	Next

Select PrintAudit Authorization Service , and click the Next button



Authorization Setup			
None	0		
PAM Example - AuthN and AuthZ	0		
PAM Example - Group AuthZ	0		
PrintAudit Authorization Service	۲		
Displaying 1 - 4 / 4		Cancel	Next

Select PA Group and click the Next button

Set Groups	
PA Group	
Displaying 1 - 1 / 1	Cancel Next

The PrintAudit Security Template is now created



Menus	->> Edit Security Se	etups -> Edit Security	Templates
PrintAudit		0	Add Entry
			Open Entry
			Delete Entry
			Delete List
	Displaying 1 - 1 / 1		Back

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



	Security Setup	
Device Status	Basic Security Setup	
Scan Profile	Use the Basic Security Setup to limit access to the configuration menus via the operator panel and the emi	bedded web server.
Copy Printer Settings	Applying this setup may overwrite a previous configuration.	
Settings	Authentication Type Password	
	Password Range: 8 - 128 characters	
Reports	Re-enter password	
Links & Index	Apply	
Applications	Advanced Security Setup	Additional Security Setup Options
Order Supplies	Step 1: Configure a Security Building Block: "Building Blocks" are the various methods for getting user credentials.	The Backup Password provides access to the Security Menus regardless of the assigned protection method or the availability of that method (such as an LDAP server or a network being down).
	Password LDAP+GSSAPI Kerberos 5	Backup Password
		Guided Security Setup
	Step 2: Set up a Security Template.	
	Security Templates are used to restrict access, and are made from 1 or more Building Blocks.	
	Step 3: Apply your Security Template to one or more Access Controls.	
	Choose from available Security Templates to control occase to execution durictions or menus, or to disable functions entirely.	

Select Access Controls

LEXMARK	Power Saver Black Cartridge Low Refresh	Lexmark X734de Address: 192.168.0.70 Contact Name: Location:
	Settings Menu Remotely	No Security 🔻
Device Status	Network/Ports Menu at the Device	No Security 💌
Scan Profile	Network/Ports Menu Remotely	No Security V
	Manage Shortcuts at the Device	No Security V
Copy Printer Settings	Manage Shortcuts Remotely	No Security V
Settings	Flash Drive Print	No Security V
	Flash Drive Color Printing	No Security 🔻
Reports	Flash Drive Scan	No Security V
Links & Index	Flash Drive Firmware Updates	No Security V
	Web Import/Export Settings	No Security 🔻
Applications	Copy Function	No Security
	Copy Color Printing	No Security
Order Supplies	Color Dropout	PrintAudit
	E-mail Function	No Security 🔻
	Fax Function	Disabled v
	Release Held Faxes	No Security 🔻
	FTP Function	No Security 🔻
	Held Jobs Access	No Security 🔻
	Use Profiles	No Security 🔻
	Create Bookmarks at the Device	No Security 🔻
	PictBridge Printing	No Security 🔻
	eSF Configuration	No Security 🔻
	Remote Management	No Security V

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

	Solutions System Network License	
Device Status	Print Audit Lexmark Embedded	
Scan Profile		
Copy Printer Settings	Information Configure License	
	Communicator Settings 🤨	
Settings	Enable PA6 🗆 🗇	
Reports	Communicator IP 🛛 🕜	
Links & Index	Communicator Port 0	
Applications	Communicator Timeout	
	Secure Server Settings 📀	
Order Supplies	Enable Secure Server 🛛 🗇	
	Secure IP	
	Test Import Export Restore Defaults Reset App	ly

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 "10.10.10.10.10.", the Secure IP set up would be
 10.10.10.10.10.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.

📕 Save 🗙 Delete	😘 🛞 🛞 🌷 Import 🔮 Expor	Liser Groups	
mbedded Syste Use this section to a walk-up copiers to v	e ms add and configure embedded syst work with Print Audit 6	ems for your	6
opier	Serial Number	Device Type	^
	Use this section to a walk-up copiers to v	Use this section to add and configure embedded systematic walk-up copiers to work with Print Audit 6 pier Serial Number	Use this section to add and configure embedded systems for your walk-up copiers to work with Print Audit 6 pier Serial Number Device Type

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

p.e				Save
rial number:				Close
port as printer:				Applu
port as user:				
thentication type	e: </td <td></td> <td>•</td> <td></td>		•	
ssword:	Requi	re additional r	password	
ssword:	🗌 Requi	re additional p	bassword	J
ssword: Bericing	Requi	re additional (bassword	
ssword: B Pricing	Requi	re additional p 뜨릿 Promp	bassword	J ced
ssword: Pricing	Restrictions	re additional p	password ts 🔓 Limits Advand	ced
ssword: Pricing A Function Print	Restrictions	re additional p Color Cost \$0.100	bassword ts 🔂 Limits Advanu Paper Size Letter (8.5 x 11)	Track
ssword: Pricing Function Print Copy	Restrictions B/W Cost \$0.100 \$0.100	re additional p Color Cost \$0.100 \$0.100	bassword Paper Size Letter (8.5 x 11) Letter (8.5 x 11)	Track
ssword: Pricing Function Print Copy Scan	Restrictions B/W Cost \$0.100 \$0.1	re additional (Color Cost \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track
Seword: Pricing 6 Function Print Copy Scan Fax	Restrictions B/W Cost \$0.100 \$	re additional p Color Cost \$0.100 \$0.100 \$0.100 \$0.100 \$0.100	bassword Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track V V V
ssword: Pricing 6 Function Print Copy Scan Fax	Restrictions B/W Cost \$0,100 \$	re additional p Color Cost \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track V V V

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

				Save
rial number:				Close
eport as printer	:		<u></u>	(de-h
eport as user:				Арріу
Ithentication ty	pe: <pre> </pre>		•	
ssword:	Regui	re additional p	bassword	
issword:	Requi	re additional p	password	
ssword: Bericing	Requi	re additional p	bassword	ced
issword: B Pricing	Restrictions	re additional p	bassword ts 🔂 Limits Advanc	Track
issword: Pricing 4 Function Print	Restrictions B/W Cost \$0.100	re additional p Fromp Color Cost \$0.100	bassword ts Conc Limits Advanc Paper Size Letter (8.5 x 11)	Track
Issword: Pricing	Restrictions B/W Cost \$0.100 \$0.100	Color Cost \$0.100 \$0.100	Password Paper Size Letter (8.5 x 11) Letter (8.5 x 11)	Track
Issword: Pricing Function Print Copy Scan	Requi Restrictions B/W Cost \$0.100 \$0.100 \$0.100	re additional p Color Cost \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track
Issword: Pricing Function Print Copy Scan Fax	Requi Restrictions B/W Cost \$0.100 \$0.100 \$0.100 \$0.100	Color Cost \$0.100 \$0.100 \$0.100 \$0.100 \$0.100	Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track
Pricing Priction Function Print Copy Scan Fax	Requi	Color Cost \$0.100 \$0.100 \$0.100 \$0.100 \$0.100	Password Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track
Ssword: Pricing Function Print Copy Scan Fax	Restrictions B/W Cost \$0.100 \$0.1	re additional p Color Cost \$0.100 \$0.100 \$0.100 \$0.100	Password Paper Size Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11) Letter (8.5 x 11)	Track V V V

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)

sopier name.			Save
Serial number:	-		Close
Report as printer:		a	
Report as user:		8	Appiy
Authentication type:	<none></none>	•	
Password	Bequire additional pa	ssword	
Function Type	Group Name	Action	
Function Type Color prints	Group Name < All users >	Action	

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)

Copier name: Serial number:				
Serial number:				Save
				Close
Report as printer:			<u></u>	A1-
Report as user:				
Authentication type:	<none></none>		•	
Password:		additional	password	
🔲 Use limits fro	m the user prol	ile if prese	nt	
-	1.1.1.10	1.1.1.	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

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

Edit Embedded fo	or Lexmark			X
ne:				Save
iber:				Close
printer:				Applu
user:			8	
ation type: <pre> </pre>	ne>		•	
. Re	equire additional pa	assword		
ng 🛛 🔒 Restrictio w Settings	ons 🛛 🖳 Prompts	Device Conf	Advanced	
play Summary Pag	je	Device IP:		
		Port:	7001	
			Edit Config	guration
				guration

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

Save
Cancel
Apply To Device
conds)

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

Communicator Settings PA S	ecure Settings		Save
Enable PA Secure: PA Secure Server Location:	http://	/webservices/	Apply To Device
eady			

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.

O 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

Document Name	Submit Date 💙	Compatibility	
Billy Ray Valentine - Quarterly Earnings.pdf	08:48	🖌 Info	
XYZ Company Financials.pdf - Notepad	08:47	🖌 Info	_
Winthorp Industries.pdf - Notepad	08:45	🖌 Info	1 of 3
Duke and Duke - Stock Portfolio.pdf - Notepad	08:45	8 Info	
Test.txt - Notepad	2012-04-26	🛞 Info	
	REFRESH	LOGOUT	1

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

(i) 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.

B Print Audit 6 Embedded - Sharp (6.3.0R) - Installation		
(()	Welcome to the InstallShield Wizard for Print Audit 6 Embedded - Sharp	
PRINT AUDIT	The InstallShield(R) Wizard will install Print Audit 6 Embedded - Sharp on your computer. To continue, click Next.	
	WARNING: This program is protected by copyright law and international treaties.	
< Back Next > Cancel		

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.

print Audit 6 Er	mbedded - Sharp (6.3.0R) - InstallShield Wizard	x
Select a Web Please select th	e site PRINT GLUDIT	٥
Select site:	Default Web Site	
InstallShield	< Back Next > Cancel	



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

时 Print Audit	6 Embedded - 9	Sharp (6.3.0R) - InstallShield Wizard	×
Database Please ente	Communicato er the location of t		
InstallShield —	Location: Port:	PJLM-DEV12 17520 < Back Next	> Cancel

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.

Print Audit 6 Embedded - Sharp (6.3.0R) - InstallShield Wizard Print Audit Secure Location	
Please enter location of the Print Audit Secure webservices	
Please enter the location of the Print Audit Secure web services (ie. localhost/PASecure)	
PA Secure Webservice Location: PJLM-DEV12/PASecure	
< Back Next	> Cancel

8. Select Install to begin installing Embedded for Sharp.



Ready to Install the Program The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your installation exit the wizard.	settings, dick Back. Click Cancel to

9. When the installation is complete, click Finish.

Print Audit 6 Embedded - S	harp (6.3.0R) - Installation
(0)	InstallShield Wizard Completed
	The InstallShield Wizard has successfully installed Print Audit 6 Embedded - Sharp. Click Finish to exit the wizard.
	< Back Finish Cancel

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.
- 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.
- 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.
- 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.



🚟 Add/Edit Embe	dded for Sharp		
Copier name:			Save
Serial number:			Close
Report as printer:			
Report as user:			
Authentication type:	<none></none>	*	
Password:	Require additional password		
nicing 🔒 Re	strictions 🖳 Prompts 🔂 Lin	nits 💡 💡 Advanc	ed
Use custom field	ds from the user profile if present	Allow co	mments

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.



Add/Edit Embedded for Sha	arp		×
Copier name:			Save
Serial number:			Close
Report as printer:	8		
Report as user:			
Authentication type: <a>None>	~		
Password: Require add	itional password		
nicing 🔒 Restrictions 🔩	Promots 🔂 Limits 💡	Advanced	I.,
Log levet:	Emors 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

Stogin - MX-2300N - Nozili	a Firefox			🛛
Elle Edit Yew History Bool	imarts Isols Help			0
🔶 👻 😌 🌾 🔶	Http://192.168.0.67/kg	gin Jitanii') (wain Jitani	* 🕨 💽 Google	G,
🔝 Custonize Litiks 🔝 Free Hotni	al 📄 Windows Marketplace 🕻	🐨 Windows Nedia 🔝 Windows		
	_			
SHARP				
MX-2300N	Login			
	Login(P)			_
	Login Name:		(Up to 255	
	Password	characters)	(1-32 digits)	
	Lag-in as the user who	s has the authority to display th	e page that requires the admini	strator
	autority.		Back to the Top on Th	Pase A
	Login(P)			
Dane				

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".
- Set Address for Application UI to http://xxx.xxx.xxx/pa6sharp/pages/Start.aspx, where 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/pa6sharp/pages/Service.asmx where 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.

O 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

B	Add Roles and Features Wizard	_
Select server role Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard S Select one or more roles to install on the selected server. Roles Use Volume Activation Services Web Server (IIS) (18 of 43 installed) Web Server (IIS) (18 of 43 installed) Web Server (IIS) (18 of 43 installed) Health and Diagnostics (1 of 6 installed) Reference Refere Reference	DESTINATION SERVER pjim-2012R2.printaudit.local Description Security provides infrastructure for securing the Web server from users and requests. IIS supports multiple authentication methods. Pick an appropriate authentication scheme based upon the role of the server. Filter all incoming requests, rejecting without processing requests that match user defined values, or restrict requests based on originating address space.
	✓ ISAPI Filters (Installed) Server Side Includes WebSocket Protocol ✓ III ✓	
	< Previous Next >	> Install Cancel

IIS 6 Management Compatibility Tools



	Add Roles and Features Wizard
Select server role Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	DESTINATION SERVER pjm-2012R2 printaudit/local Select one or more roles to install on the selected server. Roles Meb Server (IIS) (14 of 43 installed) B Web Server (13 of 34 installed) B Web Server (13 of 1 of 7 installed) B Web Server (13 of 1 of 7 installed) B Web Server (13 of 1 of 7 installed) B Web Server (13 of 6 Management Compatibility W IIS 6 Management Console W IIS 6 Management Console
	IIS 6 WMI Compatibility IIS Management Scripts and Tools Management Service Windows Deployment Services Windows Server Essentials Experience Windows Server Update Services ✓

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".

Ø	Internet Information Services (IIS) Manager	_ D X
● PJLM-2012R2	>	😳 🗠 🟠 🔞 •
<u>F</u> ile ⊻iew <u>H</u> elp		
Eile View Help Connections Start Page Application Pools Application Pools Applicatio	Image: Start of the start	Alerts The CGI module is not installed. You can specify CGI applications that are allowed to run, but they will not be able to run until the CGI module is installed. Add., Deny Edit., X Remove Edit Feature Settings R Help
Configuration: 'localhost' applicationF	10st.config	vil .:



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..."

.NET <u>C</u> LR v	ersion:	
.NET CLR V	/ersion v4.0.30319	×
<u>M</u> anaged p	ipeline mode:	
Integrated	~	

- **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 ¹ Path: /	Web Site	
<u>A</u> lias:	Application pool:	
pa6sharp	PAESharp	S <u>e</u> lect
C:\Program Files (x86) Pass-through authentio <u>C</u> onnect as T	est Settings	
_] LIJable Fleibau	ОК	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.

	Document Name	Submit On	Compatibility
Duke and Duke - Stock Portfolio.txt - Notepad		2014-11-06	8
	Billy Ray Valentine - Quarterly Earnings.txt - Not	2014-11-06	8
	XYZ Company Financials.txt - Notepad	2014-10-02	8
	This is an incredibly long name that i use for tes	2014-10-02	🛛 🚺
	This is an incredibly long name that i use for tes	2014-10-02	8
~			
2	Next		

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:

 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.

- 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:

- 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.

🕞 Print Audit Embedded for)	🙀 Print Audit Embedded for Xerox 1.0.0 Setup		
	Welcome to the Print Audit Embedded for Xerox 1.0.0 Setup Wizard		
	The Setup Wizard will install Print Audit Embedded for Xerox 1.0.0 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.		
	Back Next Cancel		

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

🙀 Print Audit Embedded for Xerox 1.0.0 Setup				
End-User License Agreement				
Please read the following license agreement carefully	Embedded			
SOFTWARE LICENSE AGREEMENT OF PJLM SOFTWARE INC. OPERATING AS PRINT AUDIT ("VENDOR") SOFTWARE LICENSE AGREEMENT SOFTWARE LICENSE AGREEMENT Vendor is willing to license the accompanying Software to you only upon the condition that you accept				
all of the terms contained in this License Agreement and any supplementary license terms included herewith ("Agreement"). READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE SELECTING "Continue" AT THE BOTTOM OF THIS PAGE. YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT.				
IF YOU ARE NOT WILLING TO BE BOUND BY THIS AGREEMENT, SELECT "Go				
I accept the terms in the License Agreement				
Print Back	Vext Cance			

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

🚏 Print Audit Embedded for Xerox 1.0.0 Setup	- 🗆 🗵
Destination Folder PRINT QUDIT	
Click Next to install or click Change to choose another folder. Embedded	
Install Print Audit Embedded for Xerox 1.0.0 to:	
C:\Program Files (x86)\Print Audit Inc\Print Audit Embedded for Xerox\	
Change	
Back Next Can	cel

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

🚏 Print Audit Embedded for Xerox 1.0.0 Setup	×
Print Audit 6 Please enter your Print Audit 6 settings	
Print Audit 6	
Enabled	▼
Print Audit 6 IP Address/Host Name 192. 168.0. 130	Connection Timeout
Communicator Port	Response Timeout
17520 Back	15 Next Cancel

- **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.

Print Audit Embedded for Xerox 1.0.0 Setup Secure Server	
Please enter your Secure Server settings	Embedded
Enabled	•
Secure Server settings	
IP Address/Host Name	
192,100,01100	
Virtual Directory pasecure	
l. I.	

- **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.

🚏 Print Audit Embedded for Xerox 1.0.0 Setup	_	- 🗆 🗵
Print Audit Embedded for Xerox 1.0.0	PRINT AUDIT	
Please select the website to install to	Embedded	
Web site name:		
Defective to the		1
Default Web Site		1
Back	Next Can	el I

8. Click Install to begin installing Embedded for Xerox.

🕞 Print Audit Embedded for Xerox 1.1.0 Setup		- II ×
Ready to install		0
Click Install to begin the installation. Click Back to review or installation settings. Click Cancel to exit the wizard.	change any of your	
Back	Install Can	cel



9. When the installation is complete, click Finish.

📴 Print Audit Embedded for Xerox 1.0.0 Setup		
	Completed the Print Audit Embedd Xerox 1.0.0 Setup Wizard Click the Finish button to exit the Setup Wizard.	ed for
Embedded	Back. Finish	Cancel

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:

💐 Print Audit 6 A	dministration		
<u>E</u> ile <u>E</u> dit ⊻iew <u>T</u>	ools <u>G</u> roups <u>H</u> elp		
🔚 New 🝷 🔚 Ed	it 📕 Save 💢 Delete 🏻 🚱 🕤 (🖲 🐺 Import 🔮 Export 🛛 🔐 🛛 s	er Groups
Main	Embedded Systems		0.
۹	Use this section to add and co walk-up copiers to work with	nfigure embedded systems for y Print Audit 6	rour 🚺
Printer Profiles			
	Copier	Serial Number	Device Type
Printer Paper Sizes			
S			
Printers			
30			
01			
User Profiles			
20			
Users			
Embedded Systems			
Advanced			•

- 1. Run the Print Audit Administration program.
- 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.
- 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.
- 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.
- 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.
- 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)

Add/Edit Embedded for Xerox
Copier name: Save
Serial number: Close
Report as printer:
Report as user:
Authentication type: <pre></pre>
Password: 🔲 Require additional password
Pricing Rompts Advanced
Use custom fields from the user profile if present Allow comments
Disable Exact Matching
Include Custom Field

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.

🚟 Add/Edit Embedded fe	or Xerox			×
Copier name:				Save
Serial number:				Close
Report as printer:				
Report as user:				
Authentication type: <a> 	ie>		-	
Password: 🔲 B	equire additio	nal password		
Pricing Rompts	Advanced			
Display Settings		Admin Crede	entials	
Display Summary Pag	e	Username:		
L		Password:	******	

• 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



DNS or IP:			•	Use SSL
User Name:	admin			Trust Name
Password:				Trust Auth
Service Url:				Trust Expired
				Connect
bservice Versio Registrations —	n: 0.0.0			List Registrations
bservice Versio Registrations	n: 0.0.0	 Checksum		List Registrations Create New
bservice Versio Registrations — Name	n: 0.0.0	Checksum		List Registrations Create New Register Multiple
bservice Versio Registrations	n: 0.0.0	Checksum		List Registrations Create New Register Multiple Create New Webl

- 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:

Registration Detail		X			
Registration Data		_			
Registration Name:	Print Audit Embedded for Xerox				
Native Service					
Service Url:	http://192.168.0.130/PAXeroxEmbedded				
Description Url:	3.0.130/PAXeroxEmbedded/Content/description.xml				
Admin Description:	Print Audit Embedded for Xerox				
Small Icon Url:	0.130/PAXeroxEmbedded/Content/images/icon.png				
Tools Icon Url:).130/PAXeroxEmbedded/Content/images/icon.png				
Vendor:	Print Audit				
Service Capabilities					
XeAccounting					
	Save Load				
	Create Cancel				

(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.

Centreware® Internet Services	XEROX WorkCentre 7835
Status Jobs Print Scan	Address Book Properties Support
Status Welcome	Welcome!
Description & Alerts Billing Information Usage Counters	Welcome to your new WorkCentre. You will have received several packages of documentation materials, which are designed to ensure a fault free installation of the WorkCentre. Please take a moment to review the provided materials before proceeding with the device installation.
Configuration Report Supplies Trays	For additional information, documentation, the latest print drivers, and much more visit: <u>http://www.xerox.com</u>
Information Pages SMart eSolutions	I Have A Cloning File Configure Device Install Later
	Assistance Links
	Software Installation Install Print/Scan Drivers
	🗌 Don't Show Welcome Page Again
	Note 1: All Saved Jobs are stored as encrypted files if encryption of user data is enabled. Encryption ensures that third parties cannot read, print, or scan and email these files. Note 2:
	This device features automatic supplies replenishment, automatic meter read and diagnostics. For more details about these automated services, please visit www.verxy.com/smartesolutions. Refer also to your Xerox sales and maintenance agreements. To discontinue automatic transmissions to Xerox, please <u>click here</u> . To see current status <u>click here</u> .
	Note 3: Third party and open source software disclosure notices and the terms and conditions related to the third party and open source software included with this product can be found on the Support - Drivers & Downloads page for this product at <u>http://www.support.xerox.com/support/</u> .
	xerox 🌍
	©2013 Xerox Corporation. All Rights Reserved. Xerox® and XEROX and Design® are trademarks of Xerox Corporation in the United States and / or other countries.

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)



Centreware® Internet Services	XEROX WorkCentre 7835	👗 admin - Logout Home Index Site Map Help
Status Jobs Print Scan	Address Book Properties Support	
Properties Configuration Overview	Entry Screen Defaults	
Description	Screen Selection	
	Machine's Control Panel	The following features allow you to control what screens are displayed after selecting one of the following buttons on the machine's hard panel: Services, Job Status, and Machine Status.
Network Logs Supplies Plan Activation Code Feature Installation Billing Impression Mode * Alert Notification Software Upgrade * Cognin / Permissions / Accounting Login Methods User Permissions	Services Print Audit Embedded for Xerox	Print Audit Embedded for Xerox
Device User Database		
Security Password Policies Installation Policies McAfee Embedded Control Secure Print Authentication (Login) FEncryption Certificates	Active Jobs Tab	Image: I
Security Certificates Certificate Key Length IP Filtering Audit Log IPsec Timeout & Resume USB Port Security Image Overwrite Security PostScript ® Passwords Hide 'User Name'	Hachine Status Information Tab	

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



Centreware® Internet Services	XEROX WorkCe	entre 7835		👗 admin - Logout Home Index Site Map H
Status Jaka Daiat Com	Address Deels	Decembing	Current	
Status Jobs Frint Scan	Information Tal	rioperties	Support	Contrar Segurt PA Alates R Part To Trans.
Properties Configuration Overview Description General Setup Configuration Report	information fai	J		
Entry Screen Defaults	Default Walku	p Screen		
Paper Management Date and Time Internationalization	The selected so	reen will be the	e default screen displayed when the user walks u	up to the machine.
Extensible Service Setup SMart eSolutions Setup Display Device Information Configure Driver Links Energy Saver Network Logs Supplies Plan Activation Code	Print Audit E Xei	mbedded for		
Feature Installation	Services		Job Status	Machine Status
Alert Notification	Print Audit I	Embedded for 3	Xerox Active Jobs Tab	Information Tab
Software Upgrade	Default Screen	n when Origin	nals are Detected	
▶ Connectivity	The selected so	reen will be au	itomatically displayed when originals are loaded i	l into the document feeder or placed on the document glass. (only when the machine is
✓Login/ Permissions/ Accounting Login Methods User Permissions Accounting Methods Device User Database >Services	in a default st	ate)	▼	
Security Password Policies Installation Policies McAfee Embedded Control Secure Priot				
Authentication (Login)				Apply
	Graphic Key			
Certificate Key Length IP Filtering Audit Log IPsec		Auth	entication Required	DOD: Accounting Required
Timeout & Resume	When these ico	ns are present	, the selected screen will not be initially displayed	ed to the walkup user.
USB Port Security Image Overwrite Security PostScript ® Passwords	Users will need	to complete ar	n authentication and/or accounting procedure bef	efore gaining access to the selected screen.
Hide 'User Name' Software Verification Test				
Solution reac			Xe	erox 🌍
			©2013 Xerox Co	Corporation. All Rights Reserved.

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.



Centreware® Internet Services	XEROX WorkCentre 7835
Status Jobs Print Scan	Address Book Properties Support
Properties Configuration Overview Description • General Setup	Xerox Secure Access Setup Manual Override Server Communication
Cloning Entry Screen Defaults Paper Management Date and Time Internationalization Extensible Service Setup SMart eSolutions Setup Display Device Information Configure Driver Links Energy Saver	IPv4 Address IP Address: Port Host Name 192 . 168 . 0 . 130 : 443 Path /PAXeroxAuthentication/Server.asmx Embedded Enabled Version: usbreader Version 1.0.15
Network Copy Supplies Plan Activation Code Feature Installation Billing Impression Mode Alert Notification Software Upgrade Connectivity	Oevice Log In Methods
▼Login/ Permissions/ Accounting Login Methods User Permissions Accounting Methods Device User Database	Accounting Information (Requires Network Accounting) Automatically apply Accounting Codes from the server User must manually enter accounting codes at the device
Services Services Security Password Policies Installation Policies McAfee Embedded Control Secure Print Authentication (Login) PEncryption Certificates Security Certificates Certificate Key Length IP Filtering Audit Log IPsec	Device Instructional Blocking Window Window Title (Reference 1) Authentication Required. Instructional Text (Reference 2) Please sign in with the Xerox Embedded application to continue. Image: Second Device Text (Reference 2) Image: Text (Reference 2)
Timeout & Resume USB Port Security Image Overwrite Security PostScript ® Passwords Hide 'User Name' Software Verification Test	Close Undo Save

- 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.



Centreware® Internet Services	XEROX WorkCentre 7835	å admin - Lo	gout Home Index Site Map Help
Status Jobs Print Scan	Address Book Properties Support	_	
Properties Configuration Overview Description * General Setup Configuration Report Cloning Entry Screen Defaults Paper Management Date and Time	Login / Permissions / Accounting > <u>Accounting</u> User Accounting Prompts Prompt Options Presets No Prompting		
Internationalization Extensible Service Setup	Services No Prompt	Prompt	Color Prompt Only
SMart eSolutions Setup Display Device Information Configure Driver Links Energy Saver Network Logs	Copies Image: Copi	0	0
Supplies Plan Activation Code	Fax [Prompt Only; No Usage Capture]		
Billing Impression Mode Alert Notification Software Upgrade Connectivity Cogin/ Permissions/ Accounting Login Methods User Permissions	Note When 'No Prompts' option is configured for other services, then generic codes will be used if accounting codes do no	ut exist in jobs.	Cancel Save
Accounting Methods Device User Database Services Security	xerox 🔊		
 Password Policies Installation Policies McAfee Embedded Control Secure Print Authentication (Login) Encryption Certificates Security Certificates Certificate Key Length IP Filtering Audit Log IPsec Timeout & Resume USB Port Security PoatScript @ Passwords Hide 'User Name' Software Verification Test 	©2013 Xerox Corporation. All Rights Reserved. Xerox® and XEROX and Design® are trademarks of Xerox Corporation in the United States and / or other countries.		

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.



.

Connections		DOV 2000	Hama						Actions
Q- 🗔 🖄 😣		RUX-2008	Home						Open Feature
Start Page	Filter:		- 00 00 -	Show <u>A</u> ll G	roup by: Area		•		Manage Server
Application Pools	ASP.NET							-	Z Restart
E 🚱 Default Web Site	1ED			۷	-	1	Pab		Stop
	.NET Authorizati	.NET Compilation	.NET Error Pages	.NET Globalization	NET Trust Levels	Application Settings	Connection Strings		View Application Pools View Sites
	9		2	2					Change .NET Framework Version
	Machine Key	Pages and Controls	Providers	Session State	SMTP E-mail				Help Online Help
	IIS								
		2	CGI	Ð	0	1	404		
	ASP	Authentication	CGI	Compression	Default Document	Directory Browsing	Error Pages		
				3	3		-		
	FastCGI Settings	Handler Mappings	HTTP Respo	ISAPI and CGI Restrictions	ISAPI Filters	Logging	MIME Types		
	4		8		2				
	Modules	Output Caching	Request Filtering	Server Certificates	Worker Processes				
	Managem	ent							

- 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.

Create Self-Signed Certificate	? ×
Specify Friendly Name	
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:	1
Specify a friendly name for the certificate:	
OK	Cancel

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".
- Under "Actions --> Edit Site" (located on the right hand side of the IIS Manager), click on " Bindings..."

ype	Host Name	Port	IP Address	Binding	Add
tφ		80	*		Edit
					Remove
					Browse
				•	

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

Туре	Host Name	Port	IP Address	Binding	Add
http		80	*		Edit
Add	Site Binding				?×
Т	ype:	IP address:		Port:	
h	ttps 💌	All Unassigne	ed	443	
Н	ost name:				
	SL certificate:				E
X	erox Embedded App	olication		View	1
					Pa

- 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="ServerlpAddress" 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)





✓ Entry Screen Defaults × ← → C ▲ Not secure Mag	w//192.168.210.5/svc_reg/sc	veen_defaults.php				enst – Ø ×	
xerox 🕥	Xerox [®] AltaLink [®] C8030				admin-Logout		
<u>.</u>	_	2	2	Address Dook		<u>.</u>	
Search	Entry Screen	Defaults					
Configuration Overview Description Configuration Report Configuration Report Configuration Report Exclup & Restore Settings Experi Management Date and Time Status LEO & Sounds Internationalization Edensible Service Setup Remote Service Setup Dapity Device Information Configure Direct Initis Energy Saver Supplies Plan Admitton Code Feature Instatistion Billing Impression Mode Holdtacion Settings Schmare Upgrade + Connectivity + Login' Permissions' Accounting + Appe	Default Walkup Screen The selected screen will Home Default Screen when The selected screen will None (Take No Act	n II be the default screen displayed whe	n the user walks up to the machin	e. nt feeder or placed on the documen	t plass. (only when the machine is i	n a default state)	
						Apply	

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".

xerox 🍞		1	Xerox [®] AltaLink [®] (C8030		🌲 admin-Logout		
<u>.</u>	and the second s	2		Address Dook		<u>.</u>		
Search	88							
Configuration Overview Description	Login Methods							
General Setup	Control Panel & Website Lo	gin Methods				Edt.		
*Login/ Permissions/ Accounting Login Methods User Permissions Accounting Methods Device User Database Acces		Control Panel Login User Name / Password Validate on the Device		8	Website Login User Name / Password Validate on the Device			
+ Security		Personalized User Prof Enabled Retrieve Profile Logged-In User	tile Information for the					
	Configuration Settings	Method		Status		Action		
	Device User Database	Control Pi	anel & Website	Required; 1	Vot Configured	Edt.		
	LDAP Servers	Personals	ced User Profile	Required;	Configured	C Edt.		
	Log Out Confirmation	Control Pr	anel	Coptional; C	onfigured	Z Eat		
	Graphic Key							
	m							

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



∫ Edit Login Methods x ← → C ▲ Not secure	Mtps://192.168.210.5/aaa/athr/c	hoose.php?from=Athn_Home				0mi - 0 ×		
xerox 🍞		Xerox [®] AltaLink [®] C8030				admin-Logout		
<u>.</u>	<u></u>	2		Address Dook		<u>.</u>		
Search Configuration Overview Description > Connectivity > Connectivity	52 / Login Methods Edit Login Methods Control Panel & Webs Image: Image	rthods te Login Methods Control Panel Login Xerox Secure Access - L Website Login User Name / Password - Autor Autor S 2 5	Unified ID System	ation for authenticated LDAP users: Fax recipients.		Cancel Save		

- 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.

Authentication Server X ↓ ← → C ▲ Not secure ↓ MI	er × @soat - 0 × secure Mtgss//192.168.210.5/auth/config/issaManualSetup.php]								
xerox 🍞	Xerox [®] AltaLink [®] C8030					💄 ad	admin-Logout		
<u>.</u>	<u>.</u>	2		Address Dook		441		<u>.</u>	
Search	Server Communication								-
Configuration Overview Description In General Setup	IPv4 Address Host Name			IP Address: Port 192 . 168 . 210	. 2	: 443			11
+ Connectivity	Path								
*Login/ Permissions/ Accounting	/PAXeroxAuthentication	Server asm							
User Permissions Accounting Methods Device User Database P Appa > Security	Embedded Enabled Version: 1.0.24								
	Device Log In Methods								
	Xerox Secure Access D Xerox Secure Access D	rvice Only (e.g., Swipe Cards) rvice + alternate on-screen au	thentication method						
	Accounting Information (R	equires Network Accounting	a0						- 1
	 Automatically apply According to the second s	ounting Codes from the server r accounting codes at the dev	ice						
						Clos	e Undo	Save	
			60018 Xeros C Xeros R. Xeros en De Xeros Corporation in th <u>Home</u> I	orporation. All Rights Reserved. sign8 and Ahu, ive8 are trademarks of a United States and I or other opurtries. Index 1 Statistica 1 MidL.					

• 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.

Accounting Methods X ← → C ▲ Not secure	6mi - 0 ×							
xerox 🕉 Xerox® AltaLink® C8030						admin-Logout		
	<u>_</u>	2	2	Address Dook	아이아이아이아이아이아이아이아이아이아이아이아이아이아이아이아이아이아이아이	٩		
Search Configuration Overview Description • Cenneral Setup • Connectivity • Copin Permissions / Accounting User Permissions Overview (Second Second Overview (Second Second Pages • Apps	55 Accounting N Control Panel & Webs Configuration Setting None (Disabled)	lethods te Login Methods Accounting Method None Status	42018. Kens Kensell, Kens and D Xanse Corporation in P Kinn 1	Acts Supportion, All Fights Reserved. report and Adocured are technological of a to Orient Status and i or other sources. Totake 1 Status One 1 Statu.	0 6			

10. Set the Accounting Method to "Network Accounting". Click on 'Save' to return to previous screen. (Select Accounting Methods)





C Edit Method x ← → C ▲ Not secure Mitput	//192.168.210.5/aaa/acct/	choose.php?from=Acct_Home				theat - Ø X
xerox 🕥		x	(erox [®] AltaLink [®] C	8030		admin-Logout
<u>.</u>	and the second s	2	.	Address Book	다. Properties	۹
Search Configuration Overview Description • CennetCitity • ConnetCitity • Configuration ConnetCitity • Configuration Contention Contention Version Ver	Edit Method Method	Current Accounting Method None None Network Accounting Xerox Standard Accounting Auxiliary Access Device	4018 Janua Januari, Januari Januari, Januari Januari Januari Januari	Separation AD Pipto Reserved. sports and Adactively are todeworks of childed Dates and (-) or other todeworks. Dates 1 Sate Mate 1 Cate		Cancel Save

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

Accounting Workflow × ← → C ▲ Not secure Mag	/192.168.210.5/aaa/acct/net</th <th>work/jba_tracking.php?from=A</th> <th>cct_Home</th> <th></th> <th></th> <th>Brat -</th> <th>σ×</th>	work/jba_tracking.php?from=A	cct_Home			Brat -	σ×
xerox 🍞		x	erox [®] AltaLink [®]	C8030		nin-Logout	
<u>.</u>	<u>_</u>	2	2	Address Dock	- 	<u>_</u>	<u>.</u>
Search	88 / Accounting						
Configuration Overview Description	Accounting Wo	orkflow					
Description General Setup Connectivity *Login/ Permissions/ Accounting	Job Types	Impacted.	Арря	Accounting Workflow			
	Copy Jobs	🖸 🖸	1	Capture Usage	•		
Login Methods User Permissions	Print Jobs	E 6		Capture Usage	•		
Accounting Methods Device User Database	Scan Jobs	e* -	00	Capture Usage	•		
+ Security	Email Jobs	2		Capture Usage	•		
	Server Fax Jobs	C		Capture Usage	•		
	Internet Fax Send Jobs			Capture Usage			
	Internet Fax Receive Jobs			Capture Usage			
			42018 Xa Xaros Xaros an Xaros Corporato Eta	es Corporation. All Rights Reserved. Designifi and Alac, and are trademarks of the Collect Dance and for other invertices. In 1 Index 1 Sec. March 1999		Cancel	Save

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



✓ Üser Accounting Prompt: X ← → C ▲ Not secure	https://192.168.210.5/aaa/acct/re	twork/prompts.php?from=Ac	ct_Home						enat – Ø ×
Xerox 🔿 Xerox® AltaLink® C8030							admin-Logout		
<u>.</u>		2			A-33	8 ress Dock			٩
Search	88 / Accounting								
Configuration Oven/ew Description In General Setup In Connectivity **Login / Permissions/ Accounting Login / Refructs User Permissions Accounting Methods	User Account Prompt Options Presets No Prompting Apps	ing Prompts					No Prompt	Prompt	Color Prompt Only
Device User Database > Apps	Copies ¹			6				•	
Security	Prints						۲	0	0
	Scans		20				۲	0	
	Note 1) Prompts are always r Copy When %o Prompts' optic	tains							Cancel Save

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

B Security Certificates x € → C ▲ Not secure Maps://192.168.210.5/properties/security/certList.php?tab=defCert							
xerox 🍞	Xerox [®] AltaLink [®] C8030						
<u>.</u>	ê (2	Address Dook		<u>e</u>		
Search Configuration Overview Description + Connectivity + Connectivity + Cognin Premissions' Accounting + Appe = Security + Password Policies Institution Policies Mothe Embedded Control Becure Print	Xerox Device Certificate Xerox Device Certificate CAS The default device certificate was created b Click Create New Xerox Device Certificat Create New Xerox Device Certificat Friendly Name	agned Device Certificate(s) RootInterme y this device to validate its identity and to enable en to modify the values that are used when generatin difficate Download the Device Root C	Siele Trusted Certificate(s) Domain rypled communication. new certificates. ertificate Authority 040 Statu	Reset to Machin Controller Certificate(s)	e/Device Factory Defaults		
Encrystion Elcope Cestificates Scontry Cestificates Cestificates Cestificates Cestificates Prevent Prevent Prevent Scontry Cestificates Cest	Default Xerex Device Certific Note A valid device certificate is recommen Xerex Device Certificate installing the Download the Device Root Certificate Device Root Certificate Authority insta	ate HTTI 502: 502: Ema OCC OC Any Ided to access some device webpages. The Dev e Device Root Certificate Authority will resolve m Authority eliation individions	*S Server, X Claent, I Encryption, Valid P Signing, Valid co Root Certificate Authority can be used out "untrusted certificate" web browser enc	27-Nov-2022 by client browsers to create a valid cer rs.	MeerEused		
		42018 X	erce Corporation, All Rights Reserved.				

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="ServerlpAddress" 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

C 🕘 👩 http://192.168.210.13/apps/inc	sex/htmi/HushConnectk D = C 🧭 Internet Services 🛛 🖸 🔁	ය 🗇 😌
	Xerox [®] VersaLink™ C400DN Printer	🛃 Admin 🗸
🔒 Home	EIP Settings	
Apps	Extensible Interface Platform	
	EIP Browser	
a Jobs	Version: X2/G_6.4.1_538.1_010_01.00.00 Widget Version: v1.3.17 c8	
🔊 Connectivity	Allow ConnectKey App Install	 III
Sermissions	Verify Server Certificates	
	Export Password to EIP Apps	
• System	Use Device Proxy Server	Not Setup 🔽 📗
	EIP Web Services	
xerox 🍞	© 2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States an	d/or other countries.



2. Click on "EIP Web Services". Under "Authentication and Accounting" ensure "Xerox Secure Access" is enabled

@	🗧 💮 🧭 http://192.168.2120.13/sppp/index.htmi#hushConnectix 🔎 = C 🖉 foteernet Services 🛛 X 🖸 🗑							
			Apps		Admin 🗸			
A		BB / EIP S	Job Management Extension	 III 				
	Apps		Print Extension	 Image: Image: Ima				
_		EIP Browser	Hardware					
-		Widget Versio	Card Reader Access	 III 				
609	Connectivity	Allow Connec	Mass Storage Access	 III 	Image: A state of the state			
2.		Verify Server	Authentication and Accounting					
-		Export Passw	Configuration	 III 				
•	System	Use Device P	Job Limits	 III 	Not Setup 🔽 💷			
		EIP Web Serv	Session Data	 III 				
			Xerox Secure Access	 Image: Image: Ima				
			Security					
	xerox 🕥	© 201	Certificate Management and Security Configuration	 III 	vation in the United States and/or other countries.			

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)

C () (ttp://192.168.210.13/apps/int	- O × ④ (2) http://192.168.210.11/apps/index.htmi#hashApps . P * C) (2) Internet Services × 口 日								
	Xerox® VersaLink™ C400DN Printer SAdmi								
🔒 Home	448	P							
Apps	Preferences	EIP Settings							
a Jobs	Inst	alled Apps							
Connectivity	CapturePoint								
Sa Permissions	Device								
System	Jobs								
	Print Audit Embedded for Xerox								
	Print and Scan for Box								
	Print and Scan for Dropbox								
Xerox 🕥 Protec	ted mode is turned off for the Internet zone.	on't show this message again I um on Protected mode 🛛 🗙							

2. Under the "Walkup Screen" section select "Print Audit Embedded for Xerox" from the dropdown



G	D 6 http://192.168.210.13/apps/ind	deulteniihhushPreference D = C 🧭 Internet Services X 🛄 🔁	- 0 × @ \$\$ @ \$
		Xerox [®] VersaLink™ C400DN Printer	🛃 Admin 🗸
ŵ	Home	Preferences	
	Apps	Walkup Screen	
		What should the default Device Control Panel screen be for a walkup user?	
-	Jobs	Print Audit Embe 🗸	
62	Connectivity		
2	Permissions		
•	System		
	xerox 🍞	© 2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or othe	r countries.

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

C () () https://192.168.210.12/system	n/inde ,D = 🛛 Certificat	t er C 🥑 Edit Login Methods 🧭 Internet	Services × Q Edit Printer	🥭 Server Web Service	- 0 × C 2 0 ☆ 0 0
		SSL/TLS Settings			Admin 🗸
A Home	🔘 / Secu	TLS 1.0			
EE Apps	Firmware Veri	TLS 1.1			Off
Address Book	Feature Enab	TLS 1.2			
	Customer Ser	Select at least one protocol.			Off
- Jous	Security Certit	Device Certificate - Server	CN=XC-68D439		
5 ⁵⁹ Connectivity	Automatic Sel	HTTP - SSL/TLS Communication	Image: A start of the start		On
Permissions	Certificate Pat	HTTP - SSL/TLS Port Number	1-65535 443		Off
O System	Certificate Re	LDAP - SSL/TLS Communication	1		
	Smart Card	SMTP - SSL/TLS Communication	Disabled		Off
6		Verify Remote Server Certificate	Not specified		
xerox 🔊	FIPS 140-2	Tony remote derver derutate			Off

4. Click on Permissions from the left Menu. Select "Accounting Method" and click Edit next to " Network"



()	https://192.168.210.12/permiss	ions ,Ω = 🔵 Certificate e G	🥑 Edit Login Methods	🩆 Internet Services	× Ö Edit	Printer	🥖 Server Web Service	- • ×		
			Xerox [®] V	ersaLink™ B405D	N MEP			🎦 Admin 🗸		
• H	lome	-	No Accounting	ACCO	unung meur	ou				
88 A	lpps	M	There are	There are no limits to the number of prints or scans a user can make.						
8 .	ddress Book	^	Xerox Standard	d Accounting						
4 ه	lobs		Track Dev	vice usage and optio	nally set sca	n and print limits	L.	Select		
6 9 0	Connectivity	✓ 痯	Network					Edit		
2 6 P	Permissions		 Tracking [Tracking Device usage. 						
• s	System	Ē	Auxiliary Device	e managed by separa achine or a payment	ate hardware t-card reader.	such as a coin⊣	operated Auxiliary	Select		
				Accounting and	d Billing Dev	vice Settings				
x	erox 🌖				Edit					

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"

C () (Http://192.168.210.13/permissi	ons/index.html#hashAc	P = C Ø Internet Services ×	9			– ଅ <mark>×</mark> ଜନ୍ମ ବି
			Liser ID		a cast manc.	😫 Admin 🗸
🛖 Home		Default Label	036110	UserID	_	
EE Apps		Default Value			-	Select
🖨 Jobs		Ask Users		1	its.	
-		A	ccount ID			
5° ² Connectivity	× I	Default Label		AccountID		Edit
Permissions		Default Value				
System		Ask Users		1	t-operated Auxiliary	Select
		Whe	n to Prompt			
		Select which functions will displa	ay the prompt.			
		Print		No Pror	mpt	
xerox 🕥	© 20	77 XANDAR Composition - All rights resourced - Xanon	Ca	ancel OK	n Corporation in the United States and	or other countries.

6. Select "Permissions" from the left Menu. Click on the "Login/Logout Settings".



🗲 🛞 🧭 https://192.168.210.12/permis	poors D = Q Certificate er_ C 🧭 Internet Services X 🖸 😌	- 8 × @☆©©
	Xerox [®] VersaLink™ B405DN MFP	🛃 Admin 🗸
🔒 Home	San / Login/Logout Settings	
BB Apps	Login Method	
2 Address Book	Simple Easy login - passwords are not required Pick User Names from the list or type in User Names	Select
🚔 Jobs	Local	
Connectivity	Basic security - passwords required Pick User Names from the list or type in User Names	Select
Permissions	Network	
System	Basic security with authentication handled by a remote server Enables the use of same login information on multiple devices Device User Accounts are used only for personalization and permissions.	Select
xerox 🌖	Convenience Basic security made easy Swipe or tap your card to log in Device User Accounts are used only for personalization and permissions.	Edit

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.

(i) 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.

Reh							
	Application Pools						Actions
8							Add Application Pool
age	This was a late or state and second at	test of events where we also		-the time and a second	and the state of t		Set Application Pool Defa
08 (************************************	applications, and provide isolation among	different applications.	er die bei ver. Ap	picatori pools are a	sociated individual proc	esses, contain one or more	Help
pication Pools	Elter:	- Chan Al Grau	but No Crevel				Online Help
	New 1	Sitist Bi Land	New Coroupi	Managed Marali	Transta.	Anderstein	
	ASP NET v4.0	Started	v4.0	Integrated	ApplicationPoolIden	Applications	
	ACD NET v4.0 Classic	Started	v4.0	Classic	ApplicationPool(den		
	Classic NET AppRod	Started	v7.0	Classic	ApplicationPoolIden	0	
	DefaultanPool	Started	v2.0	Integrated	ApplicationPoolIden	1	
	PAXEAuthAppPool	Started	v2.0	Integrated	NetworkService	1	
	PAXEMainAppPool	Started	v4.0	Integrated	NetworkService	1	
		500 000				-	

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

Edit Application Pool
Name:
PAXEAuthAppPool
.NET Framework version:
.NET Framework v2.0.50727
Managed pipeline mode:
Integrated 💌
Start application pool immediately
OK Cancel

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.

Help											
0	🔍 /PA	XeroxAut	thenticatio	n Home							Actions
83											🔬 Explore
(*************************************	Filter:		• #1 Go • •	Show All G	roup by: Area		•				Edit Permissions
ation Pools	ASP.NET										Basic Settings
efault Web Site	iiio	1				TE	4	1	1	2	View Virtual Director
aspnet_client	NET	NET	NET Error	NET	NET Profile	NET Roles	NET Trust	NET LISERS	Application	Connection	Manage Application
PAXeroxEmbedded	Authorization	Compilation	Pages	Globalization			Levels		Settings	Strings	Browse Applicati
	(des	and the second s		0							Browse *:443 (http)
	Machina Kay	Races and	Brouidare	Contino State	CMTD E mol						Advanced Setting
	Middline Key	Controls	FIOVIDEIS	36551011 31816	SPITE Childe						Help
											Online Help
	IIS	~		10.000			-			1000	
	0	2		HE O	404		(HBC)		12		
	Authentication	Compression	Default	Directory	Error Pages	Handler	НТТР	Logging	MIME Types	Modules	
	-		Document	browsing		Mappings	Kespo				
		8	Q								
	Output	Request	SSL Settings								
	Caching	Filtering									
	Manageme	nt									
	Editor										

- 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...



Edit Application	<u>? ×</u>
Site name: Default Web Site Path: /	
Alias: Application pool:	
PAXeroxAuthentication PAXEAuthAppPool	Select
Example: sales	
Physical path:	
C:\Program Files (x86)\Print Audit Inc\Print Audit Emb	
Pass-through authentication	
Connect as Test Settings	
ОК	Cancel

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.

Die Den Bop		
Connections	SVR2008 Home	Actions Manage Server
Sart Page Sart Page	File: Image: Configuration File: Form File: Form APT APT APT APT APT<	Creatert Stort Stor Year Application Pools Vera Sites Change, HET Framework Versite P Halp Online Halp

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


HINTER INFORMATION Services (IIS)	Manager				_ 8 ×
(3) (1) SVR2008 ►					😰 🖂 🟠 I 🔞 •
Ele View Help					
Connections				Alerts	
🔍 - 🗔 🖄 😣					module is not installed.
Start Page	Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.			applicati	ons that are allowed to
Application Pools	Group by: No Grouping			run, but run until	they will not be able to the CGI module is
E Sites	Description A	Restriction	Path	installed.	·
E go Default web site	ASP.NET v2.0.50727	Allowed	%windir%\Microsoft.NET\Framework64\v2.0.50727\aspnet_isapi.dll	Actions	
Aprice diam	ASP.NET v2.0.50727	Allowed	%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll	Add	
PAXeroxEmbedded	ASP.NET v4.0.30319 (32-bit)	Not Allowed	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dl		
	ASP.NET v4.0.30319 (32-bit)	Not Allowed	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dl	Allow D	6
				Eot	•
				× Remove	
				Edit Feat	ure Settings
				🔞 Help	
				Online He	alp
	Territory Manual Constant M				
Configuration: localnost applicationHost.conf	hg				1

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