



Integration with



Issue : 1.4

Prepared by

Stephen Jobs

Canon Europe Limited (CEL)

e-mail: stephen.jobs@canon-europe.com

Phone: +44 (0)208 588 8148

Fax: +44 (0)208 588 8001

EcCopy & NT Ware Integration Guide

Contents

Contents	2
Revision History	3
Introduction.....	4
Installation Procedure	4
eCopy Setup.....	4
uniFLOW OM Setup.....	13
Entering user details using the Login Manager	15
Versioning.....	18
Trouble shooting	19
Support & Escalation.....	22

ECopy & NT Ware Integration Guide

Revision History

Issue	Date	Details	Author
1.0	2/11/07	First Release	Stephen Jobes
1.1	7/12/07	Updated with feedback from ECNC	Stephen Jobes
1.2	13/12/07	Updated the versioning for integrating with a uniFLOW OM RPS	Stephen Jobes
1.3	25/01/08	Updated after CEL Print Fleet roll out	Stephen Jobes
1.4	8/04/08	Difference with eCopy v4.2	Stephen Jobes



Ecopy & NT Ware Integration Guide

Introduction

This is a generic setup guide for the eCopy and NT-ware integration. For the purpose of this procedure the setup included the following hardware/software:

With the release of eCopy v4.2 the ID service has been integrated into the core software so it is no longer necessary to use and run the SSOP41_Uniflow_CEL.exe to enable this.

Canon:

1 x iR C3380

eCopy:

eCopy SSOP version for Canon MEAP devices V4.1.0.28 running the Exchange (Microsoft Exchange 2003) and Scan to Desktop Connectors in a Windows 2003 Active Directory Environment. Please note that since the release of version 3 of eCopy the Administration console settings are the same regardless of whether the device is running with the SSOP (MEAP) client or with a ScanStation.

NT-ware:

uniFLOW Output Manager Edition V3.1.1

miniMIND Mifare Card Reader Set

Login Manager v.2.0

Please note that this only a sample configuration, to ensure the correct set up for your ID system please refer to the uniFLOW OM v.3.1 User Manual.

Final Purpose:

The main functionality is that a user can walk to a Canon MFP, identify them self (e.g. swipe their proximity card) and authenticate once against uniFLOW OM and be automatically authenticated on eCopy reducing the need to enter two sets of authentication information and thus making the use of the MFP and solutions easier for their employees.

Installation Procedure

Note: The following steps are no longer necessary if eCopy v4.2 is being used

In order to configure the integration between uniFLOW OM and eCopy the following files were provided by eCopy:

eCopy Setup

eCopy supplied files:

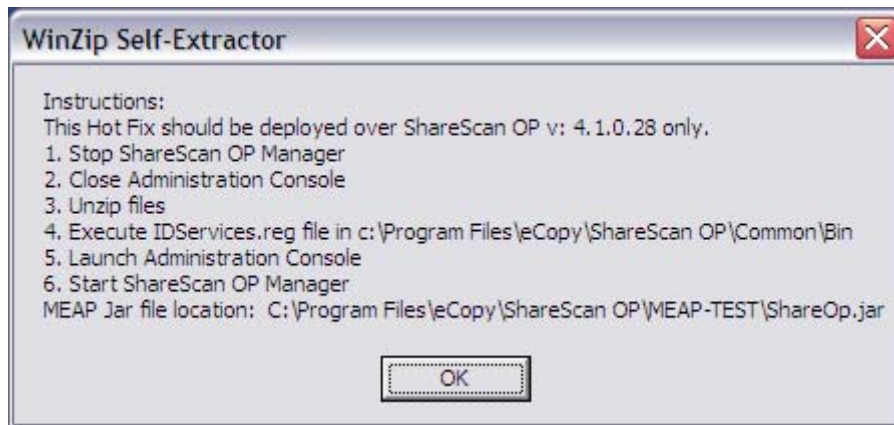
SSOP41_Uniflow_CEL.exe

The ID Service is part of the ShareScan 4.1 product but is not exposed as standard so as not to cause confusion in the cases where uniFLOW OM was not being installed. The "ID security

Ecopy & NT Ware Integration Guide

services” is only fully tested with uniFLOW OM v3.1.1 and above at this time.

Run this executable on the eCopy server which will provide the instructions that need to be followed as shown below:



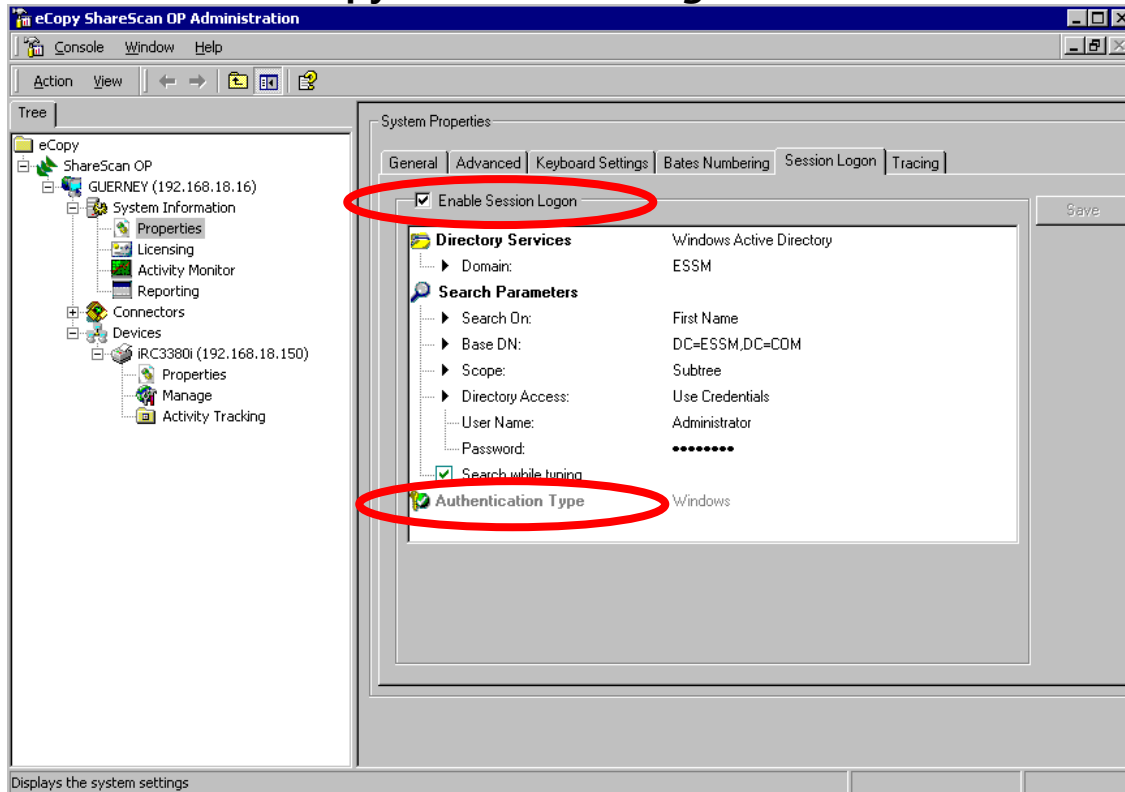
N.B. Please follow the instructions shown by running the SSOP41_Uniflow_CEL.exe extractor (shown in the above screen shot)

Please be aware that for the purpose of setup it is best to get eCopy working first before adding the uniFLOW OM identification mechanism. eCopy provides an emulator that simulates authentication information being passed to the SSOP or ScanStation session logon. If this is working then the uniFLOW OM setup is minimal.

Note: If using eCopy v4.2 continue with the steps below.

Once the above patch has been applied, within SSOP Administration enable Session Logon so that users are required to log onto the eCopy device with their AD credentials. Ensure that the 'Search while typing' check box is selected.

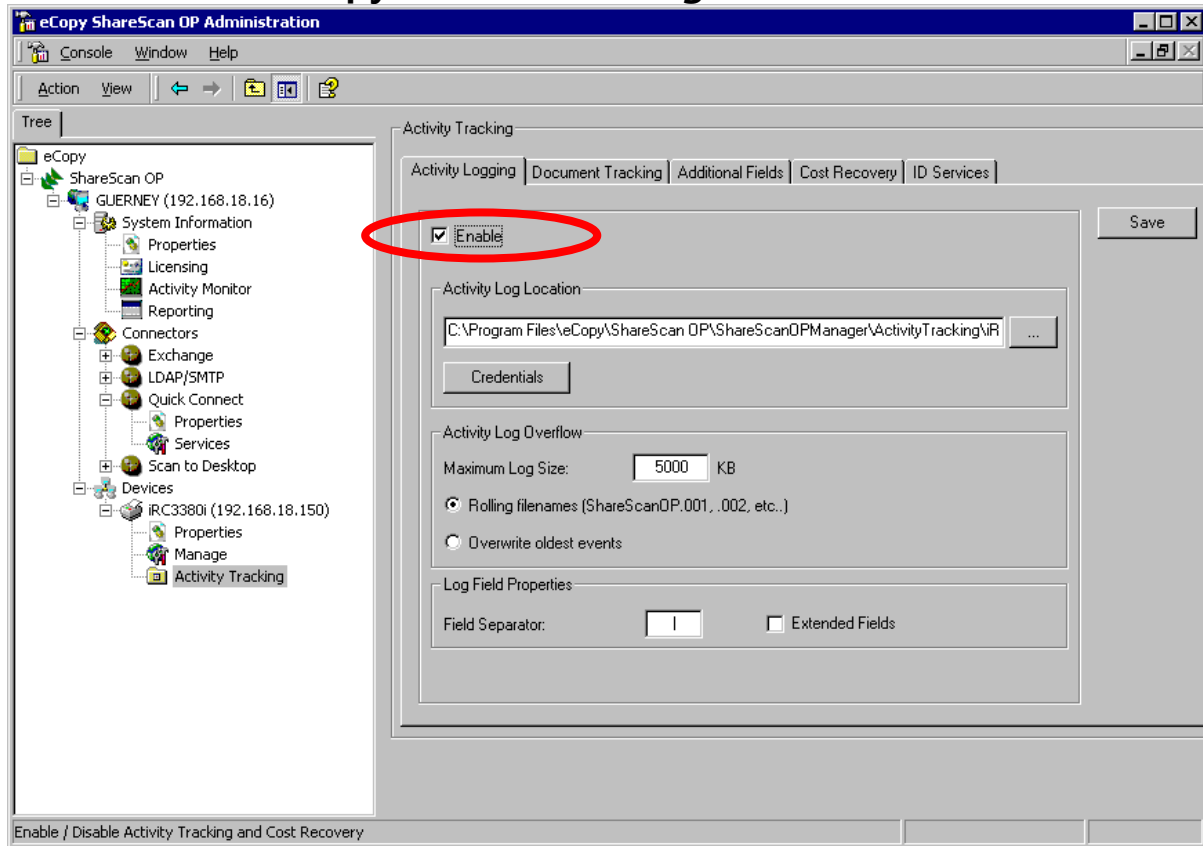
ECopy & NT Ware Integration Guide



Once a user logs on they are then identified to the Exchange, Scan to Desktop or Quick connectors. This is dependent upon which connectors have been setup in the Admin console.

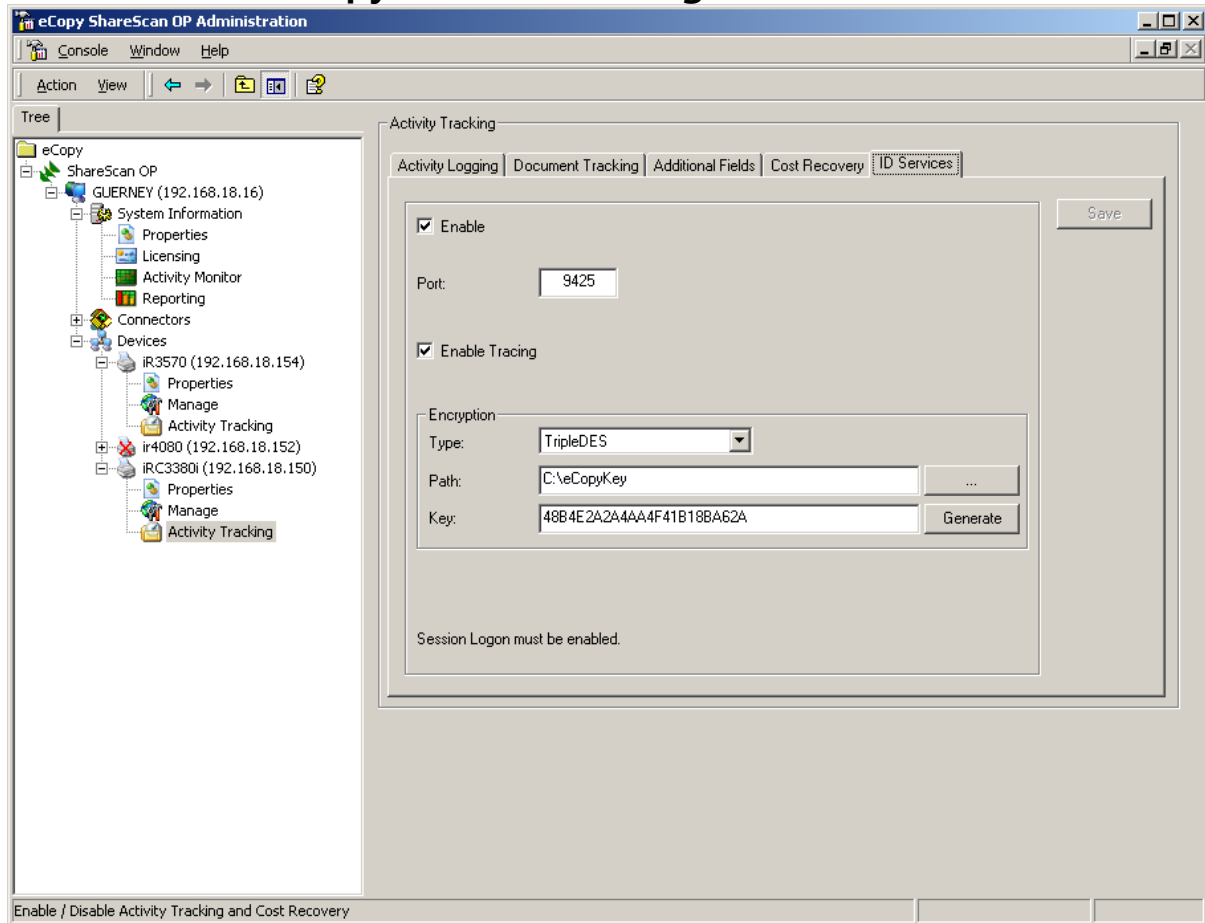
Under the 'Devices' configuration tab in the eCopy administration console, you have to enable 'Activity logging'. You'll also notice that a new tab has been created called the 'ID Service'

ECopy & NT Ware Integration Guide



Under the 'Identification Service' tab check the box to enable this service and simply select the encryption type as required. Pay particular attention to the path of the encryption key as this is important for the uniFLOW OM setup.

Ecody & NT Ware Integration Guide



By default the communication port is set to 9425, this is also auto filled in the uniFLOW OM device agent but could be changed if required. For the purpose of testing it's best to leave this as is.

There are two options for encryption, either none or TripleDES. If 'none' is selected then the transfer of the authentication details from uniFLOW OM to the eCopy Administration Console will be in clear text. It is highly unlikely that this will be used unless for trouble shooting purposes.

Assuming that the encryption will be TripleDES, it's necessary to select a path or location where the encryption key will be saved on the eCopy Administrator PC. After that simply select 'Generate' and a text file will be created in the location specified in 'Path' with the hex notation key.

Pay particular attention to the path of the encryption key as this is important for the uniFLOW OM setup. It is also advised to use the same file path if multiple devices are being configured.

Essentially the eCopy configuration is complete but it's beneficial to test this before configuring uniFLOW OM. The installation of the ID Services also installs an emulator which can verify that this configuration is working.

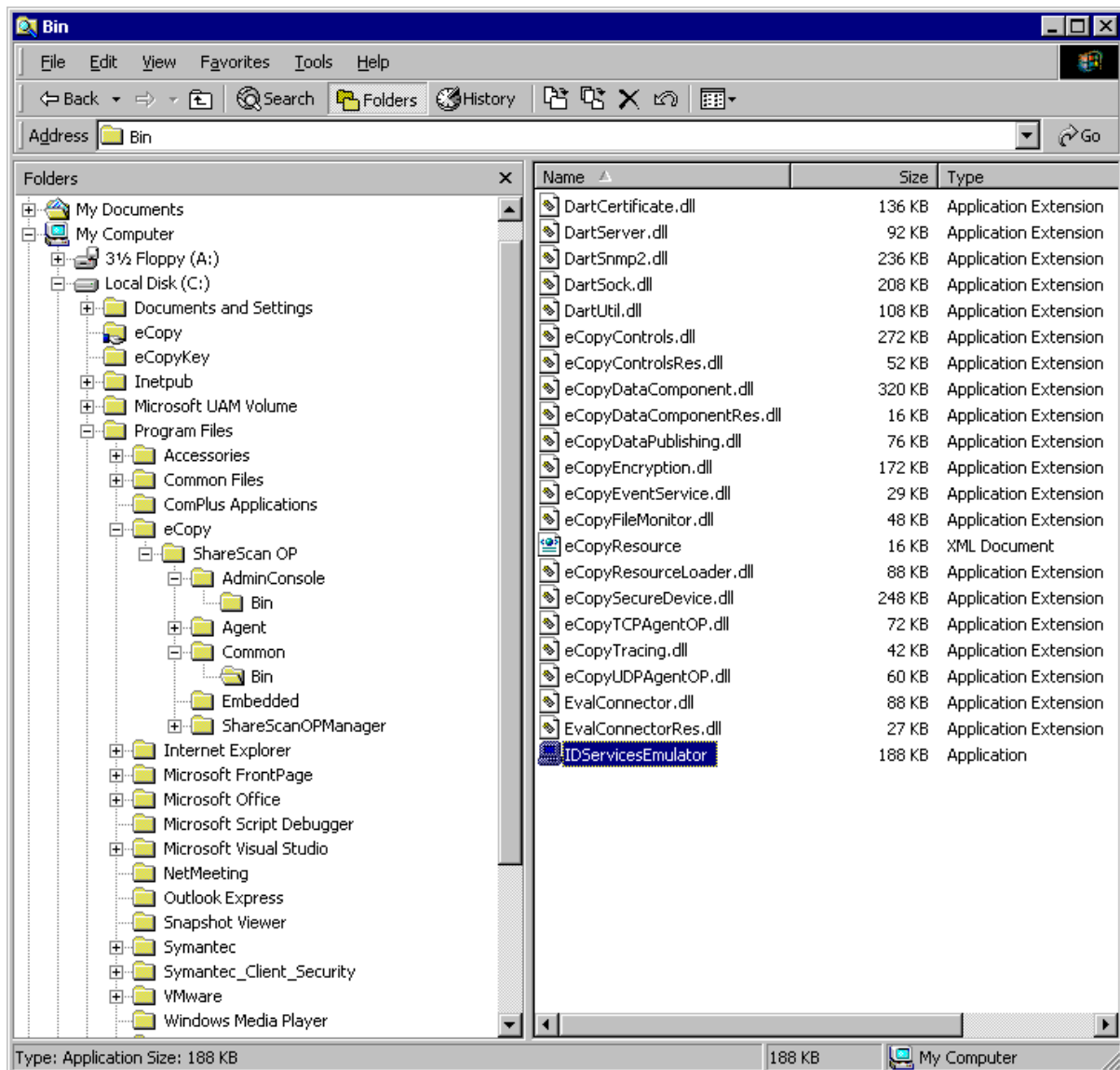
Ecopy & NT Ware Integration Guide

NB. If the setup is using a ScanStation then it is not possible to 'test' the configuration with the IDServiceEmulator. This is due to the fact that the 'ScanStation Client' has to be running on the ScanStation which means that it's not possible to run or view another application.

On the Sharescan Administration PC browse to:

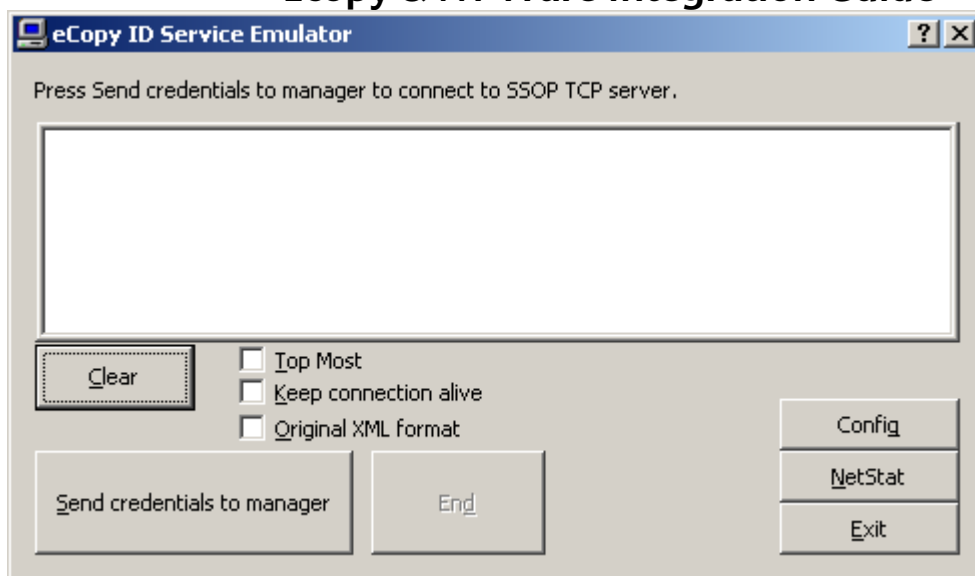
C:\Program Files\eCopy\ShareScan OP\Common\Bin

Run the 'IDServiceEmulator'

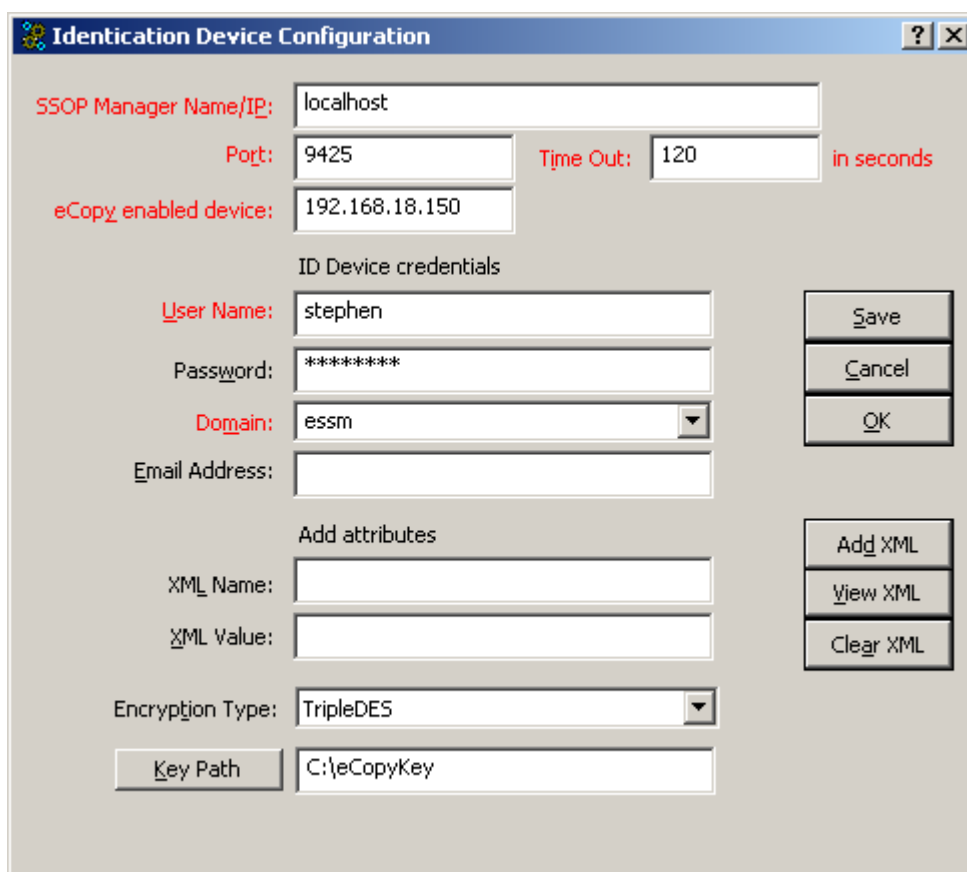


This will launch the emulator as shown below.

Ecopy & NT Ware Integration Guide



To configure this select 'Config' which brings up the screen below.



Ecopy & NT Ware Integration Guide

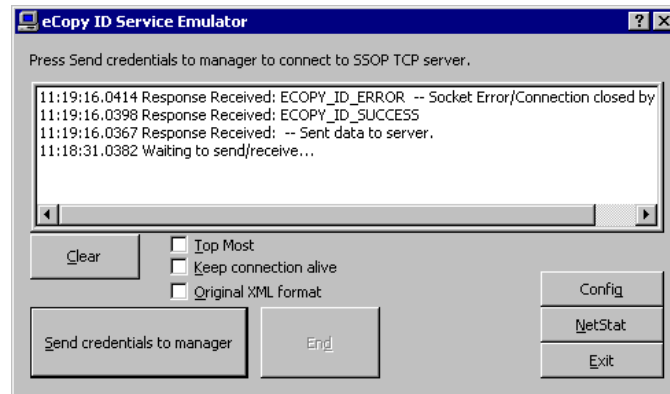
The parameters that need to be specified in the 'Identification Device Configuration' are as follows:

- **SSOP Manager Name/IP:** Enter the IP address or the DNS name of the SSOP Manager
- **Port:** Enter the port number used for this communication, by default this is set at 9425
- **eCopy Enabled Device:** Enter the IP address of the target MFP where SSOP is installed
- **User name:** Enter a user name (domain login name)
- **Domain:** Enter or select the domain the User account resides

Enter the relevant information for a valid user and the target device IP address running SSOP. The important items here are the 'Key Path' and 'Encryption Type', these should be the same as those specified in the 'ID Service' tab in the SSOP Admin console.

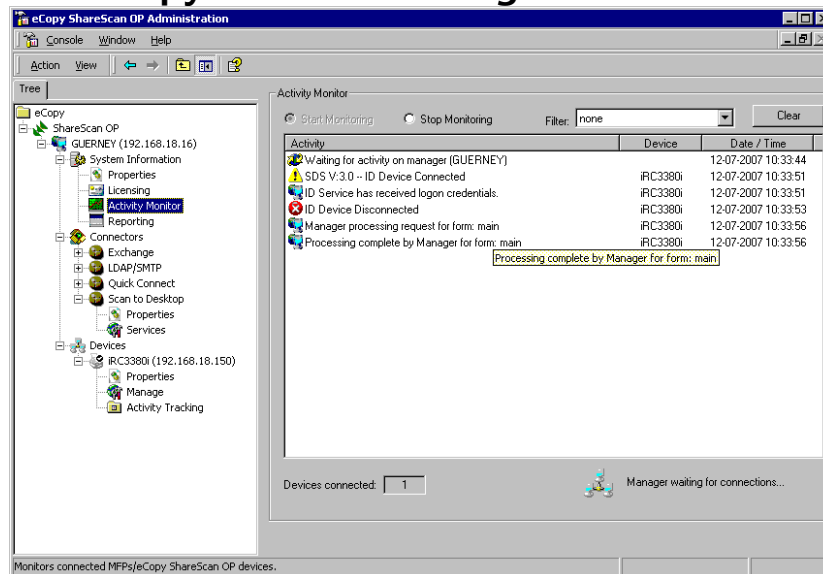
Once saved, select the 'Send credentials to manager' to test the app. You should be able to see either in the SSOP MEAP app or on the ScanStation the details you've specified being automatically populated in the eCopy Session Logon Screen. If you can then it's working, if you can't that there is a configuration issue or communication error and the problem lies with eCopy.

Essentially the ID Services Emulator is a 'dumb' application that simply sends the user authentication information to the ShareScan ID Service. The success of the log in is not shown by this application as it simply sends the relevant XML information to the eCopy ID Service. The response from the emulator will always be:

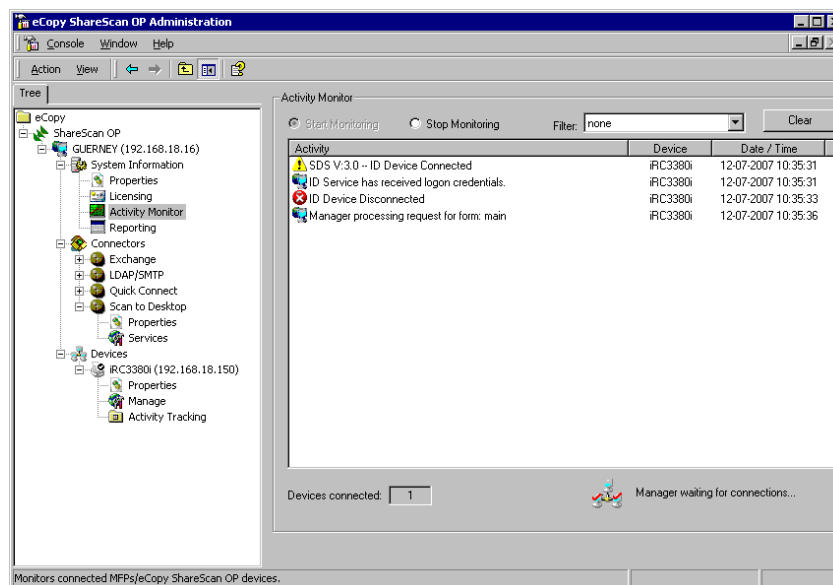


The only way to see if the credentials specified have worked are by checking SSOP on the MFP or by viewing the activity monitor in the ShareScan Administration Console. When log on information is sent to the eCopy ID Service the activity monitor will show whether or not the log on has been successful. A successful log in will display:

ECopy & NT Ware Integration Guide



Whereby an unsuccessful login for whatever reason will be displayed as:



The difference is the 'Processing complete by Manager for form: main' entry (the final entry). This will also be apparent on the device as the login will be unsuccessful.

Ecopy & NT Ware Integration Guide

uniFLOW OM Setup

NT-Ware Supplied Files:

Assuming everything is working with the eCopy side, the uniFLOW OM setup is actually quite straight forward and is part of the v3.1.1 (onwards) release.

Create the device in the Windows Spooler

Create the device in uniFLOW OM Server Configuration (please refer to the uniFLOW OM v3.1 User Manual for details)

Configure the printer in uniFLOW OM for the relevant identification system that will be used (please refer to the uniFLOW OM v3.1 User Manual for details). If you are ever unsure about the configuration, first use the wizard to create the printer and then edit it under 'Advanced printer configuration'. As an example when using a miniMIND Mifare Card reader set, I used the 'Secure Output Printer with uniFLOW OM Secure/Public Printing Applet and miniMIND or SSO' configuration.

Printer 15 item(s)

Name	Terminal Serial	Routing Group	Spooler Name	Server Name	Printer Wizard
Canon LBP5000			Canon LBP5000	MAMMOTH	Advanced printer configuration
IR5570					Advanced printer configuration
Job Ticket Pre Print			Job Ticket Pre Print		Job Ticket - Input Printer ...
Secure Print		SecureBW	Secure Print BW		Secure Print - Input Printer
Secure Print Col		SecureCol	Secure Print Col		Secure Print - Input Printer
uF CLC4040-H1 PCL5c			uF CLC4040-H1 PCL5c		Accounting only
uF IR C3380 PCL5c	2627C126	SecureCol	uF IR C3380 PCL5c		Secure Output Printer with ...
uF IR105 PCL5e Left			uF IR105 PCL5e Left		Job Ticket - Output Printer
uF IR105 PCL5e Right			uF IR105 PCL5e Right		Job Ticket - Output Printer
uF IR3570 PCL5e	KBG00005	SecureBW	uF IR3570 PCL5e		Secure Output Printer with ...
uF IR5020 PCL5e					Copyshop Device - Canon ima...
uF IR7105-S1 PCL5e			uF IR7105-S1 PCL5e		Job Ticket - Output Printer
uF IR7105-S1 PS Ver 1.0			uF IR7105-S1 PS Ver 1.0		Internet Gateway V2
uF IR8070 PCL5e			uF IR8070 PCL5e		Advanced printer configuration
uF IR8070-M3 PCL5e			uF IR8070-M3 PCL5e		Accounting only

After this is set up correctly (in the example above this was with an IRC3880), edit the printer settings again using the Advance Printer Configuration.

ECopy & NT Ware Integration Guide

The screenshot shows the 'Device Agents' tab in the configuration window. The 'General' tab is selected, and the 'MIND CPCA Copy Control' dropdown is set to 'MIND CPCA Copy Control'. The 'Counter reading' dropdown is set to '- None -'. The 'Spooler control' dropdown is set to '- None -'. The 'Other' section contains the following fields:

Field	Value
User name	2
Serial number	
Read Fax Log	no
Read Scan Log	no
Read Print Log	no
MEAP IR Serial Number	
Enforce User Budget	no
Log unselected products	no
Show Message Board	yes
Use A3 Price For Limits	
Charge Print Jobs on Log Out	
Continuous Log Read	
Use old SSOP v4.0 Format	no
TripleDES Key	48B4E2A2A4AA4F41B18
Address	192.168.18.150
eCopy SSOP Server Port	9425
eCopy SSOP Server Address	192.168.18.16

At the bottom of the window, there are five buttons: 'Save', 'Save + Back', 'Save + New', 'Delete', and 'Cancel'.

In the Device Agent tab under Other, select eCopy SSOP Identification Service from the drop down list.

The options listed relate to the setup for eCopy ID Service configuration. If you are using TripleDES encryption, cut and paste the key generated from the SSOP Admin console here. The 'Address' is the IP address of either the MFP (for SSOP MEAP Clients) or the IP address of the ScanStation. As mentioned before the server port will be pre-populated once you select 'Save'. The eCopy SSOP server address is the IP address of the SSOP Administration Console server where the ID Service extension has been installed. Click 'Save + Back'. Please ignore the 'Use old SSOP v4.0 Format' option as this is only displayed for legacy purposes so by default is set to 'no'.

Finally, it's left to the user configuration. There are different ID methods so please follow the appropriate configuration/setup for each user.

What has to be entered per user for this to work properly is found under a button 'Set User Password'.

Ecopy & NT Ware Integration Guide

The screenshot shows a web-based user management interface for eCopy. The main form is titled 'General' and contains various fields for user information. A modal dialog box titled 'Set Password' is open, allowing the user to set a password for the user 'stephen' in the 'essm' domain. The dialog includes fields for 'User Name', 'Domain', 'Password', and 'Retype Password', along with 'Set Password' and 'Back' buttons.

General Tab Fields:

- Name: Stephen Jobs
- Email: stephen@ESSM.COM
- Login: stephen
- Host Login:
- Standard Cost Center: - None -
- Standard Invoice Address: - None -
- Standard Delivery Address: - None -
- Standard Group: DSG
- Default Archive Folder: - None -
- Group Master (Secure Print): No, print only own print jobs
- Number / Chip ID: 0108080111031504
- PIN Code:
- Job Profile: - None -
- Specific Job Ticket: - None -
- Internet Gateway Login name: stephen
- Internet Gateway Status: User Data Accepted by Oper.
- Internet Gateway Account Type: Normal
- Home Server:
- Product Availability (CPCA ID only): Any
- Personal Folder:
- Money Loader User Type: Normal
- Login Manager User Type: Normal

Set Password Dialog Fields:

- User Name: stephen
- Domain: essm
- Password:
- Retype Password:

Buttons: Save, Save + Back, Save + New, Delete, Cancel, Set Password, Back, Set User Password, Get number from.

The detail that is entered here (other than the login 'user name') namely the Domain and Password is the information that is passed to the eCopy systems Session Logon after a successful login.

Essentially there are two options for the users:

Default behaviour: Users can either have uniFLOW OM pre fill the eCopy Session Logon with the domain name and domain, meaning that they have to still enter their domain password after they have authenticated through uniFLOW OM. These fields can be synchronised with Active Directory via the LDAP connector to simplify administration.

Pre filled password: *On a project basis* it could be realised that Users could access a web page and enter their details including their domain password so it's stored into the uniFLOW OM database which could then automatically log them on to eCopy once they've authenticated at a device.

Either way, when a user authenticates them self at a device, they will be given access to the device and eCopy with one unified mechanism.

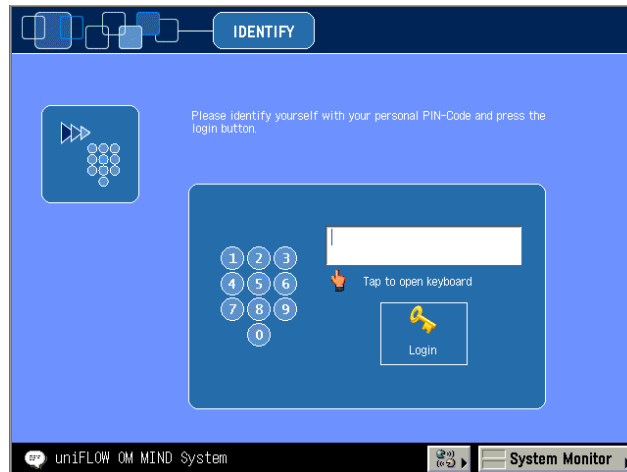
Entering user details using the Login Manager

If there are many users it is quite laborious if the person has to go to the Administrator to enter the *Domain* name and/or the *Password*. Therefore, NT-ware has provided the possibility of entering the Login data via the Login Manager v2.0.0 (onwards) on the iR as well. The advantage is obvious. No intervention from an administrator is necessary, the users can enter their passwords "on demand".

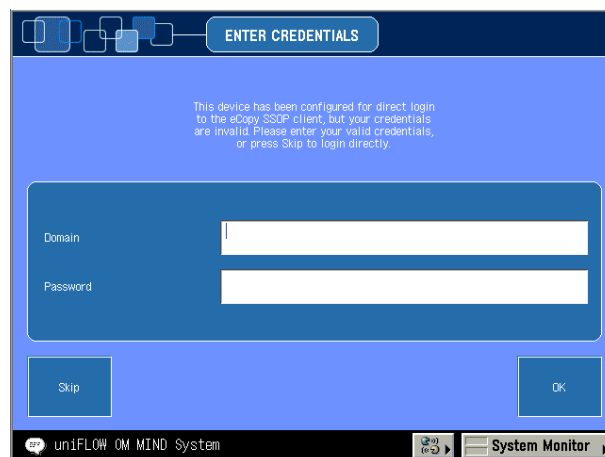
Ecopy & NT Ware Integration Guide

For a user whose domain name and or password isn't known in eCopy or uniFLOW OM yet the Logon procedure will be as follows:

1. Having logged on with card or PIN number it is checked whether the user has valid credentials (password) in uniFLOW OM in order to allow a Domain Logon.



2. Thereafter a screen for entering the logon details is displayed, where the user can enter his/her data. If the domain name has been imported via LDAP the domain name will be pre-filled and only the password has to be entered.



3. The entered data is checked. This may take a moment. If the credentials are correct the logon process is completed and the user is logged on to the eCopy device.
4. If the credentials are not correct, the password entry form is redisplayed in which the logon data can be entered once again.

The user has to enter the logon data only once, the next time he/she identifies himself/herself he/she will be logged on to the domain automatically.

Note: This login is not mandatory it can also be skipped by pressing Skip, for example if a user only wants to copy.

When the uniFLOW Login Manager v2.0 (onwards) is configured to check user credentials for eCopy SSOP Identification Service on-demand, the uniFLOW OM Server processes the following

Ecopia & NT Ware Integration Guide

steps to check if the credentials are valid:

1. If the computer uniFLOW OM Server is installed on is member of the same domain as the user to check the credentials for, uniFLOW OM tries to temporarily logon the user to the local system.
2. If this fails or the uniFLOW OM server is not member of the domain, uniFLOW OM tries to discover the Domain Controller by the NetBIOS domain name given by the uniFLOW Login Manager v2.0 frontend. If a Domain Controller is found, uniFLOW OM tries to authenticate the user against this Domain Controller
3. If this fails also, uniFLOW OM tries to authenticate the user against each LDAP connector configured in uniFLOW OM for user import.
4. If none of the above has worked, the user's credentials are expected to be invalid

EcCopy & NT Ware Integration Guide

Versioning

Working with uniFLOW OM Server

uniFLOW OM Version	eCopy Version	Patches/Files	Comments
V3.1.1 onwards	V4.1, V4.2	See Ask eCopy ID781 or in the ITS MOMKB-235	Tested with multiple devices using alternative login methods

Working with uniFLOW OM RPS

uniFLOW OM Version	eCopy Version	Patches/Files	Comments
V3.1.4 onwards	V4.1, V4.2	See Ask eCopy ID781 or in the ITS MOMKB-235	Until v3.1.4 the Login Manager doesn't prompt the user for their login credentials if set up on an RPS. If the user credentials are entered correctly in uniFLOW then this works. From v3.1.4 this will be fixed.

Ecopy & NT Ware Integration Guide

Trouble shooting

eCopy Setup

When setting up eCopy, if there are any problems when using the 'ID Service Emulator' ensure that when simulating a device logon that activity is taking place for the target device under the 'System Information' -> 'Activity Monitor' in the ShareScan OP Administration console.

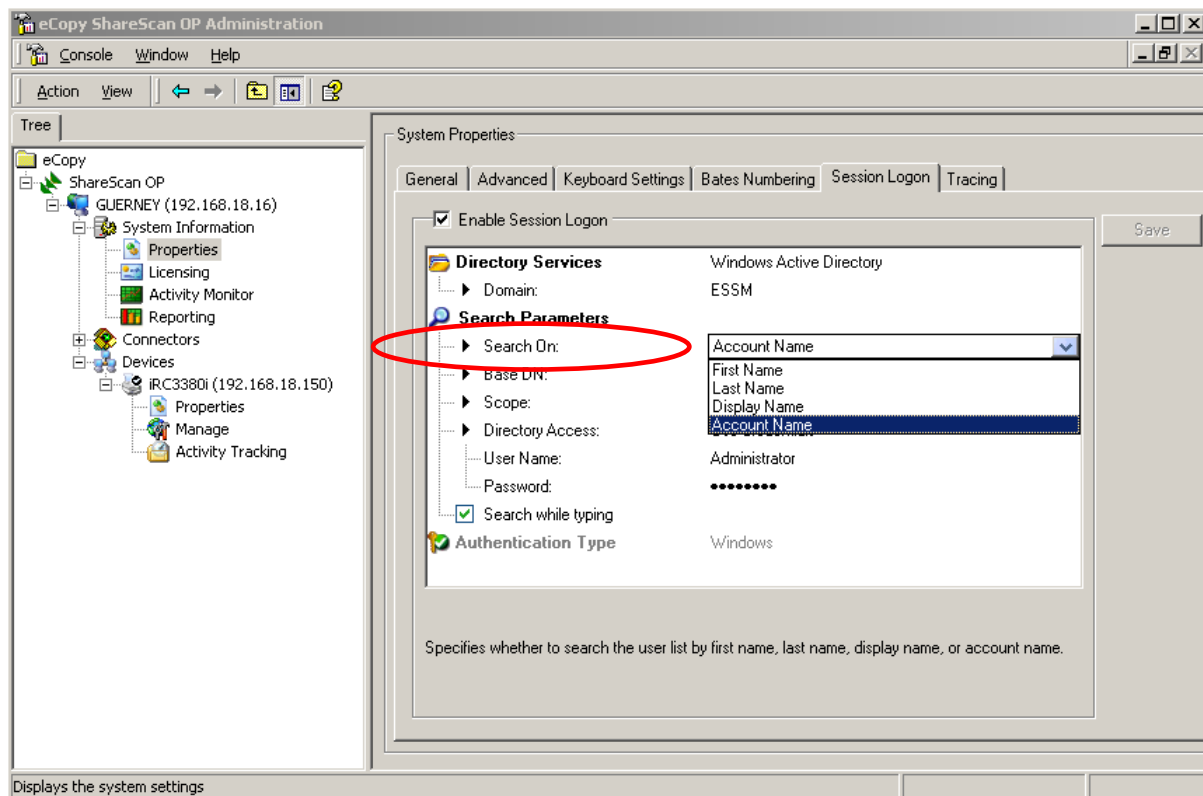
If this still doesn't resolve the issue, then check that the 'Port', 'Encryption Type', 'Path' and 'Key' are the same in the eCopy Admin console as well as the ID Services Emulator.

Where problems persist and it is necessary to escalate the issue to eCopy via Remedy please carry out the following procedure:

In the eCopy SSOP Admin Console turn on the Device tracing and try a login. To turn on tracing, go to the Properties node of the device. Click on the Tracing tab (last one on the right). Click on "Write to vendors DEBUG Console" and then Save. Now try and logon. Go back to the Tracing tab and click Retrieve Trace File, then the contents along with the support request.

It may be helpful to temporarily disable all other MEAP applications running on the device.

If the eCopy login credentials are been passed from uniFLOW OM but the session login fails with SSOP (the Search while typing function doesn't automatically fill in the complete name), then it's possible to change the search criteria that eCopy uses to the complete name 'Account name' which is passed by uniFLOW OM.



Ecopy & NT Ware Integration Guide

NT-ware Setup

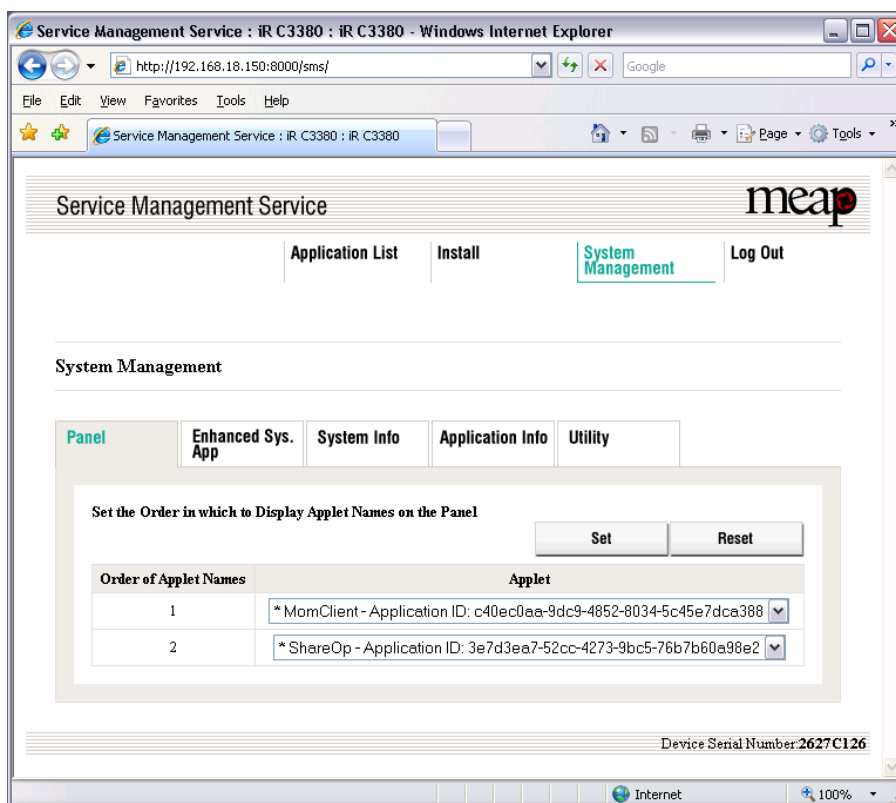
Always be careful to check that the settings in the device agent, namely the 'Port', 'Encryption Type', 'Path' and 'Key' are the same as set in the eCopy Admin console.

The check the functionality of the Login Manager to allow the user the enter their domain and password details, open the uniFLOW OM Server config -> Base Data -> User. Select the test user and click on the Set User Password. Change the listed domain and/or password to something you know is incorrect and click 'Set Password'. Login again with the test user and they should be prompted to enter the correct information.

General

If the eCopy User Name info field on the device 'Session Logon' isn't 'auto completing' then ensure that the 'Login' name specified for the user in uniFLOW OM is the same as the domain log in detail. It may also be necessary to ensure that the 'Name' field for the user in uniFLOW OM is the same as the 'Login' field.

It is possible with older device firmware that the MEAP applet display order can affect the applet functioning correctly. If there are problems then check the order of the display of the MEAP applets on the MFP. This is configured in the 'Service Management Service' of the MFP. Please ensure that SSOP applet isn't first in the list as shown below:



Ecopy & NT Ware Integration Guide

Communication issues can arise if the ScanStation being used has the Windows XP firewall blocking the specified port (default of 9425). Either disable the firewall (this could be the same issue for any firewall applied to the PC) or add exceptions for TCP/UDP for 9425.

If the eCopy ID service does not pass any information (the activity monitor doesn't show the two entries for Manager Processing) it may be necessary to reboot the server running eCopy Services Manager.

If it seems that no credentials are being passed from the uniFLOW OM Server to the eCopy embedded applications or scan stations then restart the uniFLOW services (or reboot the uniFLOW server).

Finally, it may be necessary to reboot the MFD's for the integration to work.

Ecopy & NT Ware Integration Guide

Support & Escalation

This integration is only fully supported with the release of eCopy v.4.1, v4.2 and uniFLOW OM v3.1.1 onwards.

All escalations will be decided upon whether the test using the eCopy ID Service Emulator is successful. If it is then it is likely a NT-ware issue so should be placed on the ITS. If the ID Service Emulator test isn't successful the escalation should take place via the ECNC (Remedy) as outlined below. It is expected that NT-ware and eCopy will work together to solve any escalations together without referring the issue back to the other party.

