White Paper

// Security - uniFLOW

Version 2.9

20-Feb-2015

Version 5.x

Versioning

Document Versioning	**Version**	**Author(s)**	**Date**	**Reviewer(s)**
	2.0	Thomas Lemmer	28-Sep-2012	Andre Mess, Thomas Fick, Norbert Löwe, Julian Ayling, Stefanie Küpper, Karl Vieth, Iain Werren, Dennis Fischer, Jörg Walter, Peter Fresenborg
	2.1	Thomas Lemmer	25-Oct-2012	Marja Pals, Peter Fresenborg
	2.2	Thomas Lemmer	02-Nov-2012	Peter Fresenborg, Marja Pals
	2.3	Thomas Lemmer	14-Nov-2012	Thomas Lemmer, Dirk Tiemeyer
	2.4	Thomas Lemmer	19-Sep-2013	André Meß
	2.5	Felix Schlick	20-Dec-2013	Thomas Lemmer
	2.6	Thomas Lemmer	06-Jan-2014	André Meß
	2.7	Felix Schlick	11-Sep-2014	Tudor Oprea, Thomas Lemmer
	2.8	Felix Schlick	26-Jan-2015	Thomas Lemmer
	2.9	Sebastian Husnik, Felix Schlick	20-Feb-2015	Thomas Lemmer, Lee Brooks
Document Name	White Paper - uniFLOW - Security			
Knowledgebase	MOMKB-462 (https://web.nt-ware.net/its/browse/MOMKB-462)			
File Name	White Paper - uniFLOW - Security - V2.9.pdf			
Technologies Concerned	uniFLOW V5.x, MEAP, Windows, SSL, HTTPS, MEAP, LDAP, Secure LDAP, Anti Virus, uniFLOW Client for Windows, uniFLOW Client for Mac			
Short Summary	This White Paper has been written to help you increase the security of uniFLOW and the respective network environment and servers. This document will focus on the configuration options within uniFLOW and standard security features. The document will be updated regularly.			

Document Changes	**Version**	**Topic(s)**	**Changes**
	1.3	Added the chapter "Canon Device Security"	New chapter added.
	1.4	Added iW SAM background information	Added iW SAM background information
	1.5	Web Applications: Different Application Pools (on page 45)	New chapter added.
	1.6	Web Applications: Different Application Pools (on page 45)	Updated chapter.
	1.7	NTLMv1 Authentication (on page 15)	New chapter added.
	1.8	Security Considerations (see "Web Applications: Secure pwserver on Windows 2008 (R2)" on page 38)	New chapter added.
	1.9	Web Applications: Secure pwserver on Windows 2008 (R2) (on page 38)	New chapter added.

	2.0	SQL Connectionstring and New DB User Since uniFLOW V5.1.3 (see "SQL Connection String and New DB User From uniFLOW V5.1.3 Onwards" on page 11)	New chapter added.
	2.1	Microsoft Windows RDP Server (on page 57)	New chapter added.
	2.2	Server Message Block (SMB) Signing (on page 56)	New chapter added.
	2.3	uniFLOW Client for Windows via HTTPS (on page 52)	Corrected a description.
	2.4	uniFLOW < V5.2 (on page 42), uniFLOW >= V5.2 (on page 43), uniFLOW V5.2 RPS communication (on page 51), uniFLOW Client for Windows via HTTPS (on page 52), uniFLOW Client for Mac via HTTPS (on page 52)	New chapters added.
	2.5	Creating and Importing SSL Certificates for Canon MFPs (see "Creation and Import of SSL Certificates for Canon MFPs" on page 4)	New chapter added.
	2.6	Pass-through and authentication using the uniFLOW Login Manager (on page 13), Active Directory Passwords (on page 9)	Added new encryption methods.
	2.7	General SSL Requirements (on page 3)	How to deactivate deprecated protocols.
	2.8	All topics	Improved layout and formattings.
	2.9	uniFLOW Mobile Print Service for iPad or iPhone (on page 53) IIS Security (on page 44)	New chapters added.

Disclaimer

trademark of Kantech, XEROX is a registered trademark of XEROX CORPORATION in the United States or other countries.

All other trademarks, trade names, product names, service marks are property of their respective owners and are hereby acknowledged.

While every precaution has been taken in the preparation of this document, NT-ware assumes no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. NT-ware does not assume any responsibility or liability for any malfunctions or loss of data caused by the combination of at least one NT-ware product and the used operation system and/or third-party products. In no event shall NT-ware be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

In addition, this manual provides links to the sites of affiliated or independent companies and certain other businesses. NT-ware is not responsible for examining or evaluating, and NT-ware does not warrant the offerings of, any of these businesses or individuals or the content of their websites. NT-ware does not assume any responsibility or liability for the actions, product, and content of all these and any other third parties. You should carefully review their privacy statements and other conditions of use.

Donnerstag, 30. April 2015, Bad Iburg (Germany)

Important Note

Serious problems might occur if you modify the registry of your Windows operating system incorrectly. These problems might require that you reinstall the operating system. We strongly recommend to always back up the registry of your Windows operating system before applying changes to it, just in case you do something wrong. NT-ware does not assume any responsibility or liability for any impact on the operating system after changing the registry. You understand and accept that you use this information and modify the registry of your Windows operating system at your own risk.

Copyright and Contact

NT-WARE Systemprogrammierungs-GmbH
Niedersachsenstraße 6
49186 Bad Iburg
Germany

www.nt-ware.com

Should you come across any relevant errors or have any suggestions please contact documentation@nt-ware.com or use the ***Send feedback here*** button of the uniFLOW Online Help.

Symbols

Text Styles

This style is used for text that is displayed on screen.

This style is used for text the user has to type in.

This style is used for hyperlinks to web pages, internal links to other pages in this manual.

`This style is used for code examples: XML code, variables or regular expressions.`

Pictograms

Important Note:
Information that is crucial for the correct functioning of the uniFLOW software.

External Manual:
Pointer to additional manuals for third party hardware or third party software.

Region Specific Feature:
Indicator for uniFLOW features that are not available worldwide.

External Link:
Link to an external web page.

Settings:
Detailed explanation of configuration settings or operational procedures.

Compass:
Path to the menu or configuration page in the software.

Screenshots and Diagrams

This manual contains screenshots of the software, diagrams explaining relations and pictures of products. Even though all visuals are up-to-date at the time of writing, they are subject to change.

Send Feedback

Should you come across any relevant errors or have any suggestions please contact documentation@nt-ware.com or use the ***Send feedback here*** button of the uniFLOW Online Help.

Contents

1 Introduction

This White Paper has been written to help you increase the security of uniFLOW and the respective network environment and servers. This document will focus on the configuration options within uniFLOW and standard security features.

Settings and actions described in this document should only be executed by qualified personnel. NT-ware cannot give any warranties about any damage or disadvantages suffered as a result of the implementation of the settings and actions described in this document.

We are constantly working on this document to keep it up to date. However, if you have certain questions which are not answered in this document, please contact the NT-ware Support Department.

uniFLOW requires several different ports and protocols to communicate with clients, printers, the database and other network devices. The *White Paper - TCP Ports of uniFLOW* lists all these different communication protocols and ports.

Use this document, in order to configure your firewall(s).

Download the *White Paper - TCP Ports of uniFLOW* here:

MOMKB-99 (http://its.nt-ware.net/browse/MOMKB-99)

2 Security Considerations

This section provides a guide to ensure good practice when designing and configuring your implementation of uniFLOW & MFPs in order to minimize possible security risks or concerns. As security requirements will be different for each environment, this advice should be used as a starting point so that you can select the appropriate controls for your own topology.

Minimize the attack space on your MFPs

Canon provides a security hardening guide for MFPs which provides an initial guide to configuring the MFP services. Ensure that services that you are not planning to use are disabled and that those that are left are correctly configured for your environment.

http://www.canon-europe.com/About_Us/Press_Centre/Press_Releases/Business_Solutions_News/1H11/Security_Guide.aspx

Logically separate your MFPs if possible

As explained in the hardening guide, you can limit and control what traffic is possible by only allowing uniFLOW to communicate with your MFPs. This can be done by using separate VLANs for your MFPs and restricting access into these segments.

Monitor or protect the gateway with IDS/IPS

If you have intrusion detection or prevention solutions (IDS/IPS) solutions in place, use these to monitor the gateway from the MFP VLANs. Configure alerts and investigate unexpected traffic traveling between these segments.

Monitor the MFPs

Utilize any existing network monitoring tools with your MFPs. Look out for any suspicious activity such as an MFP being unplugged from the network. This may be an indication of possible Man-in-the-Middle activity.

Restrict access to the physical network ports

Use MAC addresses or 802.1x authentication to verify the MFP's access onto the network segments if possible. This can stop unauthorized devices from collecting data on these segments.

Control any unauthorized network scanning or network captures

If not already enforced, monitor and investigate any packet sniffing or port scanning behavior on your network.

Consider the positioning of your MFP from a security perspective

Physically place MFPs so that malicious activity is likely to be observed or deterred. Consider using CCTV on MFPs printing, scanning or copying sensitive information.

Use good practice on the application platform

Ensure your web server platform is configured with defined security standards before and after installing uniFLOW (e.g. IIS Lockdown, URL scan etc.). The underlying operating system should also be hardened for its role and its patch level kept up to date. Please refer to chapter Web Applications: Secure pwserver on Windows 2008 (R2) (on page 38).

Keep client-server authentication communication at the highest possible level

Enforce NTLMv2 on clients connecting to the uniFLOW server(s) where possible. Please also refer to chapter NTLMv1 Authentication (on page 15) of this White Paper for more information.

Encrypt all MFP to server traffic

It is possible to use IPSec (an optional hardware board is required in the MFP) between MFP and the uniFLOW server(s) to ensure that no interception of this traffic could result in data being compromised.

3 SSL

3.1 General SSL Requirements

To ensure the system can be implemented for communication through secure (SSL) channels the infrastructure must have security certificates. This will allow the communication of encrypted data via port 443.

To obtain an SSL Certificate,

- contact your system administrator and check if there is a company certificate
- implement Microsoft Certificate Servers and generate a certificate
- request an SSL certificate from your service provider, for example

http://www.verisign.com

Removing Deprecated SSL Protocols

To maintain a secure web environment it is essential to deactivate outdated and deprecated protocols like SSL v2 in the IIS.

This can be done either via a registry key or with a ***Fix it*** wizard provided by Microsoft. If the ***Fix it*** wizard does not work on your operating system, you have to use the registry key to disable the protocol.

See http://support.microsoft.com/kb/187498/en-us (http://support.microsoft.com/kb/187498/en-us) for more information and to download the ***Fix it*** wizard.

Manual Procedure

1. In the Windows Registry open the following registry key:
   `HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server`
2. Create a new DWORD with the name *Enabled*.
3. Set the value of the new key to *0*. This disables the SSL v2 protocol.
4. Restart the computer.

3.2 Creation and Import of SSL Certificates for Canon MFPs

In order to use secure connections with SSL between a uniFLOW server / RPS and a Canon MFP, it is necessary to create an SSL certificate on the printer and import it to the server.

The SSL configuration also applies to MEAP connections.

The new certificate must include either the printer's IP address or the fully qualified domain name.

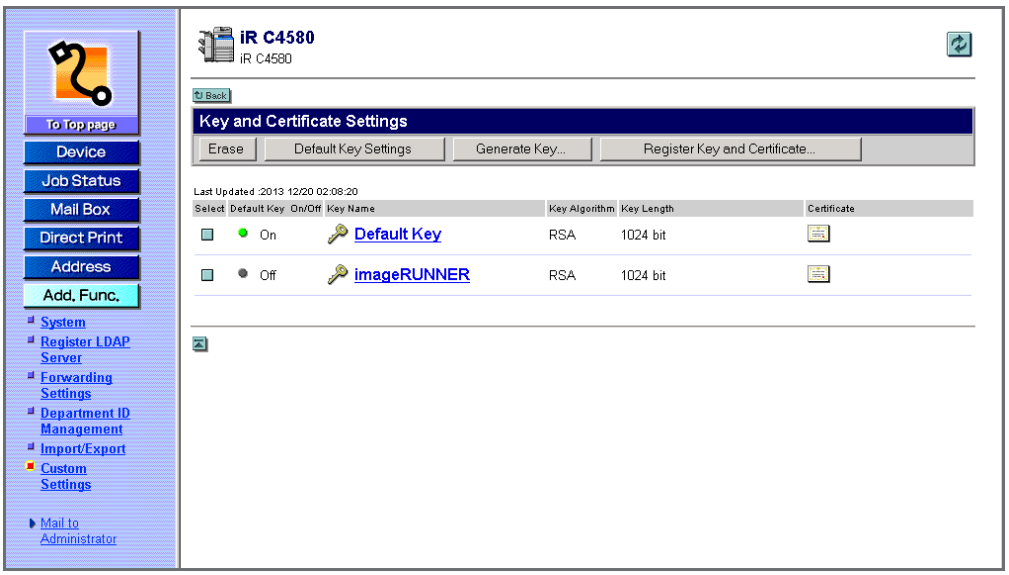
Note that the configuration slightly differs between Canon legacy devices and imageRUNNERs of the Advanced series.

These differences will be outlined in the following description.

Legacy Printers

- Open the printer's RUI in a browser and log in with system manager credentials when asked.
- Open ***Add.Func. > System*** and click on ***Edit***.
- If ***Use SSL*** is checked under ***Remote UI Settings*** uncheck it, click on ***OK*** and restart the device. Otherwise, continue with the next step.
- Open the printer's RUI in a browser and log in with system manager credentials when asked.
- Open ***Add.Func. > Custom Settings > Network Settings > Key and Certificate Settings***.
- If any other key than the ***Default Key*** was used before, check the radio button in front of ***Default Key*** and click on ***Default Key Settings*** to set it as the standard SSL key. Restart the device.
- Open ***Add.Func. > Custom Settings > Network Settings > Key and Certificate Settings > Generate Key > SSL***
- Enter the device IP address or the fully qualified domain name in the field ***Shared Name***, fill out the ***Certificate Settings*** and click on ***OK*** to create the new certificate.
- Open ***Add.Func. > Custom Settings > Network Settings > Key and Certificate Settings.***

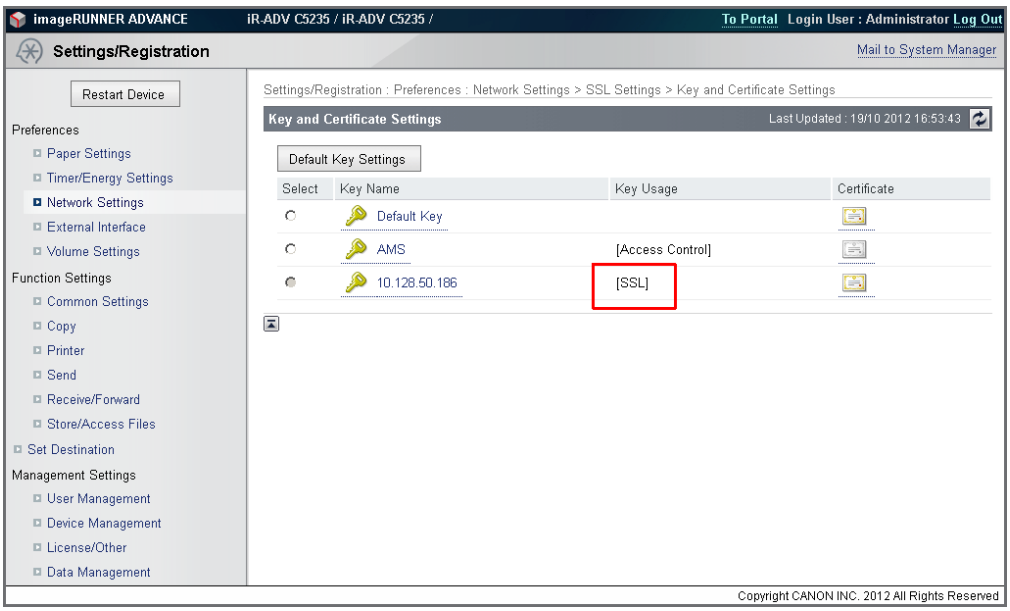
- Select the new key and click on ***Default Key Settings***. Now this key is marked as the active SSL key.



Advanced Series

- Open the printer's RUI in a browser and log in with system manager credentials when asked.
- Open ***Settings/Registration : Management Settings : License/Other > MEAP Settings***
- If ***Use SSL*** is checked uncheck it, click on ***OK*** and restart the device. Otherwise, continue with the next step.
- Open the printer's RUI in a browser and log in with system manager credentials when asked.
- Log in and open ***Settings/Registration : Preferences : Network Settings > SSL Settings > Key and Certificate Settings***
- If any other key than the ***Default Key*** was used before, check the radio button in front of ***Default Key*** and click on ***Default Key Settings*** to set it as the standard SSL key. Restart the device.
- Log in again. In ***Settings/Registration : Management Settings : Device Management > Key and Certificate Settings*** click on ***Generate Key,*** then open ***Network Communication.***
- Enter the device IP address or the fully qualified domain name in the field ***Common Name***, fill out the ***Certificate Settings*** and click on ***OK*** to create the new certificate.
- Open ***Settings/Registration : Preferences : Network Settings > SSL Settings > Key and Certificate Settings.***

- Select the new key and click on ***Default Key Settings***. Now ***[SSL]*** marks this key as the active SSL key.



Activating SSL on the Printer

- On a printer of the Advanced series open ***Settings/Registration : Management Settings : License/Other > MEAP Settings*** and check ***Use SSL.***
  On a legacy printer open ***Add.Func. > System*** and click on ***Edit***. Under ***Remote UI Settings*** activate ***Use SSL***.

This will change the connection settings for both MEAP connections and connections to the standard RUI.

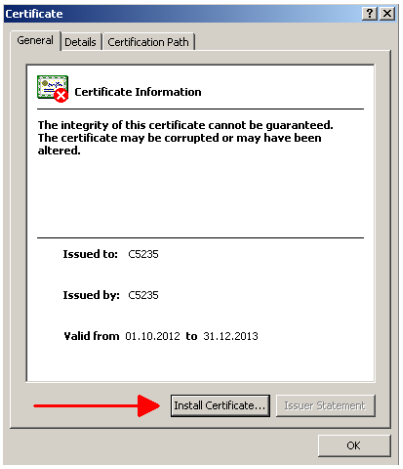
From now on the RUI is only accessible via SSL connections that is with the prefix `HTTPS://`

- Click on ***OK*** and restart the device. Now SSL is active on the printer.

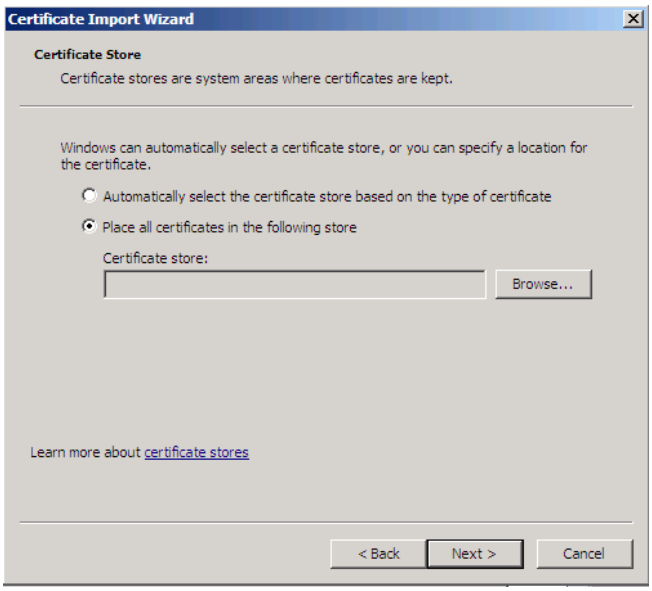
Installing the Certificate

- Now open the printer RUI from your browser again and save the SSL certificate to your file system. The way how to do that depends on your browser.

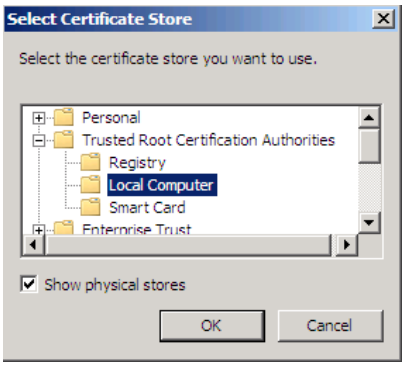
- Open the Windows file explorer and double-click on the saved certificate.



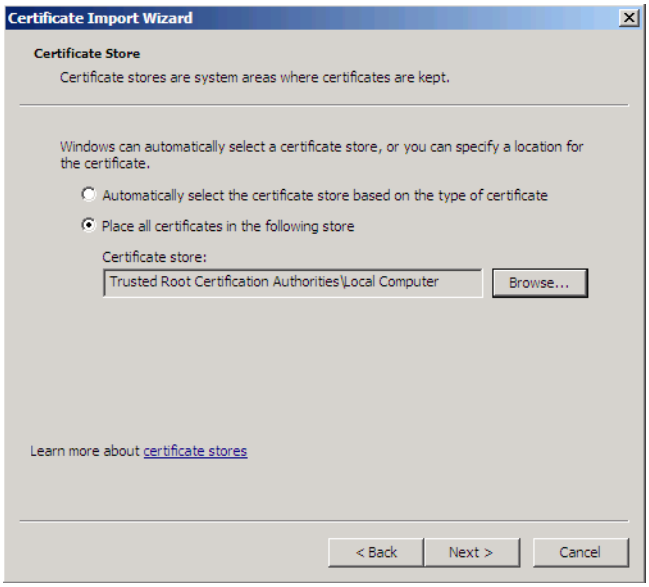
- Start the ***Certificate Import Wizard*** by clicking on ***Install Certificate*** and follow the steps.
- Check ***Place all certificates in the following store***.

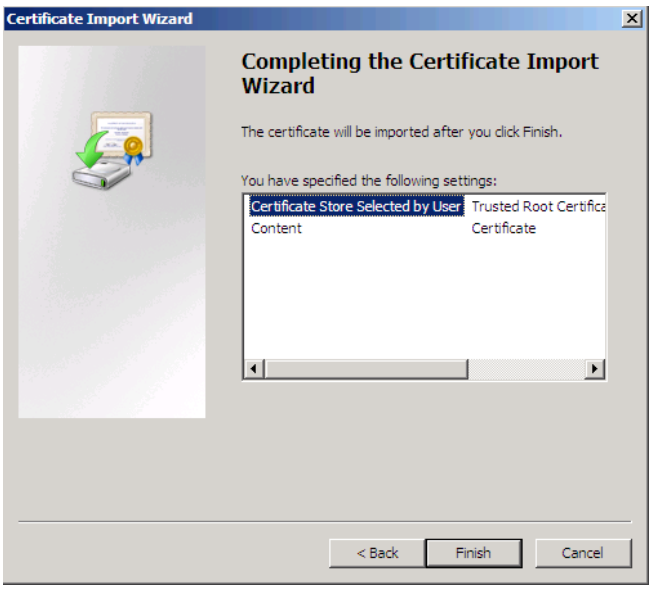


- Click on ***Browse***. Check ***Show physical store*** and select ***Local Computer*** under ***Trusted Root Certification Authorities***.



- Click on ***OK***, then ***Next*** and complete the wizard with ***Finish***.





4 uniFLOW Server

This chapter describes certain known security risks within a standard uniFLOW installation. It explains how to increase security and how to minimize the risk of a security leak.

Some other chapters only describe the actual situation. These chapters describe circumstances where you do not have to improve or change security settings, as uniFLOW operates in a secure way in these circumstances.

4.1 Active Directory Passwords

Active Directory passwords are not stored by default in the uniFLOW database. However, there are the following exceptions:

The password is only stored in the uniFLOW database if there is an integration with eCopy or if you explicitly select to store the password which can be done in the Workflow Element ***Get User Authentication*** (cf. MOMKB-351 (http://its.nt-ware.net/browse/momkb-351) and uniFLOW User Manual) or if you store username and password against the user object.

If this is the case the password is stored in a TripleDES for uniFLOW <= V5.1 SR3 and in an AES-256 encryption format for uniFLOW >= V5.1 SR4 / V5.2. There is no interface which would allow this password to be extracted. Other than in the above cases the Active Directory password is not stored in the uniFLOW database.

If authenticating on an MFP device via the uniFLOW Login Manager, the password entered is transferred in the following chain:

MFP → uniFLOW/RPS → LDAP Service

The encryption used is DES (56 bit) with a dynamic key to encrypt the password when sent from the MFP to the uniFLOW server / RPS. The validity of a password is always checked by the uniFLOW server / RPS against the LDAP service but it is not transferred back to the MFP.

The uniFLOW server / RPS does an LDAP check to validate the user credentials.

4.2 Database

4.2.1 Database Communication

Issue

The database communication between uniFLOW and the SQL server is unencrypted in a standard installation. Sensitive data such as, for example, the users' PIN codes are transmitted in clear text.

Resolution

It is recommended that the database network connections from the uniFLOW server to the SQL server are encrypted using SSL. The following Microsoft article describes how to enable SSL encryption for database connections:

http://support.microsoft.com/kb/316898/en-us
(http://support.microsoft.com/kb/316898/en-us)

4.2.2 Database and Data Storage

Certain features within uniFLOW require passwords to be entered and this data needs to be retained within the uniFLOW database. The following rules apply to the uniFLOW database (DsPcDb):

- The password itself cannot be requested via a COM call or DB query from the uniFLOW system or database.
- The uniFLOW kernel stores passwords as a binary object within a binary field in the database, so that no password information can be extracted.

Furthermore all text-based information within the uniFLOW database is for reporting purposes only and does not contain confidential data such as passwords or PIN codes.

4.2.3 Encrypted Connection String

Issue

The Connection String is an entry in the Windows Registry, which contains all data necessary for uniFLOW to access the uniFLOW database.

This Connection String is installed in each uniFLOW installation by default. As one can see, the user name and password for the database connection is written in clear text. In almost all cases this is no problem as the Connection String is based on the uniFLOW server, which is not accessible to users other than the administrator.

However, the security provisions of some companies require an encrypted Connection String.

Resolution

The NT-ware Knowledgebase (ITS) contains a White Paper which describes how to encrypt the Connection String.

MOMKB-337 (http://its.nt-ware.net/browse/MOMKB-337)

4.2.4 SQL Connection String and New DB User From uniFLOW V5.1.3 Onwards

uniFLOW uses a connection string stored in the Windows Registry to connect the uniFLOW kernel and web pages (UI) to the database. Until uniFLOW V5.1.3, only one connection string was used. To increase the security of uniFLOW, NT-ware introduced an additional connection string and a new additional database user with uniFLOW V5.1.3.

The "CONNECTIONSTRINGUI" key has been added to the uniFLOW registry hive. This connection string is exclusively used for the uniFLOW UI to introduce another layer of security. The "CONNECTIONSTRINGUI" will utilize a new database user called "uFReader". Thus, any request to the uniFLOW database from the uniFLOW UI will be handled via this read-only user. This prevents for example so called SQL injections which a potential hacker could use to execute database queries to manipulate the system or to gather information.

The old "CONNECTIONSTRING" and "pbaip" user still exist and are required for normal operation! This connection string will only be used by the kernel directly.

If the "CONNECTIONSTRINGUI" key is missing, uniFLOW will fall back to use the "CONNECTIONSTRING". This is the case if you have updated from an older version. The registry key will NOT be added by the momupdate.exe. In this case, please use the *.reg file which can be downloaded in this issue to create the respective Windows Registry entry. Please keep in mind to change the "Data Source" within the .reg file from "(local)" to your SQL Server address if you are utilizing an external SQL Server.

Furthermore the additional DB user is required. The "uFReader" user will NOT be created automatically. It will only be created when installing uniFLOW V5.1.3 or higher with a NEW database (taken from http://www.nt-ware.com/mom/sql/momdb.zip).

If you are updating and using an existing database, please use the "Create_uFReader.sql" script which is attached to the ITS issue MOMKB-654 (https://web.nt-ware.net/its/browse/MOMKB-654) to create the additional database user "uFReader".

4.3 Deactivation of auto-complete

Issue

Most browsers have a facility to remember user credentials that are entered into HTML forms (auto-complete). This function can be configured by the user and also by applications which employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application. The stored credentials can be captured by an attacker who gains access to the computer, either locally or through some remote

compromise. Further, methods have existed whereby a malicious web site can retrieve the stored credentials for other applications, by exploiting browser vulnerabilities or through application-level cross-domain attacks.

Resolution

Disable the auto-complete feature of your browser.

While the auto-complete feature may be helpful for some things, it can also seriously compromise your security and privacy, because anyone who uses your computer can see the web sites you visited and the information you entered on web pages. Also various malicious software can use auto-complete data to steal your personal information such as e-mail addresses or passwords. If a hacker were to break into your PC, he or she can easily retrieve web site passwords stored as auto-complete data.

How do I disable auto-complete?

Sometimes it can make sense to fully disable auto-complete if you want maximum security and privacy. There are several ways to do this, depending on the web browser you use:

Internet Explorer 5 and Higher

1. From Internet Explorer, choose ***Tools*** then ***Internet Options.***
2. From the ***Internet Options*** multi-tabbed dialog box that appears, select the ***Content*** tab.
3. Click the Auto Complete ***Settings*** button.
4. Uncheck everything.
5. Click the ***Clear Forms*** button.
6. Click the ***Clear Passwords*** button.
7. Press ***OK*** to close the dialog boxes.

Internet Explorer: Disable Auto-Complete in the Windows Registry

1. Load up regedit (Start > Run > Regedit then press OK).
2. Follow this path: *[HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/AutoComplete]*
3. From there find the Append Completion String value and change its string value to ***yes.***
4. Restart Internet Explorer.

Mozilla Firefox

1. From the ***Tools*** menu, select ***Options***;
2. Select the ***Privacy*** category;
3. Expand the ***Saved Form Information*** section;
4. Remove the check by clicking on the checkbox;
5. Expand the ***Saved Passwords*** section;

6. Remove the check by clicking on the checkbox. You can customize your browser to disallow storage of passwords for some of the pages you visit. To do this press the ***View Saved Passwords*** button;
7. Select ***Remove*** and click ***OK***;
8. Click on ***OK*** to return to your browser.

4.4 MEAP Communication

In general, the communication between MEAP clients and uniFLOW/RPS is in clear text XML in both directions. Whenever it comes down to secure information such as passwords, for example, when a login against Active Directory or PIN codes is used etc., the data is DES encrypted (56bit key) inside the XML.

The DES key used is based on a default key fixed inside the MEAP clients and the uniFLOW/RPS. This key is modified by MEAP device specific data, for example the Serial Number which is known by uniFLOW/RPS and the MEAP client without exchanging this information explicitly. Since MEAP Login Manager / SPP v2.2.1 the encrypted data is of a fixed length. Thus an attacker cannot guess any longer whether the PIN code is short or long.

With uniFLOW V5.1.2 onwards, for emergency accounts, all data is sent with salted hashing, such that it is not possible to recreate the plain text value by cracking the MD5 hashes.

4.4.1 Pass-through and Authentication Using the uniFLOW Login Manager

Automatic login to Therefore

After identification of the user at the device via the uniFLOW Login Manager, uniFLOW forwards the password to the Therefore device RSA encrypted. The components of the encryption keys need to be configured in the Server Configuration of the uniFLOW User Interface which is explained in the uniFLOW User Manual.

Password storage

These RSA public keys are stored centrally as ASCII hexadecimal representation. For further information on how these public keys are set, please refer to the Therefore manual "MFP Connector".

http://www.therefore.net

Automatic login to eCopy

If the Identification Service is configured via the eCopy SSOP Management Interface to use TripleDES encryption for the device specified in "Address" of the configured uniFLOW Device Agent, the following applies: this parameter has to contain the content (one line) of the file into which eCopy SSOP Management Service stores the TripleDES Key.

The key is a string with the length of 24 which means a 96 bit encryption.

The communication with the identification services is handled via Port 9425 (default).

It is possible that no encryption is used (depending on the eCopy implementation).

Password storage <= uniFLOW V5.1 SR3

Using integration with eCopy the password is stored on the uniFLOW server in a TripleDES encrypted format. There is no interface which would allow this password to be extracted.

Password storage >= uniFLOW V5.1 SR4 / V5.2

Using integration with eCopy the password is stored on the uniFLOW server in an AES-256 encryption format. There is no interface which would allow this password to be extracted.

Login against LDAP

The password entered in the uniFLOW Login Manager is transferred in the following chain:

[MFP] → [uniFLOW/RPS] → [LDAP Service]

The encryption used is DES (56 bit) with a dynamic key to encrypt the password when sent from the MFP to the uniFLOW server / RPS. The validity of a password is always checked by the uniFLOW server against the LDAP service but it is not transferred back to the MFP again.

The uniFLOW server does an LDAP bind to check the validity of the user credentials. Furthermore the password is not stored if not integrated with eCopy.

4.4.2 MEAP Scanning

Issue

When scanning a job with the uniFLOW Scan MEAP Applet, the scan job is temporarily stored by default in mailbox 00 of the device until the scan process has finished.

While the Scan UI is shown on the device, every user that is able to access the RUI of the machine with a browser can access the file at the mailbox as long as the scan process takes place on the machine. This is a potential security issue.

Resolution

A resolution for this issue is provided since uniFLOW V5.0.5.

This potential security issue can be solved by setting the parameters below. Beforehand, you have to configure an individual mailbox on the device and protect it with an individual password.

Note that this mailbox number and password must be the same on all devices where the uniFLOW Scan MEAP Applet is running.

Open the uniFLOW Server Configuration and browse to ***Server Config. > General Settings > MEAP Scanning***.

- ***Mailbox Number:***
  Enter the mailbox number where the temporary scan images should be stored.
- ***Mailbox Password:***
  Enter the password for the mailbox. Thus, users logged in at the RUI of the machine cannot open the mailbox folder to view the temporary scan file.

To become effective, you must refresh the MEAP behavior on the device. This can be done by opening the ***MEAP & miniMIND Default Behavior*** under ***Agents/Terminals*** and clicking the ***Save*** button.

Please also note that if an incorrect password has been set, it is still possible to store the temporary scan jobs in the specified mailbox, but the jobs will not be deleted after the scan job has been completed. This can lead to memory problems.

4.5 NTLMv1 Authentication

Issue

NTLMv1 is accepted for authentication against protected web applications by a Windows Server with default security settings.

Though the application can make use of NTLMv2, a fallback to accept NTLMv1 is present. NTLMv1 is considered as an insecure authentication protocol and should not be made use of as it can potentially expose windows domain credentials.

Note that this is not a uniFLOW security leak, but is related to the Windows Server authentication methods used and which of them are allowed.

Risk Level

Medium

Resolution

The NTLMv1 authentication possibility should be disabled on the Windows Server. This can be done by changing the Local Security Policy on a Windows Server 2008.

- Open the ***Local Security Policy*** in Windows Server 2008.
- Browse to ***Local Policies / Security Options***.
- Open ***Network security: LAN Manager authentication level***

You can disable NTLMv1 by changing the settings to ***Send NTLMv2 response only. Refuse LM & NTLM*** (Level 5).

Note that client, service, and program incompatibilities may occur when you modify these security settings. In a productive environment, we highly recommend testing these settings before and to plan a maintenance slot carefully.

Please refer to the Microsoft Knowledgebase under: http://support.microsoft.com/kb/823659.

Please also read the next chapter (see "NTLM Scenarios and Test Results (Behavior)" on page 16) to learn more about the different NTLM scenarios, test results and behavior.

4.5.1 NTLM Scenarios and Test Results (Behavior)

With uniFLOW V5.1 we have tested several scenarios to show which security settings, concerning NTLMv1 and NTLMv2, are causing problems with uniFLOW itself, as well as the accessing of network folders and shared printers. The results are listed in the following subchapters.

As a conclusion it can be said that once the uniFLOW server has been set to NTLMv2 only, and all clients and RPS´s have also been set to NTLMv2, all uniFLOW services or websites are accessible. However, this doesn't mean that other network services will not be affected by this setting, especially if you force this setting via GPO in a Windows domain. With the MacClient we have encountered some problems (see chapter Server (NTLMv2) - Mac Client (on page 27)). Novell Netware RPS and Internet Gateway worked.

We highly recommend that each required functionality in your specific environment is thoroughly tested, before you go live.

4.5.2 Server (NTLMv2) - Client (NTLMv1) - RPS (NTLMv1)

This chapter shows test results based on the settings listed in the following:

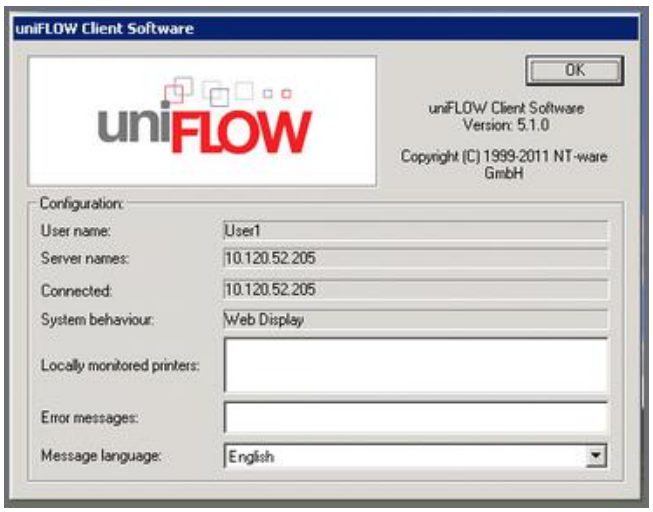
Settings

Server Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Client Settings:	Operating System: Windows XP Network security: LAN Manager authentication level: ***Send LM & NTLM responses***
RPS 1 Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send LM & NTLM responses***
RPS 2 Settings:	Operating System: Windows Server 2003 Network security: LAN Manager authentication level: ***Send LM & NTLM responses***

Test Results

MomClient

The MomClient is still able to connect to the uniFLOW server.

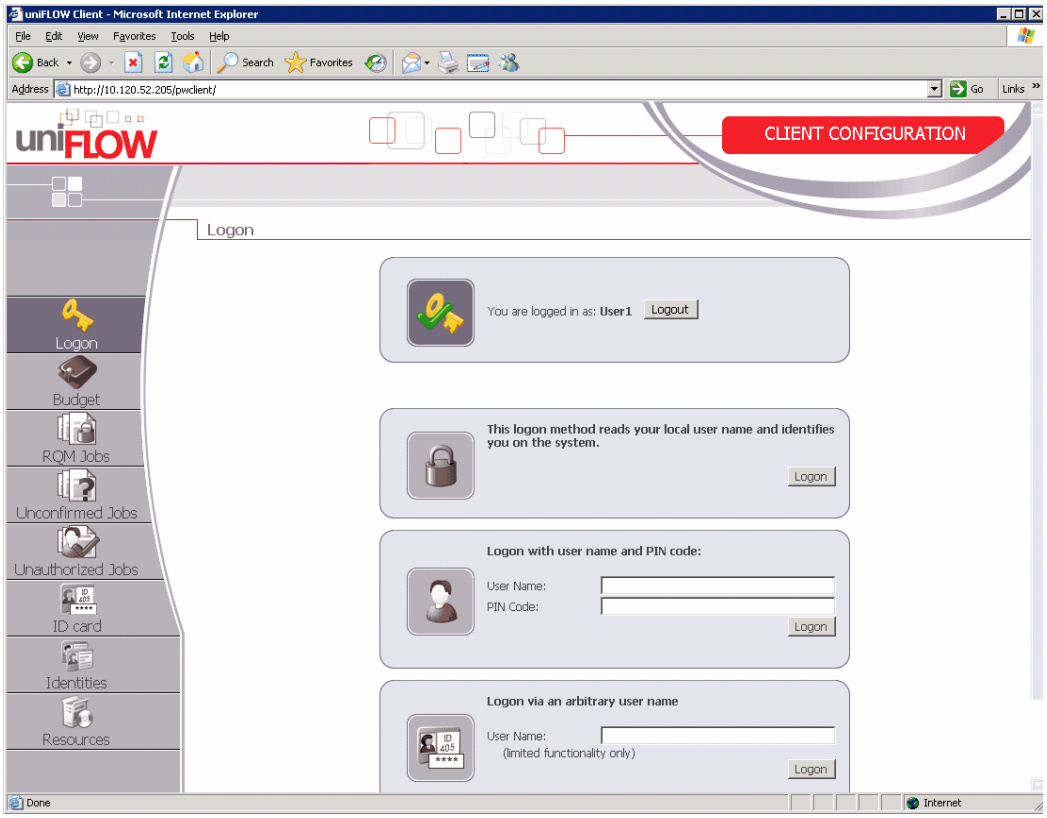


Network Shares / Shared Printers

With the Windows XP Client you are not able to connect to a network share or to a shared printer. You are also not able to print using a connected printer.

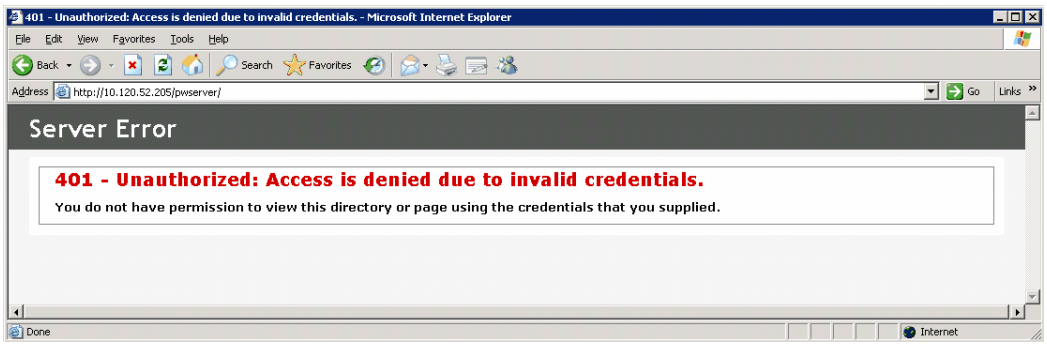
pwclient-website

You are able to access the pwclient-website and log in.



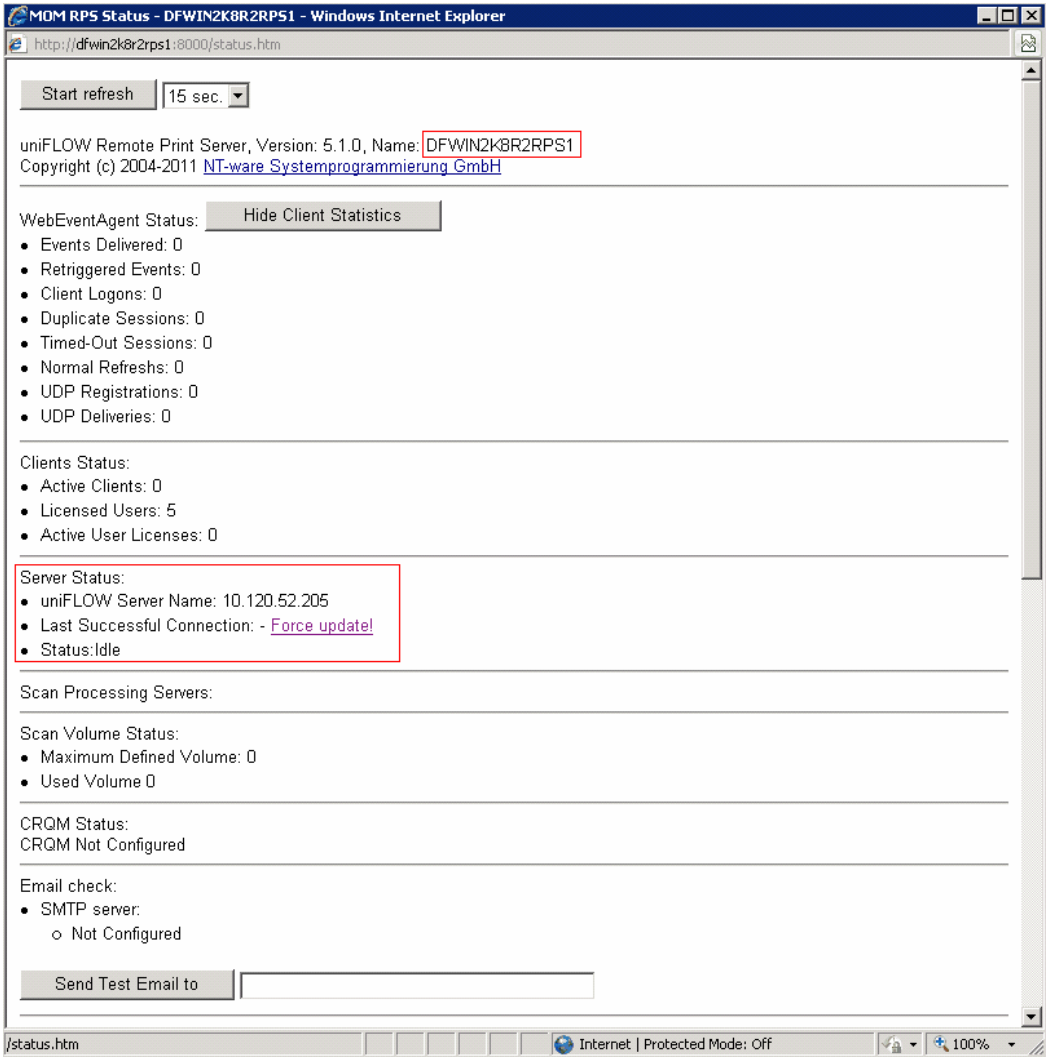
pwserver-website

You are not able to connect to the pwserver-website, although you are using the right credentials. You will receive an HTTP 401 error.

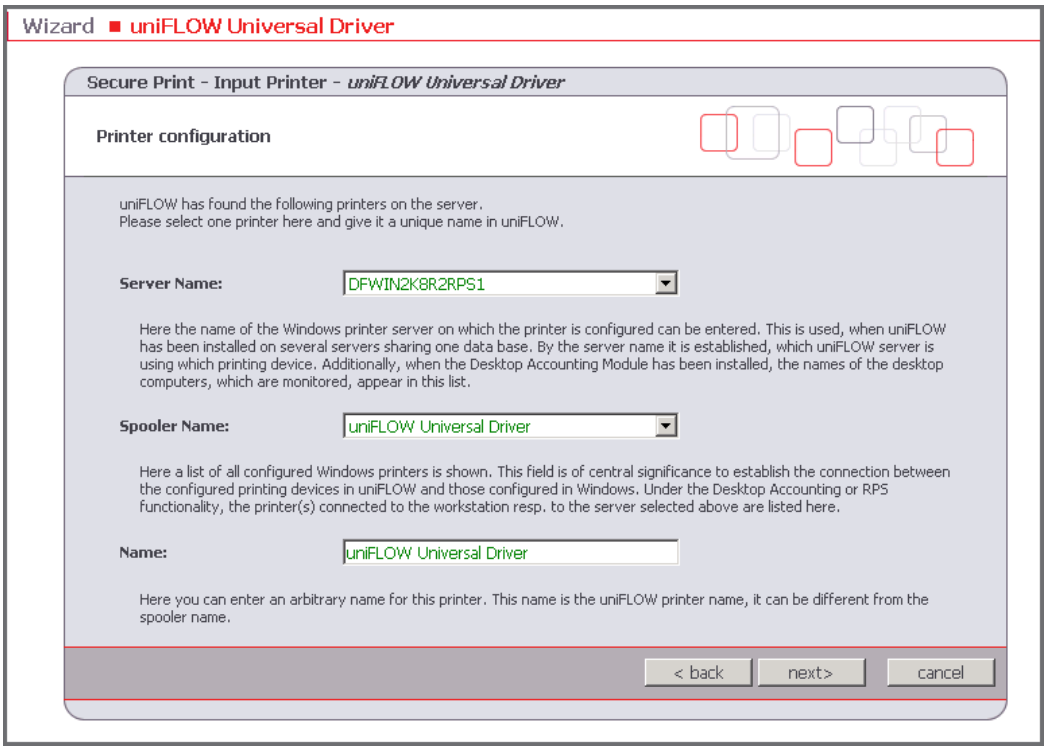


RPS – Windows Server 2008 R2

The RPS under Windows Server 2008 R2 is able to connect to the uniFLOW server.

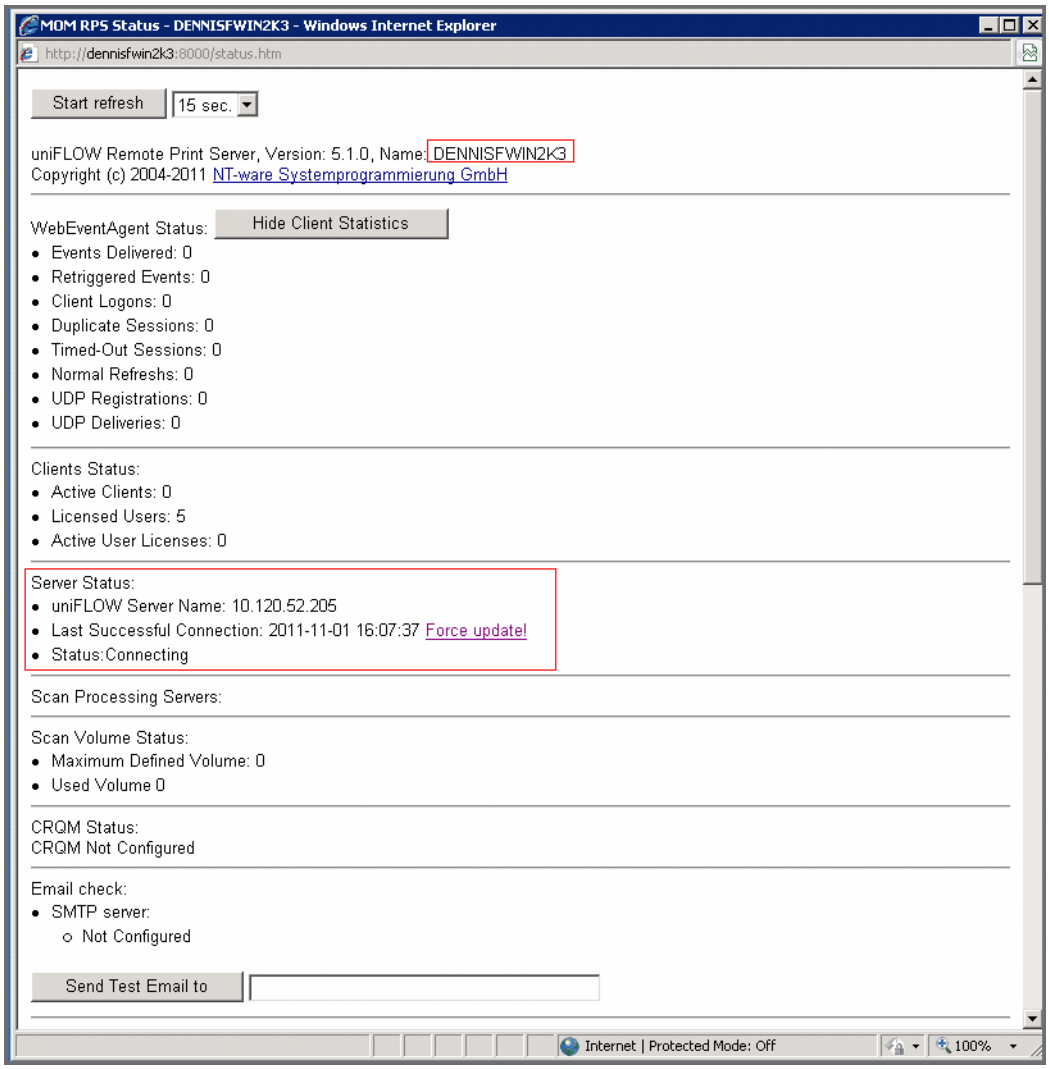


You are able to connect Printers from RPS to uniFLOW.



RPS – Windows Server 2003 (SP2)

The RPS under Windows Server 2003 SP2 is able to connect to the uniFLOW server.



4.5.3 Server (NTLMv2) - Client (NTLMv2) - RPS (NTLMv2)

This chapter shows test results based on the settings listed in the following:

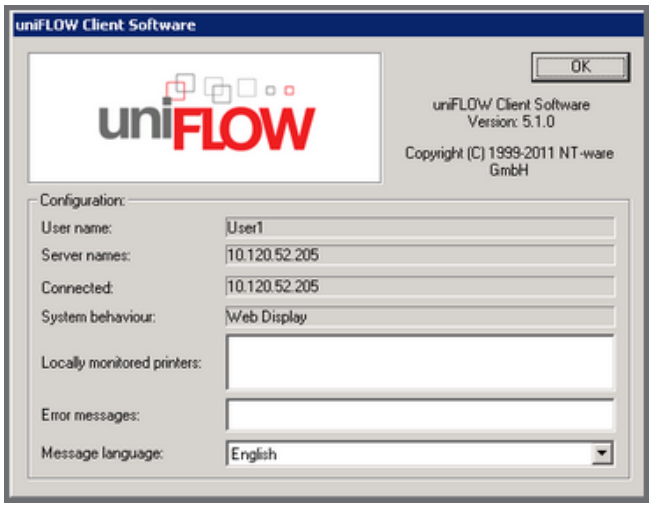
Settings

Server Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Client Settings:	Operating System: Windows XP Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
RPS 1 Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
RPS 2 Settings:	Operating System: Windows Server 2003 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***

Test Results

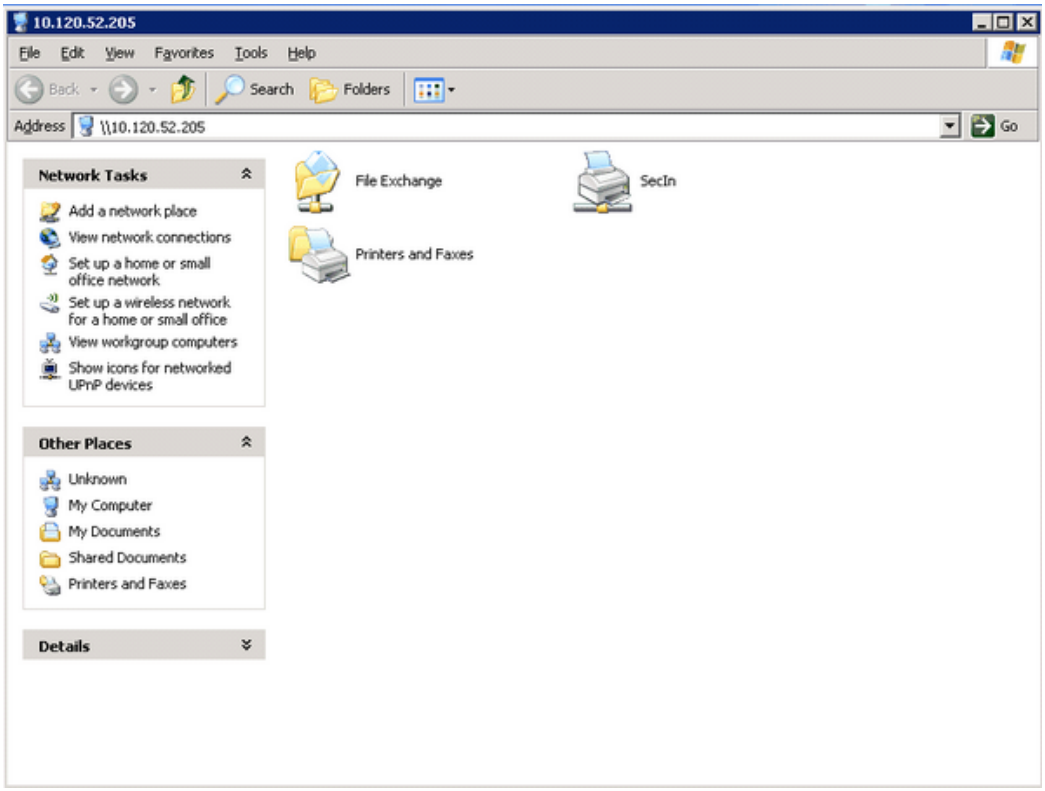
MomClient

The MomClient is still able to connect to the uniFLOW server.



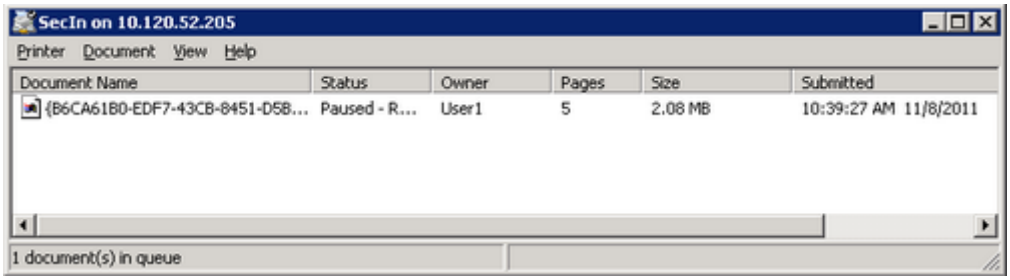
Network Shares / Shared Printers

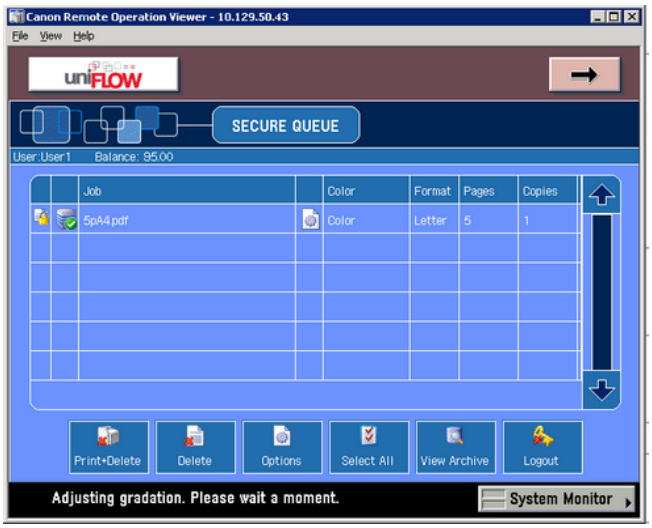
You are able to connect to network shares or shared printers.



Printing

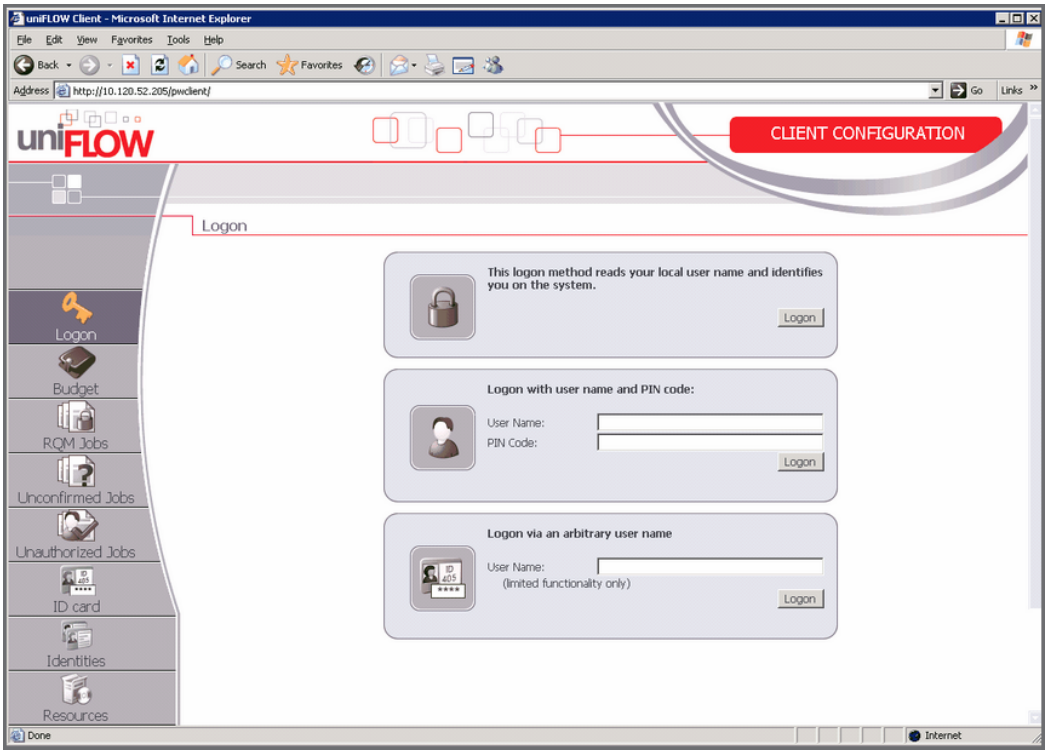
You are able to print on the uniFLOW server.





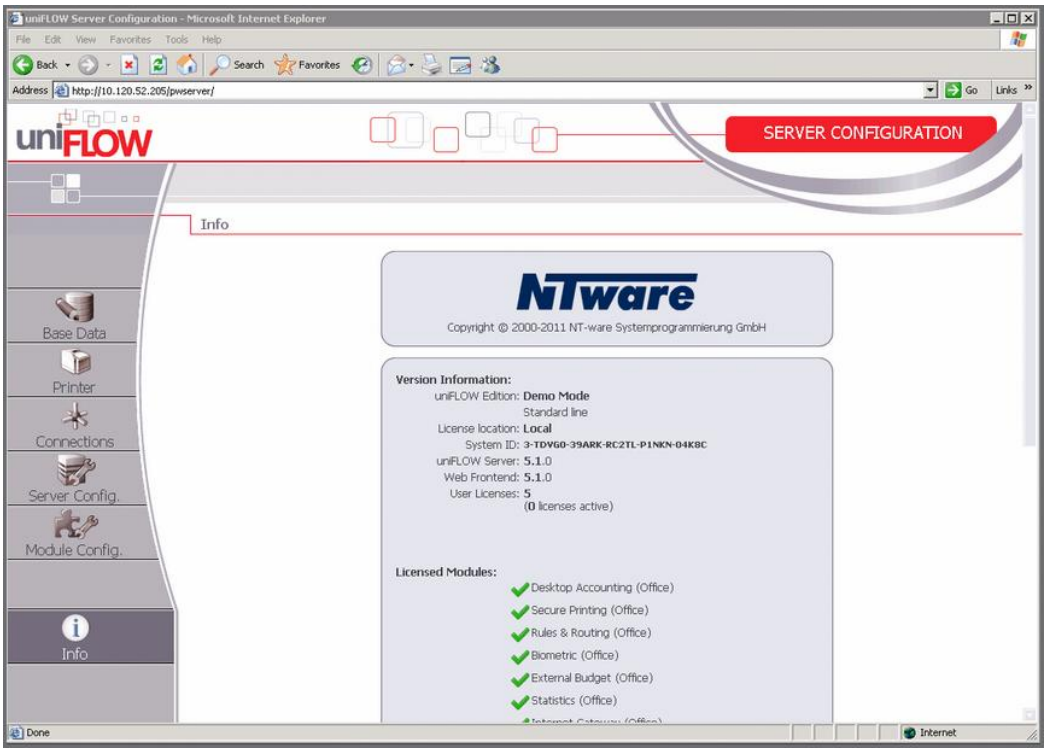
pwclient-website

You are able to access the pwclient-website and log in.



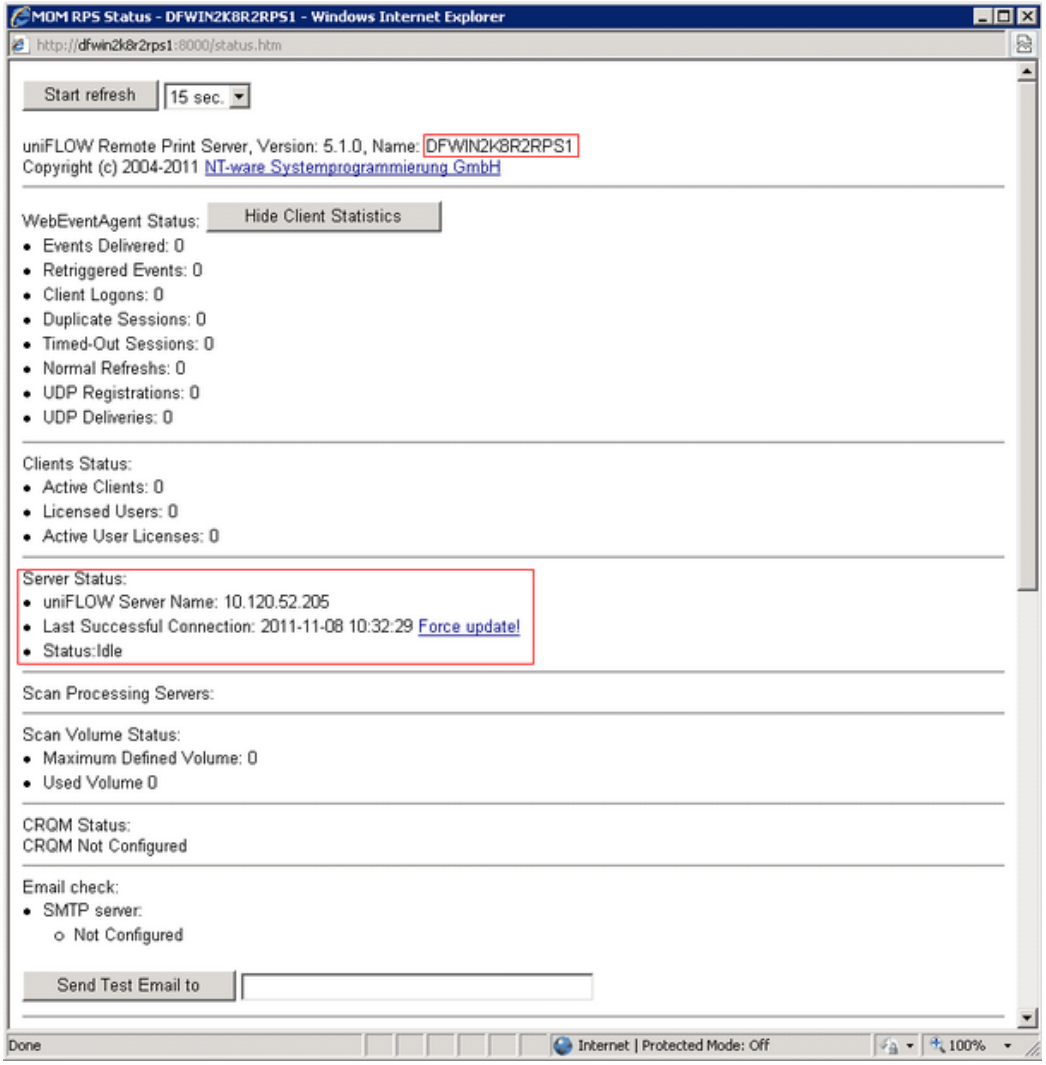
pwserver-website

You are able to access the pwserver-website.

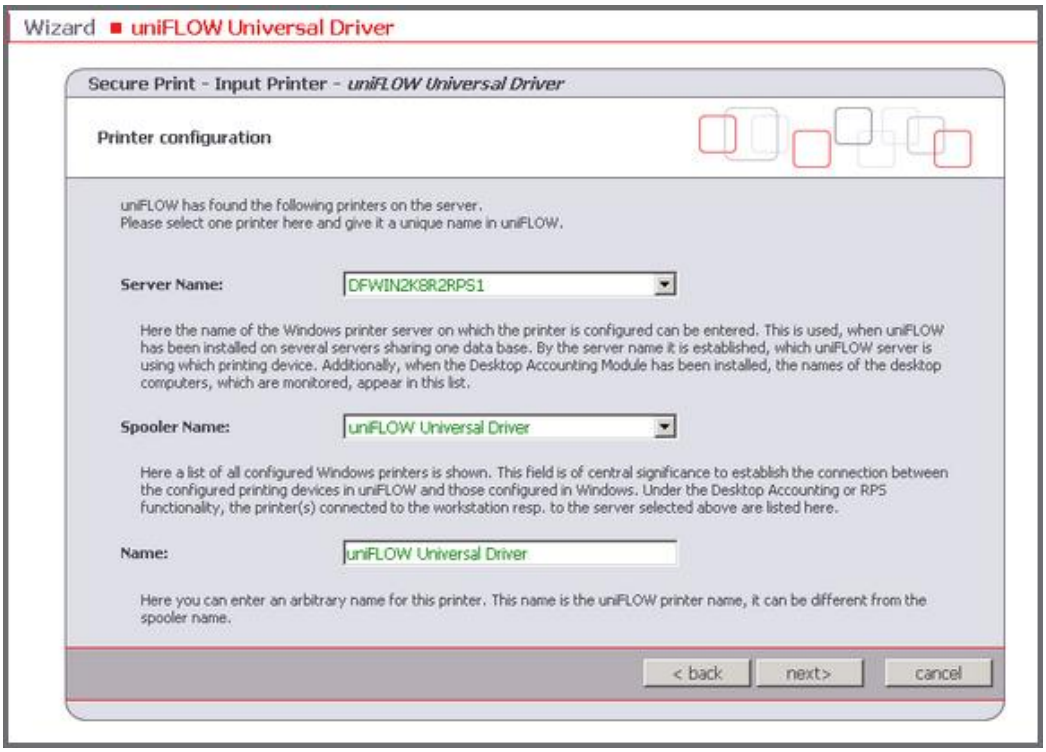


RPS – Windows Server 2008 R2

The RPS under Windows Server 2008 R2 is able to connect to the uniFLOW server.

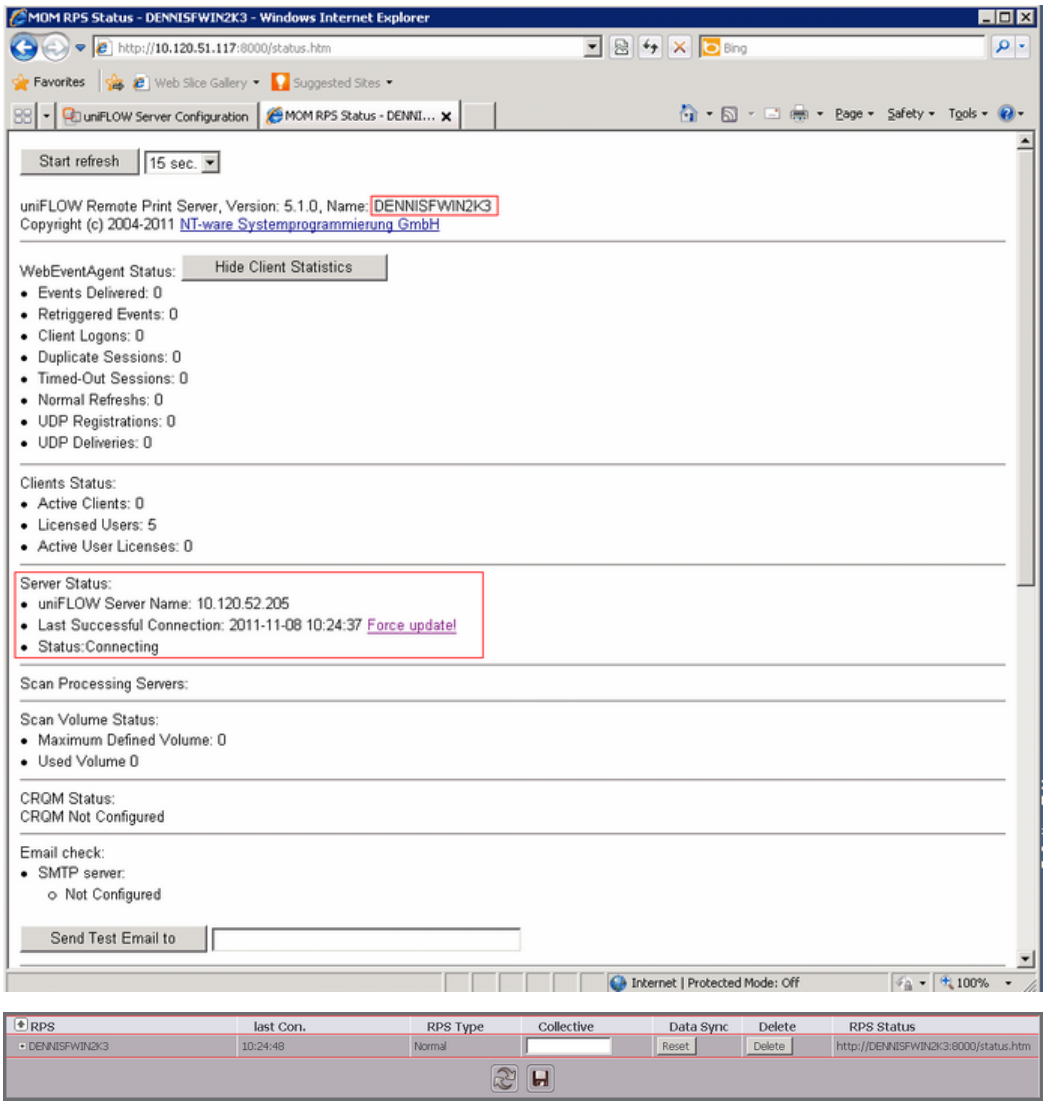


You are able to connect printers from an RPS to uniFLOW.



RPS – Windows Server 2003 (SP2)

The RPS under Windows Server 2003 SP2 is able to connect to the uniFLOW server.



4.5.4 Server (NTLMv2) - Mac Client

This chapter shows test results based on the settings listed in the following:

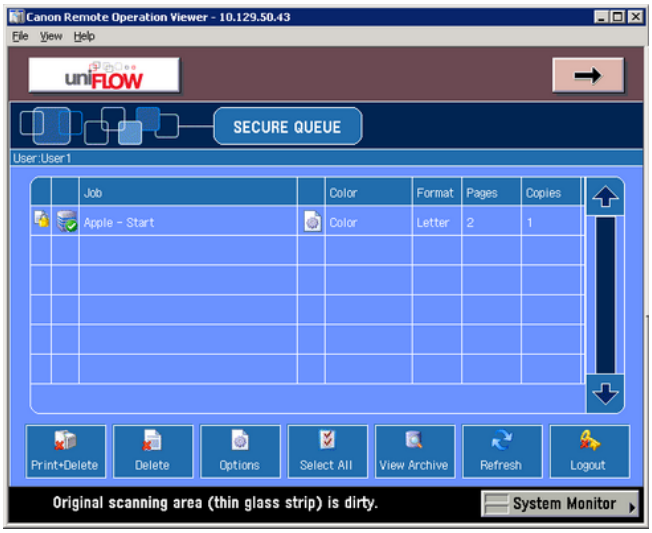
Settings

Server Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Client Settings:	Operating System: MAC OS X 10.4.11 Network security: default security settings

Test Results

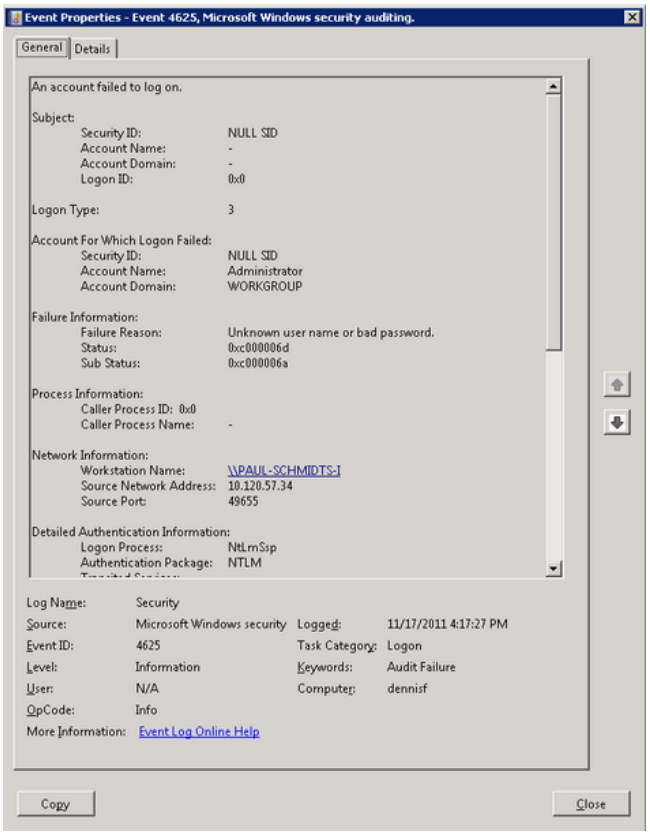
Printing

You are able to print.



Network Shares

You are not able to connect to network shares.



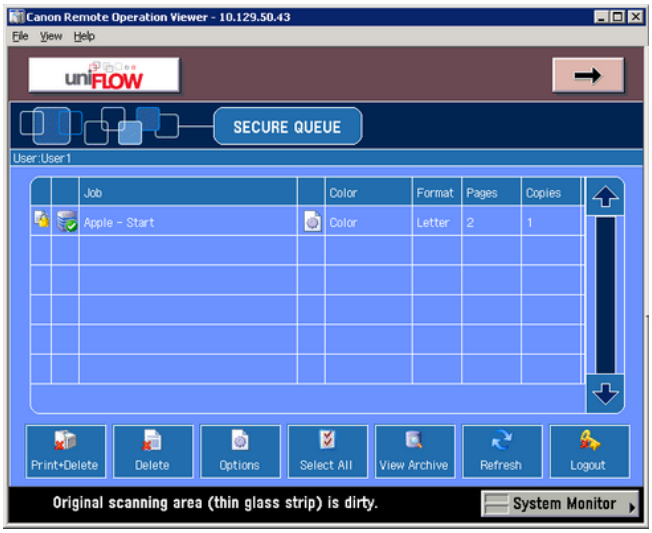
Settings:

Server Settings:	Operating System: Windows Server 2008 R2

	Network security: LAN Manager authentication level: ***Send LM & NTLM***
Client Settings:	Operating System: MAC OS X 10.4.11 Network security: default security settings

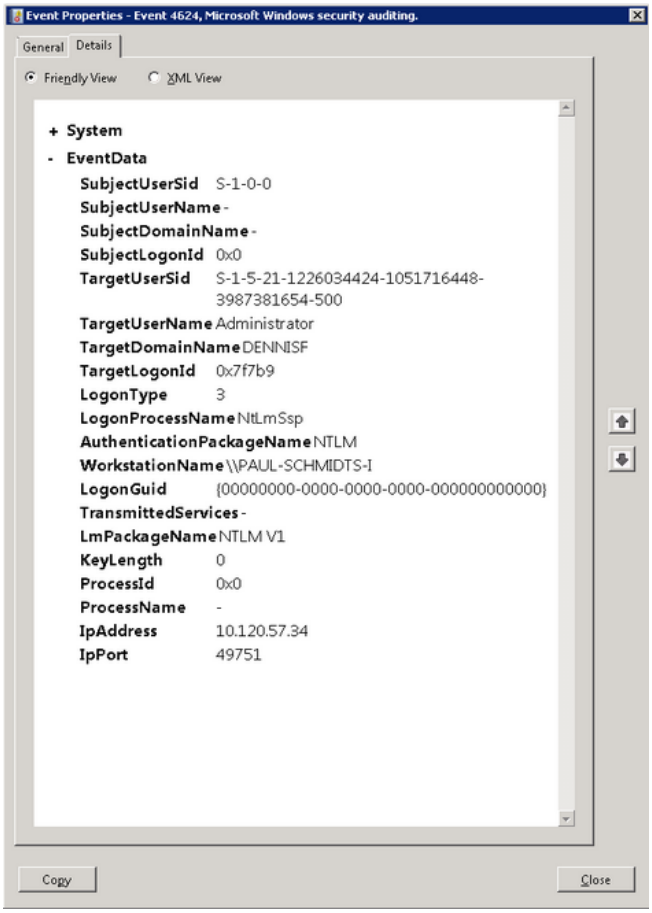
Printing

You are able to print.



Network Shares

You are able to connect to network shares.



4.5.5 Server (NTLMv2) -NetWare RPS

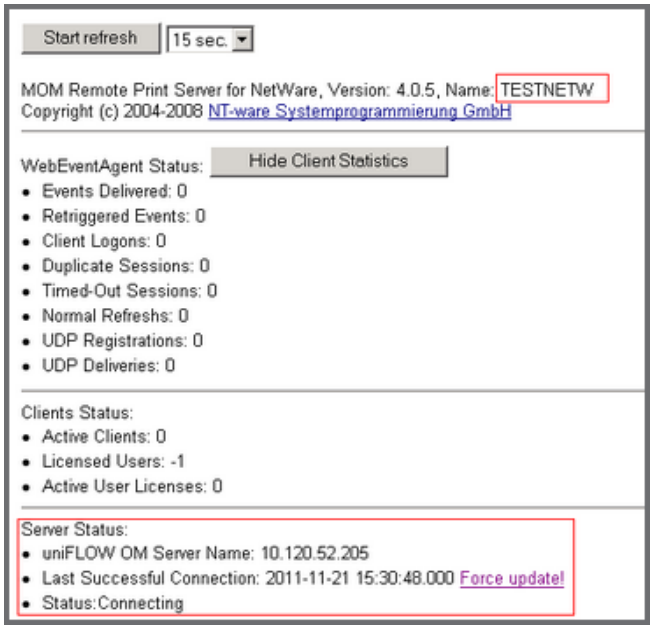
This chapter shows test results based on the settings listed in the following:

Settings

Server Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
RPS Settings:	Operating System: NetWare 6.5 SP8 Network security: default security settings

Test Results

The RPS is able to connect to the uniFLOW server.



4.5.6 Internet Gateway

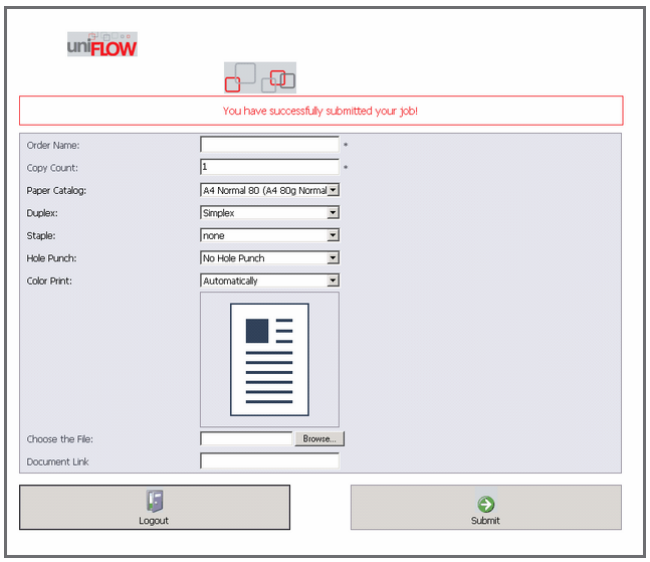
This chapter shows test results based on the settings listed in the following:

Settings

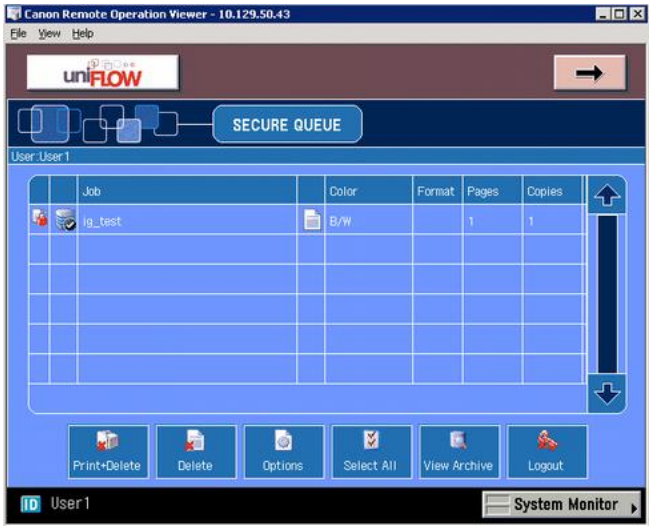
Server Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Client Settings:	Operating System: Windows XP **Setup1:** Network security: LAN Manager authentication level: ***Send LM & NTLM responses*** **Setup2:** Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Internet Gateway Setting:	Operating System: Windows Server 2008 R2 **Setup1:** Network security: LAN Manager authentication level: ***Send LM & NTLM responses*** **Setup2:** Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***

Test Results

You are able to upload jobs from the client to the Internet Gateway.



You are able to pick up your job on an output printer connected to the uniFLOW server.

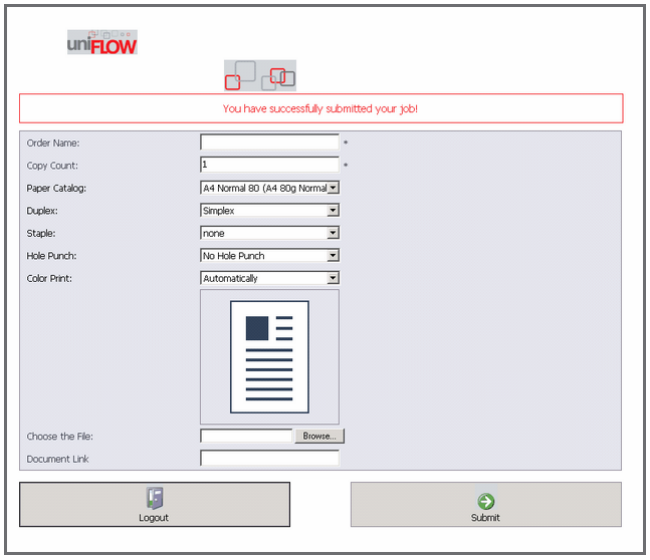


Settings

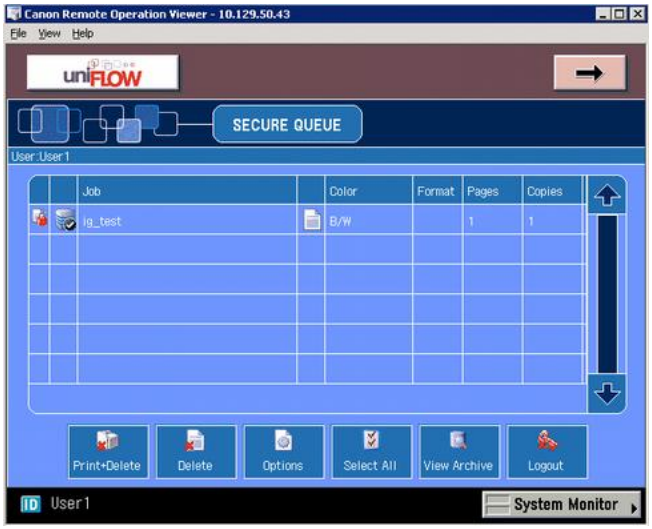
Server Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Client Settings:	Operating System: Windows XP Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Internet Gateway Setting:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send LM & NTLM responses***

Test Results

You are able to upload jobs from the client to the Internet Gateway.



You are able to pick up your job on an output printer connected to the uniFLOW server.

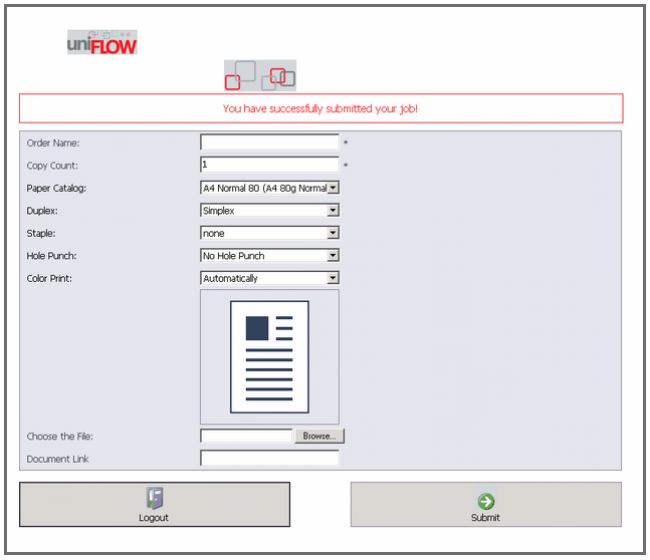


Settings

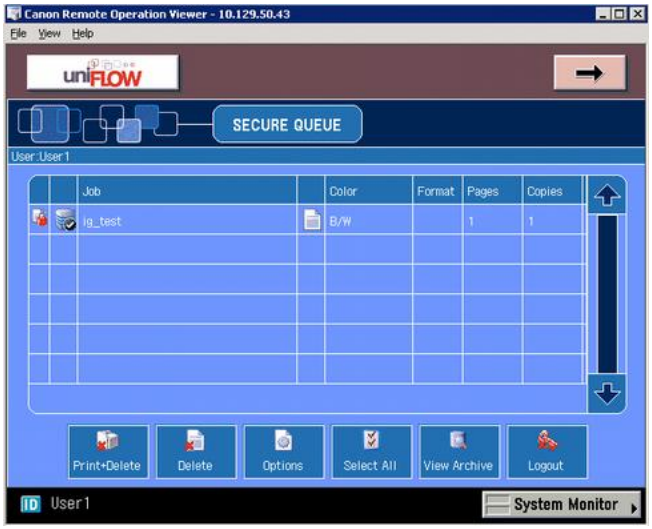
Server Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Client Settings:	Operating System: Windows XP Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***
Internet Gateway Setting:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***

Test Results

You are able to upload jobs from the client to the Internet Gateway.



You are able to pick up your job on an output printer connected to the uniFLOW server.

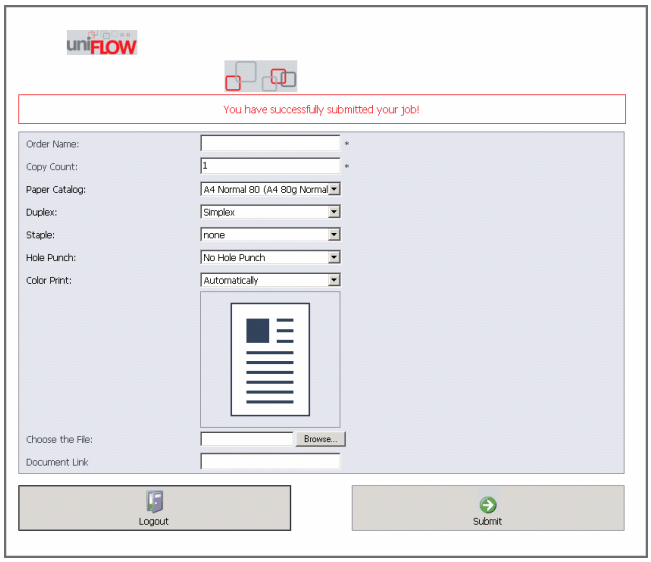


Settings

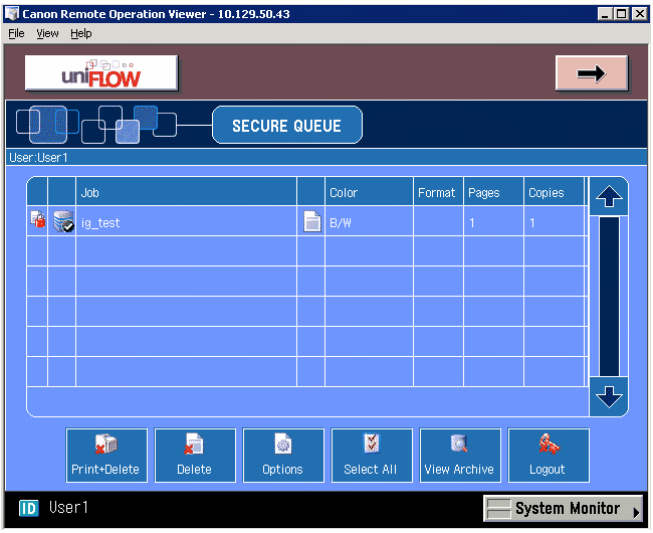
Server Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: Send NTLMv2 response only, Refuse LM & NTLM
Client Settings:	Operating System: Windows XP Network security: LAN Manager authentication level: Send NTLMv2 response only, Refuse LM & NTLM
Internet Gateway Settings:	Operating System: Windows Server 2008 R2 Network security: LAN Manager authentication level: Send NTLMv2 response only, Refuse LM & NTLM

Test Results

You are able to upload jobs from the client to the Internet Gateway.



You are able to pick up your job on an output printer connected to the uniFLOW server.



4.5.7 Scanning

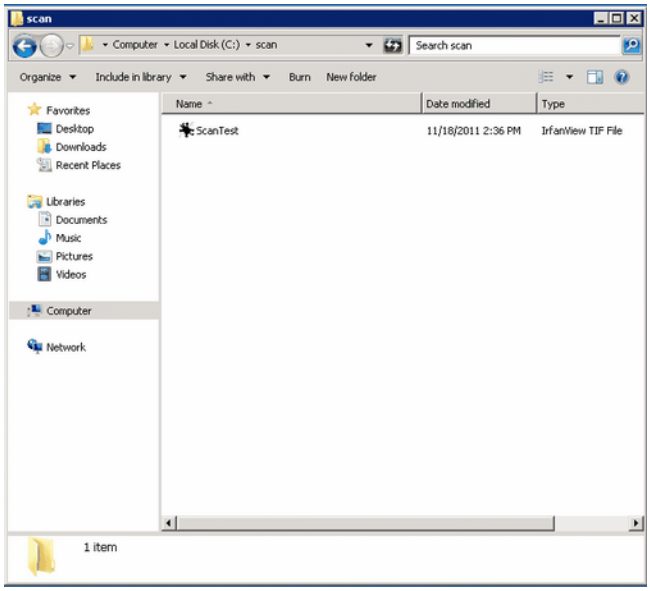
This chapter shows test results based on the settings listed in the following:

Settings

Server Settings:	Operating System: Windows Server 2008 R2 **Setup1:** Network security: LAN Manager authentication level: ***Send LM & NTLM responses*** **Setup2:** Network security: LAN Manager authentication level: ***Send NTLMv2 response only, Refuse LM & NTLM***

Test Results

You are able to scan to a folder.



4.6 Secure LDAP (LDAPS or LDAP over SSL)

When importing user data from an Active Directory or Novell eDirectory, Secure LDAP can be used on the uniFLOW server and Windows RPS. A NetWare RPS support for Secure LDAP does not yet exist.

Further information regarding the setup and configuration can be found in the uniFLOW User Manual. Please keep in mind that certificates are mandatory.

The connection to the LDAP system is a read only connection.

4.7 SMTP

When configured, uniFLOW/RPS relays emails from the MFP to the internal mail server. SMTP Secure (SMTPS) is scheduled for a later version of uniFLOW.

If there are security concerns regarding this topic, the inbound SMTP traffic should be restricted to the uniFLOW server / RPS.

4.8 Web Applications

4.8.1 Web Applications: Secure pwserver on Windows 2008 (R2)

Configuring URL Authorization Rules in IIS 7

This chapter applies to Windows Server 2008 and Windows Server 2008 R2.

You can grant or deny specific computers, groups of computers, users, groups or domains access to sites, applications, directories, or files on your uniFLOW server. To achieve that, you need to install and configure the ***URL Authorization*** role feature of IIS 7.

The following example shows, how you deny access for all common users to the uniFLOW Server Configuration web (pwserver) but allow access to administrators only.

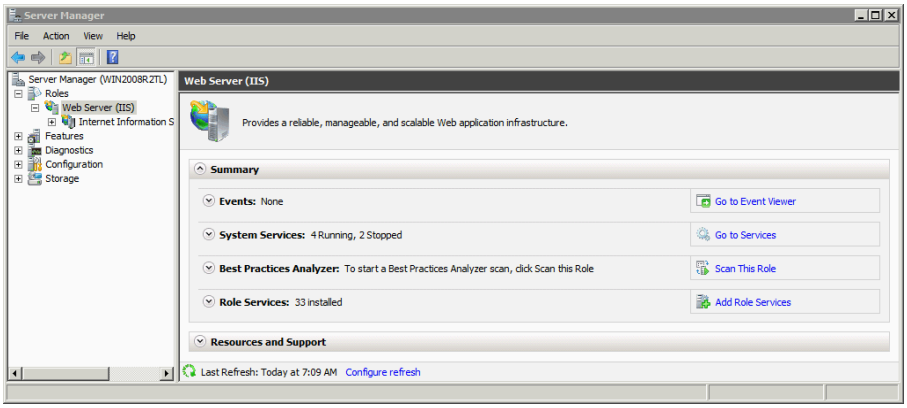
For more information about this IIS security feature, please refer to:

http://technet.microsoft.com/en-us/library/cc772206%28v=ws.10%29.aspx

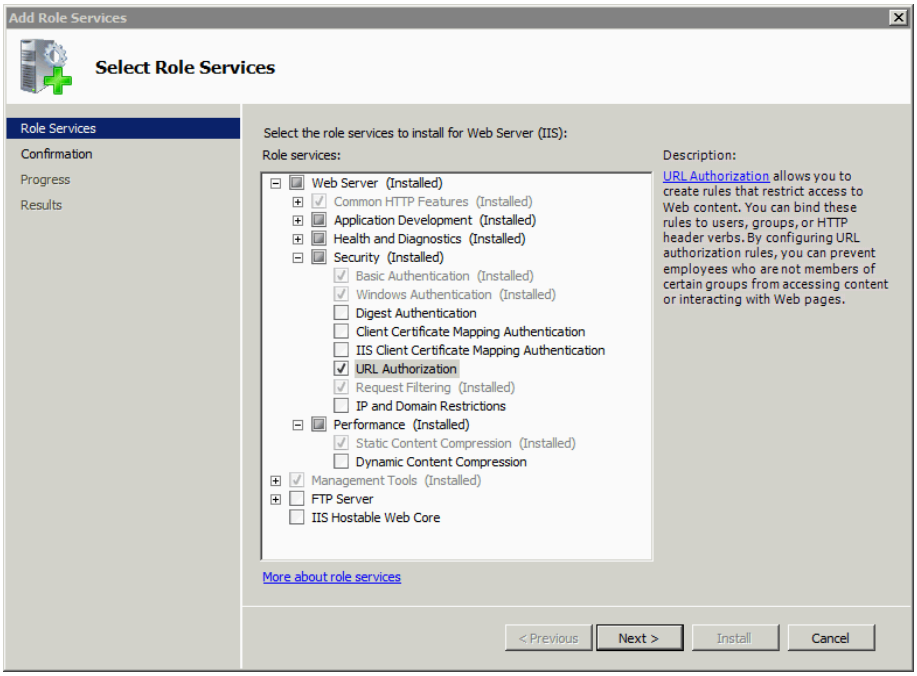
Installing the IIS URL Authorization Role Feature

- Open the ***Server Manager*** and navigate to ***Roles – Web Server (IIS)***.

- Select ***Add Role Services***.



- Check ***URL Authorization*** and click ***Next***.



- Check your settings in the next screen and click ***Install*** to confirm the installation.
- Click ***Close*** when the installation is completed.

Configuring the IIS URL Authorization Role Feature

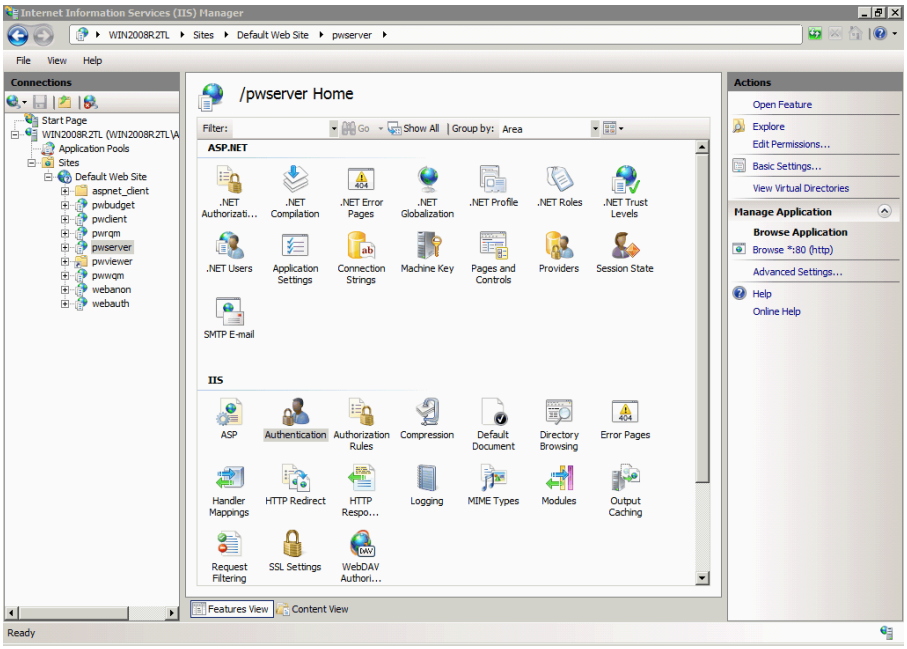
Before you continue configuring the ***URL Authorization*** role feature, it is recommended to create a security group on the uniFLOW server or in Active Directory and add all users who should get permission to access the uniFLOW Server Configuration (pwserver) web.

In this example we have created a local security group called "uniFLOW". Members of this group will gain access to the uniFLOW Server Configuration later.

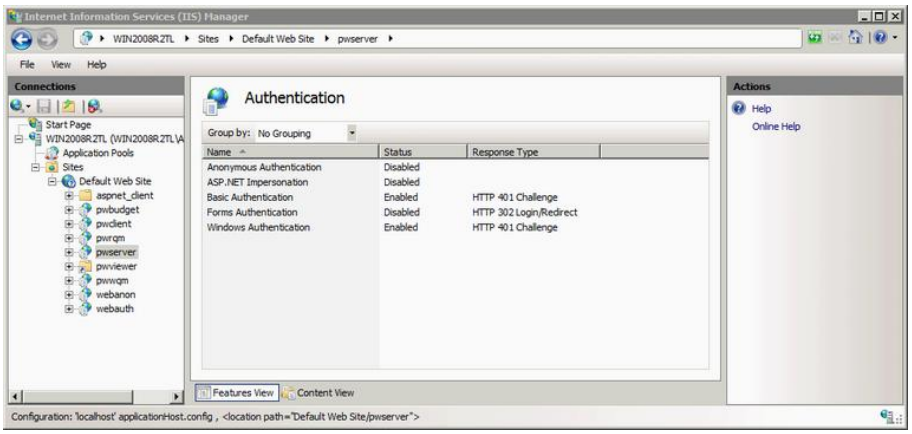
Afterwards, proceed as follows:

- Open the ***Internet Information Services (IIS) Manager***.
- Navigate to ***Sites > Default Web Site***

- Select ***pwserver*** and double click the ***Authentication*** feature under ***IIS***.

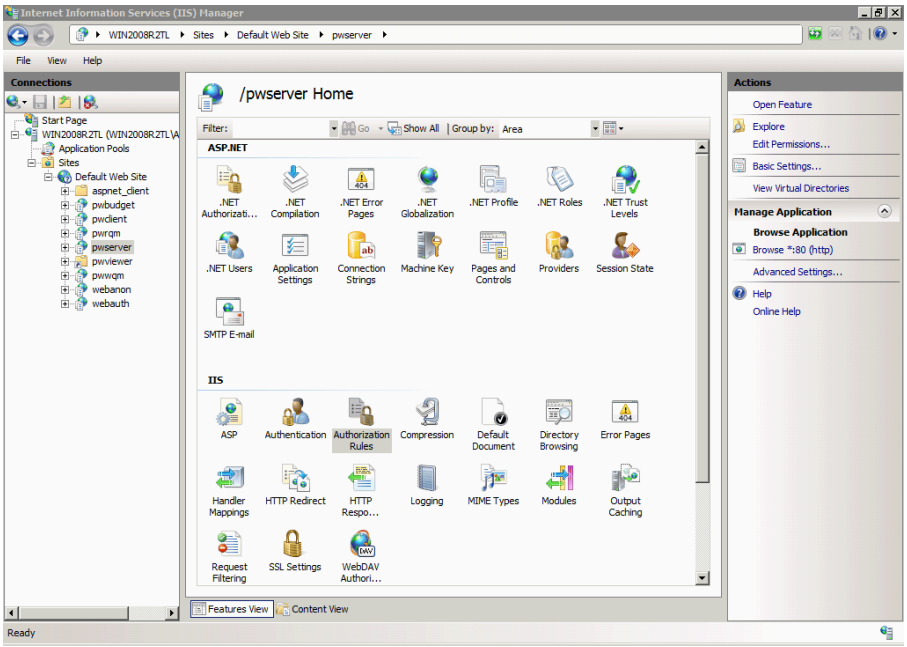


- Right click on ***Anonymous Authentication*** and select ***Disable***.
- Enable ***Basic Authentication*** and ***Windows Authentication***.
- Make sure authentication is configured as can be seen in the following screenshot:

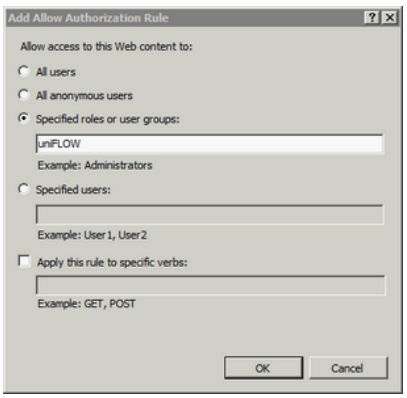


- Navigate to ***Roles – Web Services (IIS) – Sites - Default Web Site***.

- Select ***pwserver*** and double click the ***Authorization Rules*** feature under ***IIS***.



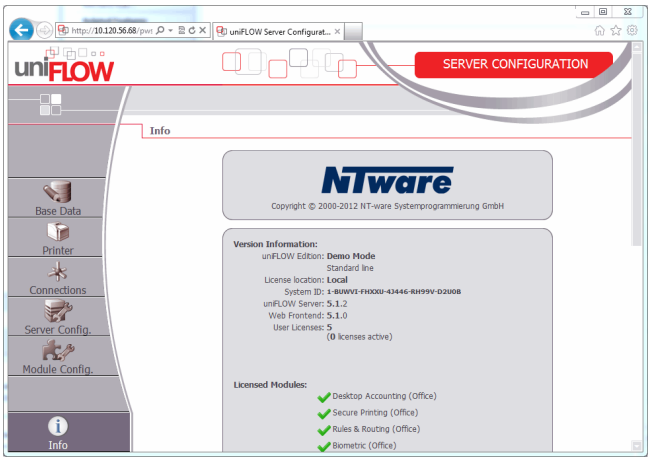
- Remove existing authorization rule(s). To do so, select the rules, right click and select ***Remove***.
- Add a new allow rule. To do so, select ***Add Allow Rule*** from the ***Actions*** pane.
- Select ***Specified roles or user groups*** and add a domain or local group you would like to grant access to the pwserver site in following format:
  - Domain Group: *DOMAIN\uniFlowAllowDomainGroup*, for example *NTware\uniFLOW*
  - Local Group: *uniFLOW*



- Test the authorization rule by opening the browser and navigating to *http://<uniFLOW server>/pwserver*.
- Enter credentials for a user who is a member of the group authorized to access pwserver.

If ***Windows Authentication*** enabled and currently logged on user is a member of the group for which access is granted, user credentials are automatically passed onto IIS and no manual logon is required.

- Authenticated user is granted access to the uniFLOW Server Configuration page.



4.8.2 Web Applications: SSL/TLS

4.8.2.1 uniFLOW < V5.2

Issue

There are a number of web applications running on the uniFLOW server, all of which are running over HTTP which is a clear text protocol. As such, passwords and unique user ID values are submitted through an unencrypted connection and are vulnerable to capture by an attacker in a suitable position on the network. This includes any malicious party located on the user's own network or within the application's hosting infrastructure. Even if switched networks are employed at some of these locations, techniques exist to circumvent this defense and monitor the traffic passing through switches.

The following uniFLOW system options are using a standard or compressed HTTP connection for the communication with the uniFLOW server:

- uniFLOW Client for Windows (cf. chapter uniFLOW Client via HTTPS (see "uniFLOW Client for Windows via HTTPS" on page 52))
- uniFLOW Client for Mac
- MEAP Login Manager
- MEAP - uniFLOW Secure/Public Printing Applet
- EAI (Embedded Application Interface) - Third Party Applets

Resolution

The web applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. It is therefore recommended that all uniFLOW web applications are configured to use HTTPS rather than HTTP.

http://support.microsoft.com/kb/324069/en-us

Note that this procedure assumes that your site already has a certificate assigned to it.

4.8.2.2 uniFLOW >= V5.2

Usage of HTTPS in uniFLOW V5.2 onwards

In order to provide a secure communication, uniFLOW makes use of HTTPS as default communication protocol. For that reason, please consider the following:

- HTTPS is the required default communication protocol for uniFLOW. A redirection mechanism from HTTP to HTTPS is in place.
- In order to use HTTPS as a communication protocol, a self-signed certificate is created and installed in the IIS during the installation of uniFLOW. You can replace the certificate in the IIS afterwards in case a different certificate should be used. The self-signed certificate is unique to each installation and is valid for 10 years. Afterwards it needs to be renewed.
- We recommend to add this self-signed certificate to the "Trusted Root Certification Authorities" certificate store, in order to prevent messages like "There is a problem with this website's security certificate.", when accessing uniFLOW web pages in a browser (see chapter ***Certificate Installation*** in the uniFLOW User Manual / Installation Manual or MOMKB-681 (https://web.nt-ware.net/its/browse/MOMKB-681)). This should be done after the uniFLOW installation.
- In case a different certificate shall be used, this has to be manually acquired and installed in the IIS manager. This may be required for example, if you need a certificate from a trusted root certification authority. You can get such certificates for example from VeriSign or others.

In case you need to replace or renew the certificate in the IIS, please refer to the Microsoft Knowledgebase.

Updating uniFLOW and HTTPS

In case you want to update uniFLOW using the uniFLOW Update Wizard, please note that the wizard will not set the "Require Secure Channel" flag in IIS by default. Otherwise, this would lead to the problem that RPS's and clients which have not yet been updated are not able to connect to the uniFLOW server anymore. Please refer to chapter ***HTTP/HTTPS Communication*** in the uniFLOW User Manual / Installation Manual for details.

For details about upgrading Remote Print Servers, please refer to the respective subchapter of the ***uniFLOW Update/Upgrade*** chapter in the uniFLOW User Manual / Installation Manual.

4.8.2.3 IIS Security

There are certain technologies like cross-site-scripting that can exploit a security vulnerability where cookies are set without the HttpOnly flag.

The following instructions show how to configure the IIS to prevent this.

The following procedure works with IIS V7.0 (Windows Server 2008) or higher.

It was tested by NT-ware with IIS V7.5 on Windows 2008 R2.

- Download and install the URL Rewrite Module from http://www.iis.net/learn/extensions/url-rewrite-module/using-the-url-rewrite-module (http://www.iis.net/learn/extensions/url-rewrite-module/using-the-url-rewrite-module).
- In the root WWW directory (usually *C:\inetpub\wwwroot*) open the file *web.config* in a text editor. If it does not exist, create an empty text file with this name and copy the complete XML code listed below into the file. If the file already exists, copy only the `<rewrite>` section from below into the section `<system.webserver>` as seen below.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
      <system.webServer>
            <rewrite>
              <outboundRules>
                <rule name="Add HttpOnly" preCondition="No
HttpOnly">
```

```
                    <match   serverVariable="RESPONSE_Set_Cookie"
pattern=".*" negate="false" />
                    <action     type="Rewrite"     value="{R:0};
HttpOnly" />
                    <conditions>
                    </conditions>
                </rule>
                <preConditions>
                    <preCondition name="No HttpOnly">
                        <add       input="{RESPONSE_Set_Cookie}"
pattern=".*" />
                        <add       input="{RESPONSE_Set_Cookie}"
pattern="; HttpOnly" negate="true" />
                    </preCondition>
                </preConditions>
              </outboundRules>
            </rewrite>
      </system.webServer>
</configuration>
```

- To finish the configuration save the file and restart the IIS and uniFLOW.

4.8.3 Web Applications: Different Application Pools

Issue

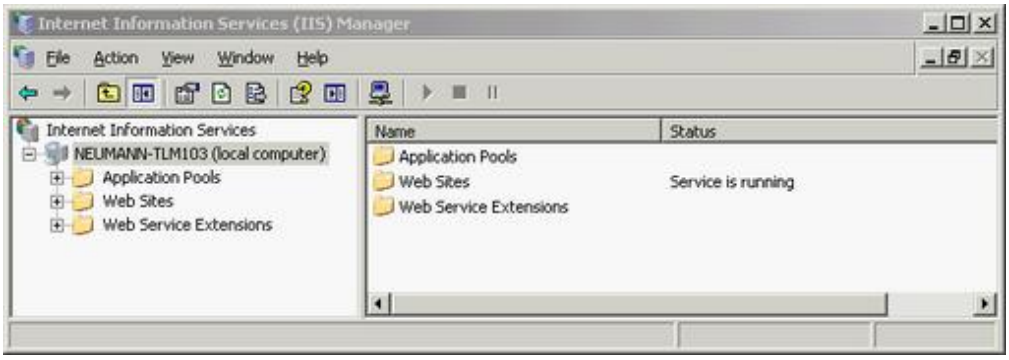
All Web Applications make use of the same application pool within uniFLOW and the RPS. This vulnerability makes accessing shared resources easy should an individual application function become compromised.

Resolution

It is advised that each separate web application have it’s own application pool. The following descriptions show how to achieve that for the IIS 6 and the IIS 7.

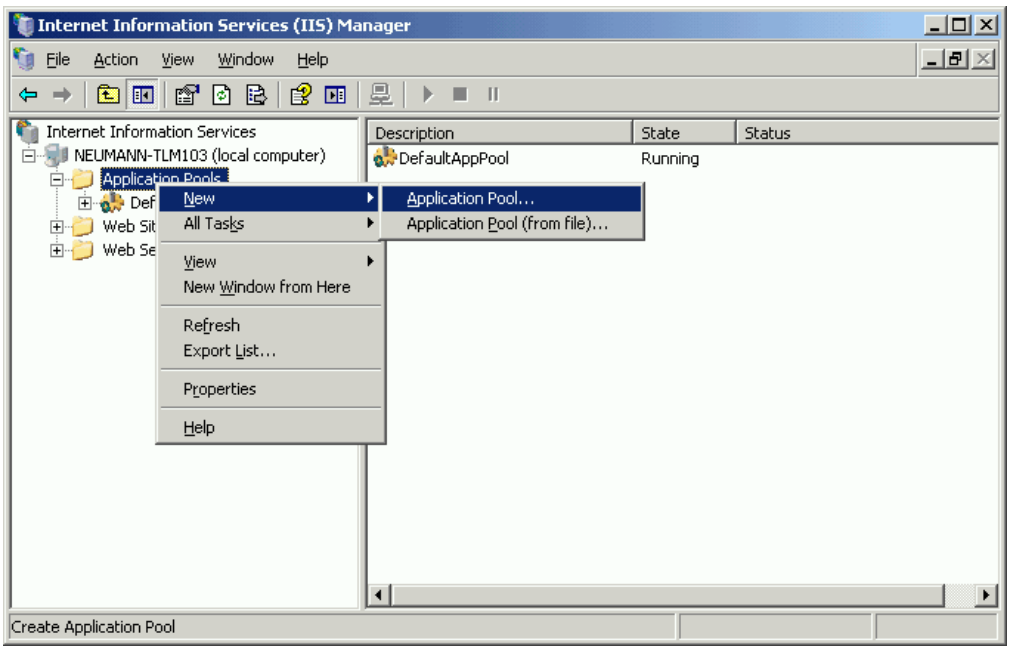
IIS 6

- Open Start → Administrative Tools → Internet Information Service (IIS) Manager



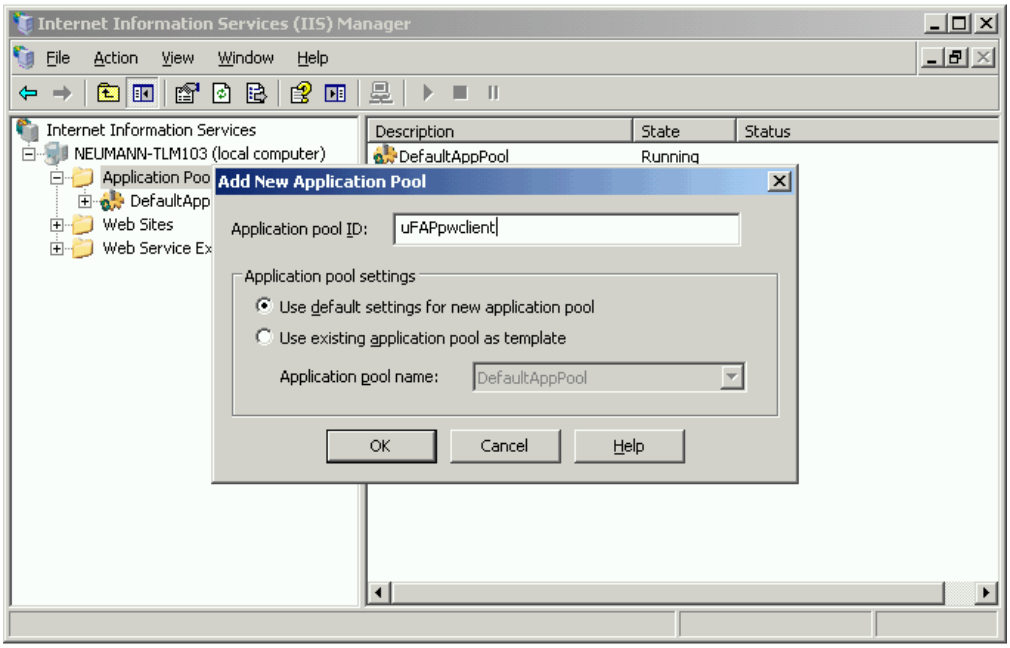
- Right Click ***Application Pools*** and select ***New*** à ***Application Pool***…

Ensure you create a separate ***Application Pool*** for each web application instance.

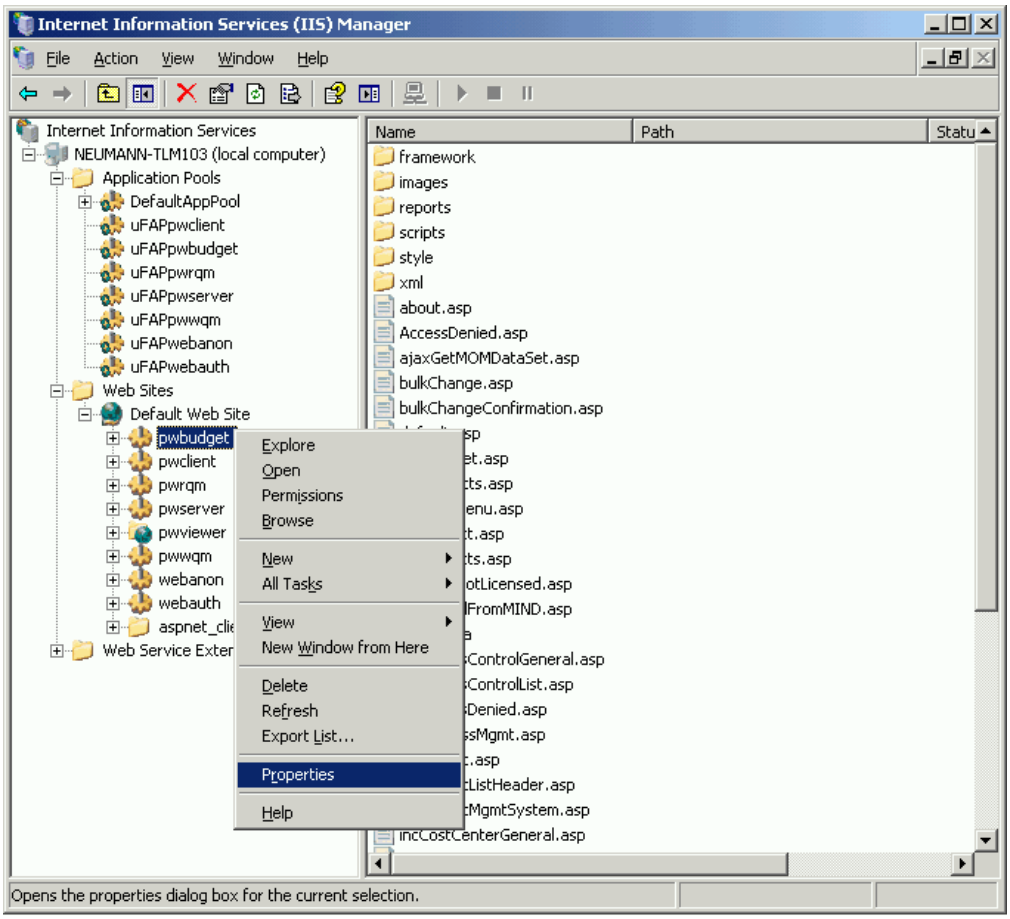


- In the next pop-up enter the new application pool name (***Application pool ID***).

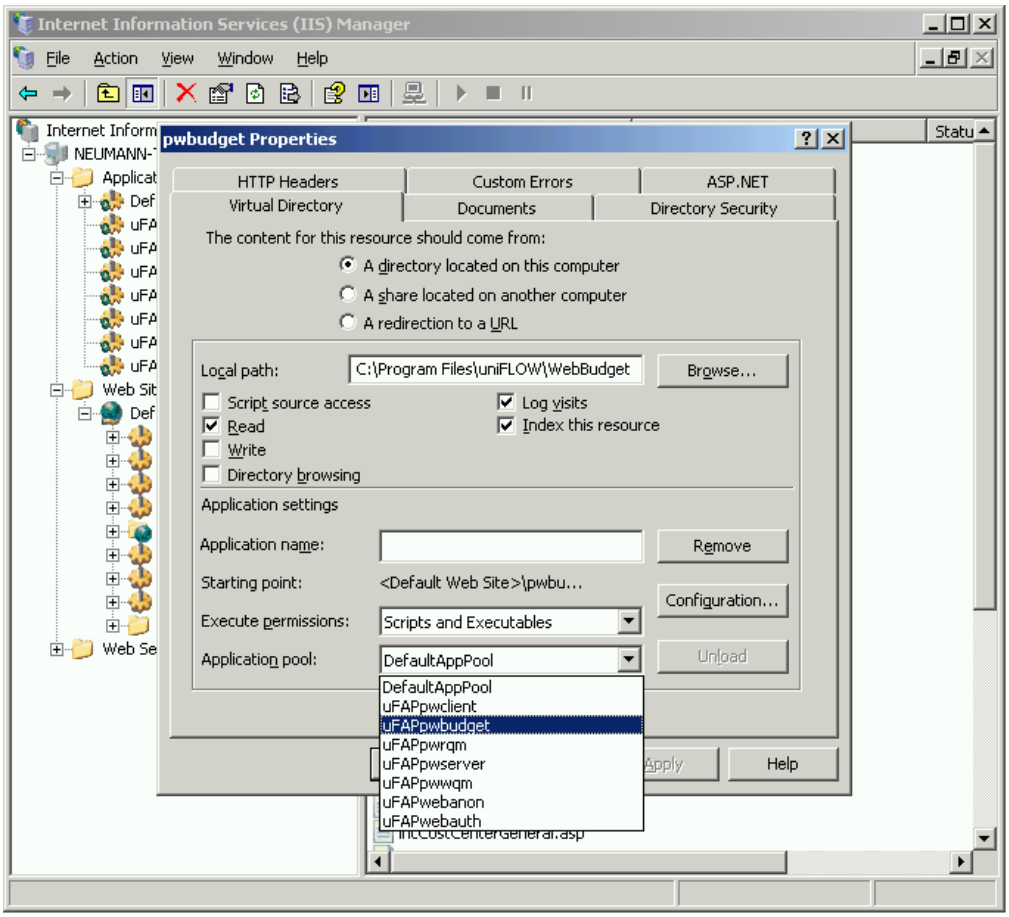
- Repeat these steps for each web application instance and name them accordingly.



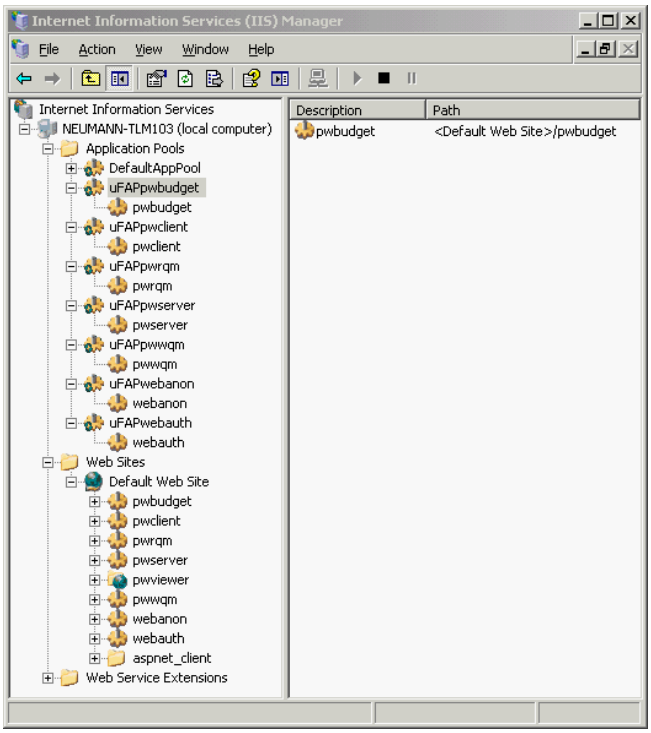
- Now assign each web site to the respective application pool.
- Right click each web site and select ***Properties***.



- Use the drop down list and select the respective ***Application pool***.

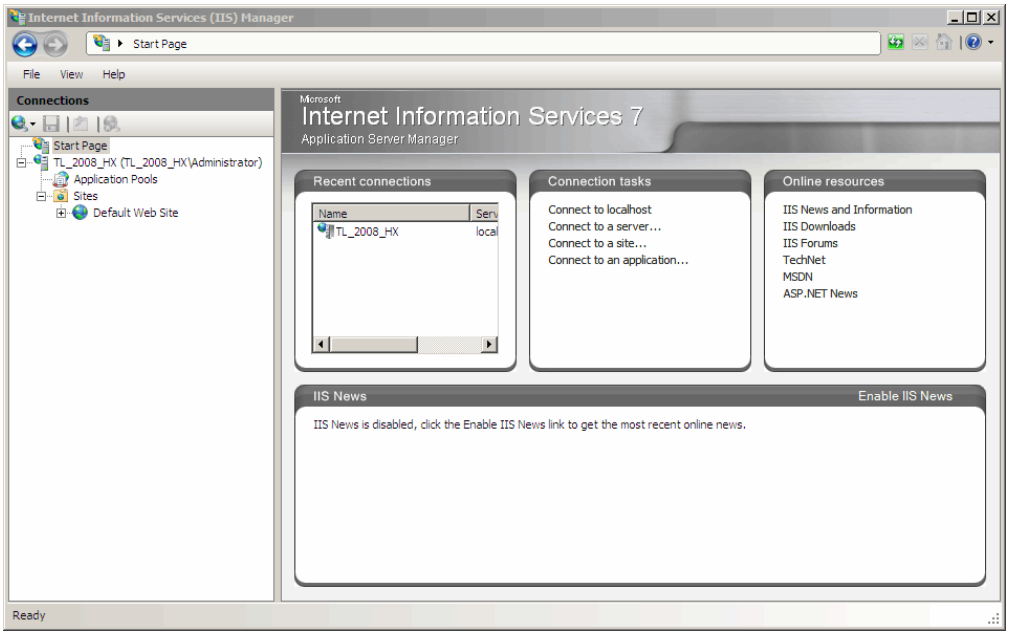


- Once all sites have been re-mapped then the application pools should look like this.



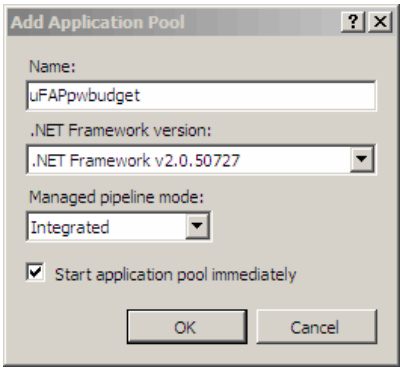
IIS 7

- Open the Internet ***Information Services (IIS) Manager***



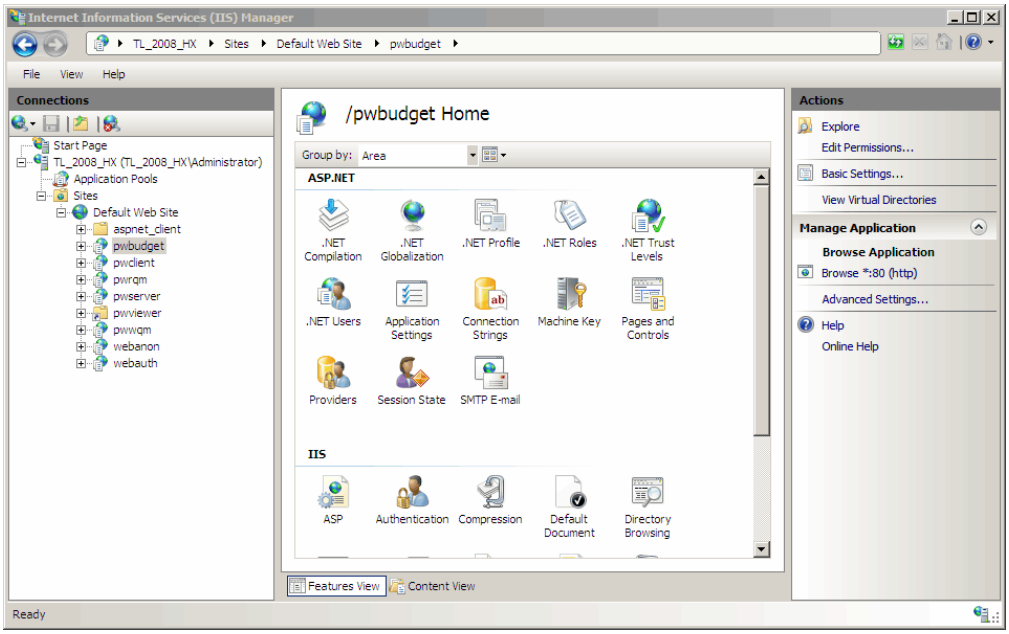
- Select ***Application Pools***
- In the right hand pan select the ***Add Application Pool...*** link
- Enter the required information for the new application pool.

Ensure you create a separate ***Application Pool*** for each web application instance.

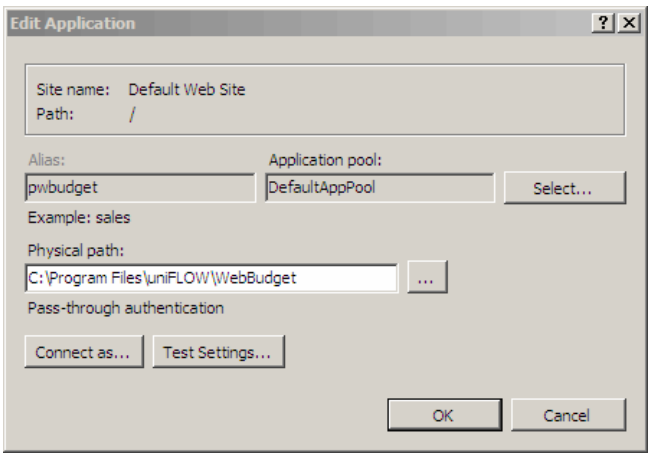


- Once all application pools have been created you need to remap all the web sites.

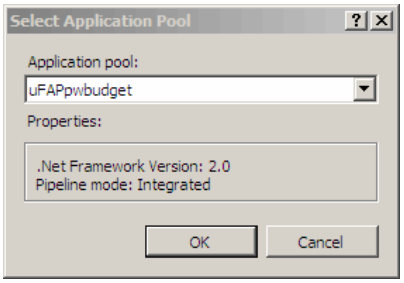
- Select each web site and in the right hand pan select the ***Basic Settings...*** link.



- On this dialog box click on ***Select...*** to select the respective application pool.

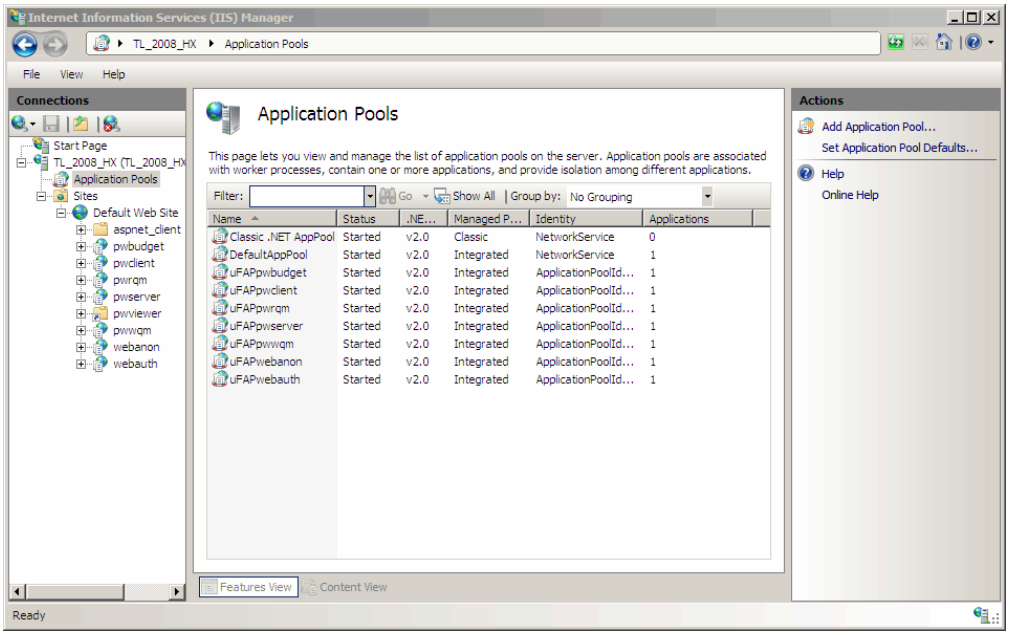


- Use the drop down list to select the new application pool.



- Repeat these steps for each web application instance.

- After all changes have been made it is advisable for an IIS reset to be carried out from the command line.



5 uniFLOW Remote Print Server

5.1 uniFLOW V5.2 RPS Communication

In uniFLOW V5.2 and later, the synchronization of connected Remote Print Servers is secured with signed communication packets. With this functionality, the identity of a Remote Print Server is verified during a synchronization process. Please be aware that this functionality is completely independent from any HTTPS settings used in an installation.

Note that this is only valid for a new installation. If you have upgraded from an older version, the functionality might be different, depending on the settings you have chosen while using the uniFLOW Update Wizard.

Please refer to the uniFLOW User manual chapter ***uniFLOW Update/Upgrade*** for further details.

6 uniFLOW Client

6.1 uniFLOW Client for Windows via HTTPS

This chapter is relevant for uniFLOW Clients older than V5.2. Since uniFLOW V5.2 the uniFLOW Client communicates via HTTPS by default.

The uniFLOW Client for Windows communicates by default via HTTP. However, it is possible to enable a secure HTTPS communication.

To enable HTTPS communication, you have to do the following:

1. Create a Server Certificate in the IIS of the uniFLOW server and enable HTTPS communication.
2. Install the uniFLOW Client for Windows as usual.
3. Import the Server Certificate on the client computer. This can be done by simply double clicking the exported certificate on the client computer which starts the ***Certificate Import Wizard***. In the ***Certificate Import Wizard*** select the ***Trusted Root Certification Authorities / Local Computer*** store.
4. Add the following Windows Registry Key on the client computer:
   Generate a DWORD value named ***UseHTTPS*** with value "1" to enable and "0" to disable HTTPS communication.
   System Key:
   `[HKEY_LOCAL_MACHINE\Software\NT-ware\Mom\MomClient]`

   Value Name: `UseHTTPS`
   Data Type : `REG_DWORD`
   Value Data: `0/1`
5. Amend the ***ServerName*** registry key as follows:
   System Key:
   `[HKEY_LOCAL_MACHINE\Software\NT-ware\Mom\MomClient]`

   Value Name: `ServerName`
   Data Type : `Reg_SZ`
   Value Data: `<uniFLOW server IP>`
6. Restart the Windows Client.

6.2 uniFLOW Client for Mac via HTTPS

HTTP/HTTPS Communication

Since uniFLOW V5.2, the communication between the clients and the uniFLOW server runs via HTTPS by default. This is the case for any fresh standard installation of uniFLOW. For that reason, the new uniFLOW Client for Mac version can communicate with the uniFLOW server only via the HTTPS protocol.

If you have upgraded the uniFLOW server from an older version than V5.2 and the default communication runs via HTTP, the uniFLOW Update Wizard will install a certificate to enable a communication via HTTPS but does not enable the "Require Secure Channel" flag in the IIS. This makes a communication via HTTP and HTTPS possible. This means that in case you have upgraded uniFLOW, all old uniFLOW Clients for Mac will still work, although they still communicate via HTTP. In case a secure communication is required, you can upgrade all clients to the new version which communicates only via HTTPS.

7 uniFLOW Components

7.1 uniFLOW Mobile Print Service for iPad or iPhone

This chapter provides some detailed security information about the uniFLOW Mobile Print Service for iPad or iPhone (MomApSvc).

iOS Device to MomApSvc

- When the MomApSvc is configured with "user name / password" user identification, the MomApSvc requires from the iOS device to use a secure connection (TLS) for each print job request. If the connection is not secured, the MomApSvc will reject the print job request. This is because the credentials are sent together with the print job request.
- For other user identification methods than "user name / password", the MomApSvc allows print jobs coming over non-secure connections.
- In the current version, the MomApSvc certificate is self-signed and generated on every service restart.

MomApSvc to uniFLOW Server

- In order to verify the credentials, the MomApSvc makes a request to the uniFLOW server. Before doing that, the payload of the credentials is encrypted using a custom encryption method that uses a key which changes for each request.
- Starting with uniFLOW V5.3, the MomApSvc can verify the credentials using secure connection to uniFLOW.

- Credentials are never stored by MomApSvc, but they might be cached/remembered on the iOS device.

Additional Information

- The credentials are encrypted with a 3DES key that changes on each login request. In order for uniFLOW to be able to decrypt the credentials, the MomApSvc sends the 3DES key to uniFLOW, but is encrypted using an RSA key that both uniFLOW and MomApSvc know.

For uniFLOW V5.4 or higher

- Besides IPP, the service supports IPPS (secure IPP). In the latter, the communication is done over secure TLS connection.
- The MomApSvc certificate is persistent and there is an option to import key/certificate pairs.

8 Additional Software

This chapter lists additional software which frequently runs on the uniFLOW server.

8.1 iW SAM

This chapter gives security related and background information about iW SAM. It answers FAQs about how iW SAM works in background.

How are images stored on the MEAP device by the iR Agent and what format is used to store the files?

The image after print, scan or copy will be stored onto the HDD for iW SAM on the devices.

The format of the image data is as follows:

- Canon Original Format
- TIFF
- JBIG
- JPEG
- TEXT
- etc.

How are images transferred to the iW SAM Express Server from the MEAP device by the iR Agent and what format is this?

The stored image data by the above format will be transferred from the iR Agent to the iW SAM Express Server by using SwA (SOAP Messages with Attachment) as the protocol.

Over which port is the imageRUNNER sending the files to the iW SAM Express Server?

In case HTTP is used, it will be the port number 80.

In case HTTPS is used, it will be the port number 80 and 443.

How is the image transferred from the iW SAM Express Server to the uniFLOW server?

Explain the process of how the image is arriving from the device and being converted and sent to the shared folder in uniFLOW.

The iW SAM Express Server will receive the image data and job log data from the iR Agent by using SwA (SOAP Messages with Attachment). This data will be stored into the "Spool Folder" on the iW SAM Express Server. The image format in the "Spool Folder" will be the same as listed above.

Afterwards, the "DataProcessService", which is the one of the internal module on the iW SAM Express Server, will convert the image data format in the "Spool Folder" from the current format to the format uniFLOW understands, which is the JPEG or TIFF format with the resolution changed and/or the image rotated.

The "ExportService", which is also the another internal module on the iW SAM Express Server, will then store the new formatted data into the "ExportFolder" which is configured in iW SAM. uniFLOW will then retrieve that image data from the "ExportFolder".

8.2 Acrobat Reader

Issue

The version of Adobe Reader installed on the uniFLOW application server is outdated. An older version can be affected by multiple vulnerabilities.

Resolution

Upgrade to the latest version of Adobe Reader.

9 Infrastructure

This chapter contains information about known security issues and advises in regards to the environment uniFLOW is running in.

9.1 Operating System

Issue

Missing operating system security patches.

Windows servers are often found to be missing a number of Windows operating system security updates, leaving them at risk from publicly disclosed vulnerabilities.

The majority of the vulnerabilities that affect the servers can only be triggered if a user on the system were to visit a malicious web site or access a malicious file. Remote code execution is not possible without some level of user interaction on the server. As it is unlikely the servers would be used in this way the probability of exploitation is much lower.

Resolution

We strongly recommend that you ensure that a Windows patch management policy is robustly enforced on their production office environment. All missing patches and service packs (for both the Windows operating system and other Microsoft software, e.g. IIS and Office) should be applied as soon as possible.

In addition, we strongly recommend that you complement the patch management process with a tool like the Microsoft Baseline Security Analyzer to check patch levels regularly and ensure that patches are not accidentally missed.

http://www.microsoft.com/technet/security/tools/mbsahome.mspx

9.2 Server Message Block (SMB) Signing

The Server Message Block (SMB) protocol is used for providing and obtaining network file services. It makes it possible to copy files between network computers. In case the server is in a network with untrusted clients, security issues can arise. These can be for example man-in-the-middle attacks or active message attacks. However, enabled SMB signing will add security to the SMB protocol and prevents for man-in-the-middle attacks. With SMB signing, a signature will be added to each network package. This

way, the client 'knows' if the package comes from the right server and vice versa and thus this prevents for vulnerabilities.

Issue

If Server Message Block (SMB) signing on the host computer is disabled, the SMB server is vulnerable to man-in-the-middle attacks.

Resolution

Enforce SMB signing on your host's configuration.

- For SMB signing at least the following operating systems / platforms are required:
  - Samba >= V3.0
  - Windows XP or newer
- We highly recommend that you check beforehand that your file server in use supports SMB signing.

Learn more about Server Message Block signing here:

Overview of Server Message Block signing

http://support.microsoft.com/kb/887429/EN-US

How to set up the SMB policy settings on a Windows Server

Step 4 of the following Microsoft Knowledgebase article explains how to enable the SMB signing.

http://support.microsoft.com/kb/839499/en-us

Possible Server Message Block communication problems

http://support.microsoft.com/kb/916846/en-us

9.3 Microsoft Windows RDP Server

Microsoft Windows RDP Server Man-in-the-Middle Weakness

Issue

It may be possible to access remote hosts because the version of Remote Desktop Protocol Server (Terminal Service) running is vulnerable to Man-in-the-Middle (MitM) attacks. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key.

The RDP client makes no effort to validate the identity of the server when setting up encryption; therefore, an attacker who can intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MitM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

Resolution

Force the use of SSL as a transport layer for this service if supported.

Select the ***Allow connections only*** from computers running ***Remote Desktop with Network Level Authentication*** (NLA).

Configuring authentication and encryption:

http://technet.microsoft.com/en-us/library/cc782610.aspx

To configure authentication and encryption follow the instructions in the linked Microsoft Technet article. Change the RDP encryption level in the ***Terminal Services Configuration*** to one of the following so that it uses strong cryptography:

- ***High***
- ***FIPS Compliant***

Note that with an activated NLA (Network Level Authentication), RDP sessions are only possible from Windows Vista (or higher). Windows XP can handle NLA after an update of the RDP client to version 6.5 or higher (version 7 recommended). The full feature set of the new RDP client are available with Windows 7 and Windows Server 2008 R2.

http://support.microsoft.com/kb/969084

9.4 Anti-Virus

As every Virus Scanner works differently, NT-ware cannot give any detailed information about certain Virus Scanner settings or behaviors. However, NT-ware encountered some minor issues with certain Virus Scanners which could all be resolved so far.

One of the problems with Anti Virus software is that it 'locks' files while scanning. So if a new spool file is created by the spooler, it will be scanned. uniFLOW will try to access the spool file just after it has been created (through the spooler / APJ print processor). If the file is locked, this will fail. Note that this is only one of the possible problems.

For that reason and from these experiences, we recommend that you do the following:

- Install and configure your Virus Scanner as usual. Test your system and print environment with uniFLOW and see if you encounter problems and check if everything runs normally.
- If you encounter problems, do the following:
  - Check if the Anti Virus Software is causing the problem. This can be done, for example, by simply disabling the Virus Scanner for this test.
  - If the Anti Virus software has been identified as a source of the problem, enable the Virus Scanner and exclude the uniFLOW folders and spool folders from the Anti Virus to see if this causes the problem. The uniFLOW folders are in general:
    - *C:\Program Files\uniFLOW*

- *C:\Program Files\Common Files\NT-ware Shared*
  - If this is the case, one can go ahead and exclude the file types *.dat, *.tmp, *.shd and *.spl within this folder (whether this is possible depends on the Anti Virus software). In this case the folder will still be scanned (i.e. to check if there is a virus or malware) but it will exclude *.dat, *.tmp, *.shd and *.spl files.

9.5 Network Security

uniFLOW requires several different ports and protocols to communicate with clients, printers, the database and other network devices. The ***White Paper - TCP Ports of uniFLOW*** lists all these different communication protocols and ports.

Use this document, in order to configure your firewall(s).

Download the *White Paper - TCP Ports of uniFLOW* here:

MOMKB-99 (http://its.nt-ware.net/browse/MOMKB-99)

9.6 Canon Device Security

Canon has placed an increased focus on the topic of security. For this reason, Canon offers several application software for their printing devices, such as for example:

- Canon Encrypted Secure Print Software (on page 59)
- Canon Secure Watermark (on page 60)
- Canon Data Erase Kit (on page 60)
- Canon Security Kit (see "Canon Security Kit (B2/A2)" on page 61)
- Canon HDD Data Encryption Kit (on page 62)

Please refer to the Canon website for more information about the specific applications or other security related documents or applications for Canon devices.

In the following we list known issues and resolutions with the application software listed above in conjunction with uniFLOW.

9.6.1 Canon Encrypted Secure Print Software

The Canon Encrypted Secure Print Software enables you to encrypt print data sent from a computer using the Secured Print function, and decrypt it at the device. This can strengthen the security of print data by helping to prevent the contents of your

printed documents from being seen by other users, and helping to prevent the unauthorized use of confidential information.

Issues

The Encrypted Secure Print Software encrypts the print job on the client before it is sent to the printer. The printer then decrypts the print data stream.

The printer driver will use the username and password that the user enters to encrypt the spoolfile. The printer will then decrypt the data after the user has entered his username and password again on the device. For this reason, the encrypted spoolfile cannot be de decrypted by uniFLOW. Hence it is not possible for uniFLOW to analyze and account the spoolfiles for such print jobs. Furthermore it is also not possible to use Rule Based Routing workflows or any other workflow which requires a spoolfile analysis.

Resolution

The only possible method to account such print jobs with uniFLOW is CPCA accounting instead of spoolfile accounting.

9.6.2 Canon Secure Watermark

Enables users to embed hidden text in the background of copies. Examples include: "CONFIDENTIAL," the date and time, or a department name. The embedded text becomes visible when copies of the document are made on a copier.

Issues

No known issues.

9.6.3 Canon Data Erase Kit

Data is automatically and completely erased following each print, copy, and scan job. Document data is also overwritten when an item is manually deleted. Three automatic methods can be selected: Overwrite null data one time, Overwrite random data one time or Overwrite random data three times.

Issues

No known issues.

HDD Erase function does not delete job log information from the device so has no impact on uniFLOW.

For detailed information about the Canon Data Erase Kit, please refer to the respective Canon manuals.

9.6.4 Canon Security Kit (B2/A2)

The Canon Security Kit is optional software for the Canon imageRUNNER series which adds security enhancements to the multifunction device (MFD).

The Security Kit is a device control software, providing users with hard disk drive encryption and hard disk drive erasure functions. The security of the existing identification and authentication functions is also enhanced by this installation.

Issues

With the Canon Security Kit you can enable or disable the job history. When this setting is enabled, '0' will always be returned in response to a request for a job history from a remote application. In other words, a type of software that manages the machine with reference to the machine's job history (as for example uniFLOW) cannot be used.

Resolution

Enable the job history log on the machine to enable uniFLOW to read out meaningful entries from the job log.

uniFLOW offers a solution that user names and print job names can be decrypted so that it is no longer possible for users to gather from the print job logs who has printed what and when. To do so, the Workflow Element ***Encrypt Job Name in CPCA*** is required.

Please refer to the uniFLOW User Manual for more information about this Workflow Element.

Enabling/Disabling display of Job Log

You can disable the display of logs (Job Log) stored by the machine. This affects not only the local UI but also the remote UI. It is important to keep in mind that log collection (job account log/fax communication log) otherwise possible with a specific application (for example uniFLOW) will no longer be available, as there will be no response to a command for data collection. Data in the form of a jam log, error log, and alarm log, however, will be available for collection.

If the setting of the additional functions item explained below is disabled, the display of the copy, send, fax, print and receive logs are disabled.

Whether or not the Job Log will be displayed depends on whether the function is enabled or disabled in Additional Functions.

Service Mode Item (level 2)

COPIER → Option → USER → LGSW-DSP

- 0: disable display in Additional Functions (default)
- 1: enable display in Additional Functions

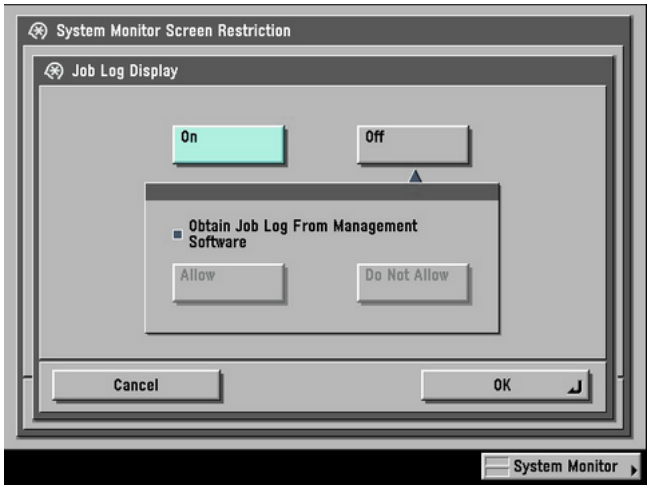
Changing the setting from 0 to 1 enables the display in Additional Functions. Change the setting value according to the user's request.

Additional Functions → System Settings → System Monitor Screen Restrictions → Job display

Additional Functions Items

Additional Functions → System Settings → Job Log Display=on/off

- on: enable display of Job Log (default)
- off: disable display of Job Log



Comments

The HDD Erase function does not delete job log information from the device, meaning it has no impact on uniFLOW. This kit has been superseded by the HDD Data Encryption Kit and HDD Data Erase Kit which conform to common criteria requirements.

9.6.5 Canon HDD Data Encryption Kit

Also known as:

- *Canon HDD Data Encryption & Mirroring Kit*
- *Canon imageRUNNER Hard Disk Drive Data Security and Encryption*

The encryption board identifies and authenticates the machine, and it is enabled only with the iR machine at the installation.

A device's HDD temporally records image data like scanned images and PDL data etc. at any time. After the printing operation is completed, the normal operation is that only management information is deleted, so the image data information remains on the HDD.

Therefore, there is some concern that the HDD could be taken by a third party, the data analyzed by accessing it directly using Disk Editor, and the original data recovered. As countermeasure, information is always encrypted in areas where the data such as

images and PDL data are saved temporarily. By doing so, recovering the original image data on the HDD is made too difficult.

With the existing iR Security Kit, the function is enabled with the registration of the license key, and only the area user data is encrypted. With the HDD Encryption Kit, instead of the license option form, the encryption board encrypts all data recorded on the HDD.

Mechanism of data encryption

The encryption board encrypts the received signal sent from the controller board, and then records it on the HDD. The encryption board receives and recovers the encrypted data stored on the HDD, and then sends it to the controller. By pairing up an encryption board and an HDD, the encryption board becomes workable. Therefore, if there are a number of HDDs, the same number of encryption boards is needed.

Issues

This kit should not cause problems with uniFLOW when reading out CPCA logs. When this is enabled on the device and you encounter any problems, then please check that that the Job Log Conceal function is not enabled.

Successful tests with the following devices have taken place by NT-ware: iRC2380i/iRC3080/iR3225n/iR5075.

10 Definitions and Acronyms

Acronym	Description
DES	The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption.
DRQM	The "Distributed Release Queue Management" (DRQM) functionality takes the My Print Anywhere functionality of uniFLOW one step further. It allows print jobs to follow users worldwide. Jobs are released "anywhere" where the users identify themselves.
HTTPS SSL/TLS	HTTPS is a secure communication channel that is used to exchange encrypted information between a client computer and a server. It uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS). With HTTPS (Hypertext Transfer Protocol Secure) the connection between web browser and web server is encrypted. Mostly 40, 128 or 256 bit, depending on the encryption key strength. Using an https: URL indicates that HTTP is to be used, but with a different default TCP port (443) and an additional encryption/authentication layer (Secure Sockets Layer (SSL)) connection between the HTTP and TCP. It is not a separate protocol, but refers to the combination of a normal HTTP interaction over a secure layer.
IG	The Internet Gateway module is used to submit jobs from the internet via a web browser to the uniFLOW system. Generally, this is implemented in a print room job submission environment.

LDAP	LDAP (Lightweight Directory Access Protocol) is a protocol for accessing on-line directory services. A directory service organizes computerized content and runs on a directory server computer. Via LDAP it is possible to read out all information about, for example, users and computers of a directory server computer, such as the users of a Windows Server 2003 Active Directory or Mac OS X Server Open Directory or Novell eDirectory. LDAP defines a relatively simple protocol for updating and searching directories running over TCP/IP.
LDAPS	Also called Secure LDAP or LDAP over TLS. Allows a secure connection to an LDAP-Server over TLS (Transport Layer Security).
RPS	uniFLOW Remote Print Server module: this component can be installed on additional print servers and communicate back to a central uniFLOW server. The RPS does not have a user interface and is administered through the primary uniFLOW system.
RSA	RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography.
SMTP	Simple Mail Transfer Protocol is an Internet standard for email transmission across Internet Protocol (IP) networks.
WAMP	WAMP or WampServer are packages of independently created programs. It is an acronym formed from the initials of the operating system (Microsoft Windows) and the package components: Apache, MySQL and PHP. It is also available for Linux as LAMP or XAMPP.