White Paper

// Escalation Requirements - uniFLOW

Version 4.3

19-Feb-2016

Versioning

Document Versioning	Version	Date	Author(s)	Reviewer(s)
	2.0 - 2.13	Sep-2009 - 25-Sep-2012	NT-ware	Andre Mess, Vincent Maeder, Thomas Lemmer, Stefanie Küpper, Matthias Frye, Matthias Budke, Marja Pals, Norbert Löwe, Jason Apel, Matt Bradshaw
	2.14	03-Jun-2013	Felix Schlick	Thomas Lemmer
	2.15	21-Aug-2013	Sebastian Husnik	Thomas Lemmer
	2.16	30-Aug-2013	Felix Schlick	Thomas Lemmer, Matthias Budke
	2.17	20-Nov-2013	Felix Schlick	Thomas Lemmer
	2.18	28-Nov-2013	Thomas Lemmer	Thomas Lemmer
	2.19	26-Feb-2014	Sebastian Husnik	Thomas Lemmer
	2.2	22-Apr-2014	Sebastian Husnik	Thomas Lemmer
	2.3	06-May-2014	Sebastian Husnik	Thomas Lemmer
	2.4	05-Jun-2014	Sebastian Husnik	Thomas Lemmer
	2.5	25-Jun-2014	Thomas Lemmer	Thomas Lemmer
	2.6	10-Jul-2014	Felix Schlick	Matt Bradshaw, Thomas Lemmer
	2.7	15-Jul-2014	Thomas Lemmer	Thomas Lemmer
	2.8	21-Jul-2014	Felix Schlick	Thomas Lemmer, Matthias Budke, Matt Bradshaw
	2.9	30-Jul-2014	Sebastian Husnik	Thomas Lemmer

	2.10	28-Oct-2014	Sebastian Husnik	Thomas Lemmer
	3.0	15-Jan-2015	Sebastian Husnik	Thomas Lemmer
	3.1	20-Jan-2015	Sebastian Husnik	Matt Bradshaw, Thomas Lemmer
	3.2	26-Jan-2015	Sebastian Husnik	Thomas Lemmer
	3.21	16-Feb-2015	Sebastian Husnik	Thomas Lemmer
	3.3	09-Apr-2015	Felix Schlick	Jan Droste, Thomas Lemmer
	3.4	21-Apr-2015	Felix Schlick	Norbert Löwe, Thomas Lemmer
	3.5	04-May-2015	Sebastian Husnik	Thomas Lemmer
	3.6	10-Jun-2015	Claudia Kleinekemper	Thomas Lemmer, Matt Bradshaw
	3.7	16-Jun-2015	Sebastian Husnik	Thomas Lemmer
	3.8	01-Jul-2015	Sebastian Husnik	Thomas Lemmer
	3.9	08-Jul-2015	Claudia Kleinekemper	Matthias Budke, Thomas Lemmer
	4.0	23-Sep-2015	Felix Schlick	Thomas Fick, Thomas Lemmer
	4.1	12-Oct-2015	Felix Schlick	Thomas Lemmer
	4.2	09-Dec-2015	Sebastian Husnik	Thomas Lemmer
	4.3	19-Feb-2016	Thomas Lemmer	Thomas Lemmer

Document Name	White Paper - Escalation Requirements - uniFLOW
Knowledgebase	MOMKB-245 (https://web.nt-ware.net/its/browse/MOMKB-245)
File Name	White Paper - Escalation Requirements - uniFLOW - V4.2.pdf
Technologies Concerned	uniFLOW V4.0, V4.1, V5.0, V5.1, V5.2, V5.3, V5.4, MEAP, MIND, miniMIND, Windows Server
Short Summary	This White Paper describes the NT-ware escalation requirements for uniFLOW. Please find an HTML version of this document here (http://www.nt-ware.com/wps/WP_Escalation_Requirements_uniFLOW/index.htm).

Document Changes	**Version**	**Topic(s)**	**Changes**
	2.14	-	Various improvements and new document design.
	2.15	How to enable logging for the MomRptServer.exe (Reports / Statistics)	New chapter added.

		(see "MomRptServer.exe (Reports/Statistics) Log Activation" on page 46)	
	2.16	How to create logs with Process Monitor tool (see "Process Monitor Tool Log Generation" on page 57)	New chapter added.
	2.17	Support URLs (on page 101) How to generate a Scan Processing Server log (see "Scan Processing Server Log Activation" on page 66)	Added new info about the Techdispdb.asp. Added a note about restarting the Scan Processing server.
	2.18	RPS (on page 100)	Corrected RPS Techsupport Page Info.
	2.19	mom Technical Support Interface (see "*uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3)*" on page 80)	Added a note.
	2.19	How to use Netstat to check ports open by the uniFLOW Services (see "Netstat Usage to Check Open Ports by uniFLOW Services" on page 47)	New chapter added.
	2.2	How to enable the HTTP Access log for uniFLOW/RPS (see "HTTP Access Logging" on page 38)	Chapter improved.
	2.3	How to check Browser Error Messages (see "Browser Error Message Check" on page 15), How to capture spool files (see "Spool File Capturing" on page 68)	Chapters improved, added Windows registry keys for 32-bit and 64-bit systems to several chapters.
	2.4	Workflow Diagnostic Interface (on page 89), Workflow Diagnostic Writer (on page 96)	Changed note in chapter, new topic added.
	2.5	How to create a Report with the MPS Reporting Tools	Corrected link and description.
	2.6	How to generate a Wireshark log (see "Wireshark Log Generation" on page 84)	Updated and improved chapter.
	2.7	How to create logs with Process Monitor tool (see "Process Monitor Tool Log Generation" on page 57)	Corrected a link.
	2.8	Escalation Requirements (on page 1) Workflow Diagnostic Writer (on page 96)	Added component matrix, corrected Workflow Diagnostic Writer topic.
	2.9	Escalation Requirements (on page 1)	Added links.
	2.10	ODBC SQL Connection Test (on page 51) Troubleshooting Device Connection Issues with GetIPInfo.js (on page 74)	Added chapters, removed "How to"-style from headings.
	3.0	All topics	Adjusted formatting style, headings, removed document type tables and integrated them with direct links into the categories under chapter Issue Types.

	3.1	Print Job Handling Issues (on page 10), Error Role (on page 37), Workflow Diagnostic Interface (on page 89)	Added new chapter Error Role, Adjusted Print Job Handling table, deleted self-reference and added reference to Error Role to chapter Workflow Diagnostic Interface.
	3.2	All topics	Improved layout and formattings.
	3.21	Mobile Print / iSend / Email (on page 8)	Added Wireshark logs and event log creation to Mobile Print escalation requirements.
	3.3	EAI Logging (on page 35)	Added topic about EAI logging.
	3.4	Windows Event Viewer (Windows Server 2008 R2 or Higher) (see "Windows Event Viewer" on page 83)	Removed MPS Reporting Tool, added chapter about Windows Event Viewer.
	3.5	uniFLOW Technical Support Interface Log Export (see "*uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3)*" on page 80), Database Backup (on page 21), Dump Generation (on page 28)	Updated for uniFLOW V5.4, changed chapter database backup, changed topic Dump Generation.
	3.6	HTTPS Communication (on page 39)	Added information on disabling HTTPS communication.
	3.7	Océ PRISMAdirect logging (on page 50)	Added information on Océ PRISMAdirect logging.
	3.8	IIS Log Analysis (on page 44)	Added information about how to read an IIS log file.
	3.9	uniFLOW SmartClient Issues (on page 14)	Added issue type "uniFLOW SmartClient Issues".
	4.0	ICARUS Server for Web (on page 40) ICARUS Server for Web Ports (on page 99)	Added topics for uniFLOW V5.4.
	4.1	uniFLOW Technical Support Interface Log Export (uniFLOW >= V5.4) (on page 81)	Added topics for uniFLOW V5.4.
	4.2	uniFLOW Service for Google Cloud Print Logging (on page 77)	Added information on how to log the uniFLOW Service for Google Cloud Print.
	4.3	RPS (on page 100)	Corrected.

Disclaimer

NT-WARE Systemprogrammierungs-GmbH, all its affiliates, partners and licensors disclaim all warranties, including, but not limited to, warranties about the accuracy or completeness of statements of this site's/document's content or the content of any site or external sites for a particular purpose. This site/document and the materials, information, services, and products at this site/document, including, without limitation, text, graphics, and links, are provided 'as is' and without warranties of any kind, whether expressed or implied.

Company and product names mentioned herein are registered or unregistered trademarks of their respective companies. Mention of third-party products is for information purposes only and constitutes neither an endorsement nor a recommendation. NT-ware assumes no responsibility with regard to the performance or use of these products. Also, NT-ware makes no claim to these trademarks. Any use of trademarks, logo, service marks, trade names, and product names is prohibited without the written permission of the respective owners.

Adlib, Express and Express Server are either registered trademarks or trademarks of Adlib Publishing Systems Inc.; Adobe®, Adobe® Reader®, Acrobat®, Distiller®, PostScript® and products of the CREATIVE SUITE(S) are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries; Android is a trademark of Google Inc.; Apple®, the Apple® logo, Mac®, Mac OS®, Macintosh®, iPhone®, iPad® and AirPrint® are trademarks of Apple Inc. registered in the U.S. and other countries; Box of Box Inc.; Blackboard Transact™ of Blackboard Inc.; CANON, imageRUNNER, imageRUNNER ADVANCE, MEAP, CPCA, AMS, iW AMS, iW Desktop, iSend, iW SAM are trademarks or registered trademarks of Canon Inc.; CardSmith® is a trademark of CardSmith LLC; CBORD CS Gold® of the CBORD Group Inc.; Crystal Reports and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company; Dropbox of Dropbox Inc.; eCopy™, eCopy ShareScan® and eCopy ScanStation™ are marks or trademarks of Nuance Communications, Inc.; Evernote® of Evernote Corporation; FileNet® of IBM Corporation; Foxit®SDK and Foxit® Reader of Foxit Corporation; Google Docs of Google Inc.; Google Cloud Print™ web printing service is a trademark of Google Inc.; Helix™ Production Workflow is a trademark of NT-WARE Systemprogrammierungs-GmbH; HP, HEWLETT-PACKARD, PCL and LASERJET are registered trademarks that belong to Hewlett-Packard Development Company; KONICA MINOLTA is a registered trademark of KONICA MINOLTA Inc.; iOS® of Cisco Technology Inc.; iDRS™ SDK and IRISConnect™ are unregistered trademarks of I.R.I.S. Group S.A.; JAWS pdf courier™ are trademarks of Global Graphics SA.; Microsoft®, Windows®, Windows Server®, Internet Explorer®, Internet Information Services, Microsoft® Word, Microsoft® Excel, Microsoft SharePoint®, Microsoft SharePoint® Online, OneDrive®, One Drive® for Business, SQL Server®, Active Directory® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries of Microsoft Corporation; Neevia Document Converter Pro™ of Neevia Technology; NetWare®, Novell®, Novell eDirectory™ of Novell Inc. are registered/unregistered trademarks of Novell Inc. in the United States and other countries; MobileIron® of Mobile Iron Inc., Océ, Océ PlotWave®, Océ ColorWave® and PRISMA are trademarks or registered trademarks of Océ Holding B.V., OpenOffice.org™ of Oracle Corporation; PAS™ is a trademark of Equitrac Corp.; PosterJet is copyrighted and an internationally registered trademark of Eisfeld Datentechnik GmbH & Co. KG; RedTitan EscapeE of RedTitan Limited; NETAPHOR®, SiteAudit™ are trademarks of NETAPHOR

SOFTWARE Inc.; SAMSUNG is a trademark of SAMSUNG in the United States or other countries; Therefore™, Therefore™ Online of Therefore; UNIX® is a registered trademark of The Open Group; uniFLOW®, uniFLOW Serverless Secure Printing®, Helix Production Workflow®, MIND®, microMIND®, and MiCard® are registered trademarks of NT-WARE Systemprogrammierungs-GmbH; pcProx®, AIR ID® are registered trademarks of RFIdeas Inc.Readers; CASI-RUSCO® is a registered trademark of ID Card Group; Radio Key® is a registered trademark of Secura Key; GProx™ II is an unregistered trademark of Guardall; HID® ProxHID is a registered trademark of HID Global Corporation; Indala® is a registered trademark of Motorola; ioProx™ is an unregistered trademark of Kantech; Xerox, Xerox and Design, as well as Fuji Xerox and Design are registered trademarks or trademarks of Xerox Corporation in Japan and/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.

Friday, February 19, 2016, 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

Tel: +49 - 54 03 - 7243 - 0
Fax: +49 - 54 03 - 78 01 03

Email: info@nt-ware.com

Register of Companies: Amtsgericht Osnabrück
No. of entry in Register of Companies: HRB 110944
Chief Executive Officer: Karsten Huster
Responsible according to § 6 MDStV: Karsten Huster
VAT registration no. according to §27 a Umsatzsteuergesetz: DE 230932141

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.

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.

Further Information:
Pointer to additional manuals, installation manuals, white papers or the NT-ware Knowledgebase.

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 Data Protection Checklist

Before sending any data to NT-ware, please ensure that you have permission to do so and that you act in accordance with the data protection laws defined by national and/or supranational legislation.

The following checklist is a brief set of rules that helps you to decide whether you are allowed to send data. In case you are not sure about the legal obligations, contact your Data Compliance Manager (DCM)/Legal department.

Allowed to process?	• Contract with NSO/customer in place? • In case of sensitive Personal Data, are (written) consents of the individuals in place?
Processing purpose	• Define the purpose: installation of software, fixing a customer's problem, setting-up of a database, etc.
Data relevant for the purpose?	• If not, ask your DCM for further advice, delete/do not use non-relevant data, give feedback to the customer or NSO.
Data processing for a specific purpose.	• Adequate, relevant and not excessive. • Conducted only by relevant persons. • Transfer to other countries only after consultation with the DCM/Legal department. • Data shall only be kept as long as necessary.

What does NT-ware do in terms of Data Protection?

NT-ware ensures processing of personal data according to the relevant data protection regulations.

If customer data are personal data, NT-ware will handle these data in a secure way and will only process relevant customer data for clearly defined purposes, for example, to solve an issue with an NT-ware product. Only designated employees of NT-ware are allowed to process and to access customer data. When the purpose of the processing of customer data is accomplished, the customer data used will be deleted from the NT-ware system, except when the customer has explicitly agreed that the customer data should be not deleted from the NT-ware system because of additional reasons.

2 Escalation Requirements

Please provide certain standard information when escalating an issue to a higher support level. This will guarantee effective and efficient processing of the issue.

The following basic information is always required, independent of the error type:

uniFLOW OM Version:			Serial Number:	
Activated Modules:				
Operation System:			Patch Level:	
SQL Server / MSDE:			Version:	
Hardware - if involved:	MIND		Serial Number:	Firmware Version:
	miniMIND			
	MiCard			
Login Manager, Version:				
Device(s) - if involved:	Type:	Controller:	Firmware Version:	Driver:
Are RPSes involved?				
Cluster installation?				

Apart from the above, please also include:

- An exact description of the error.
- An exact description of the steps that already have been taken in trying to resolve the problem.
- A description of the results of the above taken steps.
- Log files and other data that are needed depending on your issue (see chapter Issue Types (on page 2)).

3 Issue Types

Depending on the type and content of your issues certain document or log types are recommended.

The following tables give you an overview of those document types.

Priorities of Information

Depending on the error type, certain **filtered** information – focusing on the error in question – is needed that will enable localizing, analyzing, reproducing it and finally, fixing the problem.

In this chapter you'll find a brief outline of the information that might be needed to analyze certain error types. The information needed will always be dependent on the error type. You'll get detailed instructions from the next higher support level, as to what information is needed.

Certain points are of a higher priority than others. Please see the priority reference below.

***	-	This information has to be provided and will definitely be requested by NT-ware.

**	-	This information will be very helpful in order to solve the reported issue.
*	-	This information can be very helpful in order to solve the reported issue.

The upload size of attachments is limited to 10MB on the ITS. Therefore NT-ware has introduced a secure File Exchange Interface which provides enough storage for all required data. In order to get a project folder created please create an ITS issue. Our Support Team will take care of this immediately. You will receive a HTTP/FTP link to the project folder and a password to this folder in two separate emails.

3.1 Accounting Issues

For accounting errors the following information can be useful:

Recommended Logs and Data for Analyzing Purposes	Priority
• Spool files Also provide a description of the accounting data you would have expected, the accounting data you receive and the original file in use (Word.doc, Excel, PDF etc.) See: Spool File Capturing (on page 68)	xxx
• CPCA log A description of how to enable CPCA logging is given in the related paragraph. See: CPCA Logging (on page 18)	xxx
• Database backup See: MSDE / SQL 2005 Express / SQL 2008 Express (see "Microsoft SQL Server 2008 R2 Express" on page 21)	xx
• Counter from devices (start/end of a defined time frame) To capture the device counters you can easily configure a "total counter" task in HelixPW. Note that the Total 101 meter is not configured by default anymore. It has been decided that all logical meters should be removed from devices. The reason behind this is to ensure that there is visibility within Oracle and e-maintenance for true A3 and A4 clicks and therefore allow a premium click charge for A3 copies. The 101 meter cannot distinguish between A4+A3.	xx
• Settings in uniFLOW Snapshot of the uniFLOW configuration. See: uniFLOW Snapshot Creation (on page 80)	xx
• MPS-report There are 8 different versions of the MPS report tool, each gathering different types of information. In this case especially, the event logs are of importance. See: MPS Reporting Tool Report Creation	xx

Recommended Logs and Data for Analyzing Purposes	Priority
• Troubleshoot device connection issues: See: Troubleshooting Device Connection Issues with GetIPInfo.js (on page 74)	x
• SQL Profiler Database Monitoring (on page 69)	x
• Event Logs	x
• XML Export (uniFLOW Configuration / IIS Backup Creation (on page 43) / Statistics Problem Check (on page 70))	x
• Printer Export (on page 54)	x
• Reporting export If errors occur during the executing of statistic tasks it is possible to generate a copy of the xml configuration file for further analysis. See: Statistics Problem Check (on page 70)	x

3.2 Additional Error Logging

Recommended Logs and Data for Analyzing Purposes	Priority
• SMTP Logging on uniFLOW See: SMTP Log (on page 67)	xx
• MEAP Logging To enable additional MEAP logging please get in contact with the NT-ware Support Team via ITS to get further instructions and the necessary files.	x
• uniFLOW Client for Windows Logging (on page 76)	x
• Scan Processing Server Log Activation (on page 66)	x
• Browser Error Message Check (on page 15)	x

3.3 CRQM Issues

Recommended Logs and Data for Analyzing Purposes	Priority
• Screenshots	x
• uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3) (on page 80) • uniFLOW Technical Support Interface Log Export (uniFLOW >= V5.4) (on page 81)	x
• Workflow Diagnostic Interface (on page 89)	x
• Process Monitor Tool Log Generation (on page 57)	x
• CRQM Logging (on page 20)	x
• Event Logs	x
• XML Export (uniFLOW Configuration / IIS Backup Creation (on page 43) / Statistics Problem Check (on page 70))	x
• Netstat Usage to Check Open Ports by uniFLOW Service (see "Netstat Usage to Check Open Ports by uniFLOW Services" on page 47)	x

3.4 Database Issues

For the analysis of database errors, the following information can be useful:

Recommended Logs and Data for Analyzing Purposes	Priority
• Database backup See: DsPcDb Database Backup (see "Database Backup" on page 21)	xxx
• MPS-report from the database server With the MPS-report tool it is possible to gather critical system and logging information. There are 8 different versions of the tool. Each version gathers some of the same basic information but there are specific reports unique to different support scenario categories. See: MPS Reporting Tool Report Creation	xx
• Extract of NT-ware Windows registry hive See: Windows Registry Hive (Registry Keys) Extraction (on page 61)	xx
• Snapshot of the uniFLOW configuration See: uniFLOW Snapshot Creation (on page 80)	x
• In case you had to restore the Database, read the following chapter See: PBAIP-User Repair after Database Restoration (on page 52)	x
• In case you cannot access the database via network See: SQL Express 2005 Network Access Activation (on page 68)	x

Recommended Logs and Data for Analyzing Purposes	Priority
• SQL Server Profiler shows how SQL Server resolves queries internally. This allows administrators to see exactly what Transact-SQL statements or Multi-Dimensional Expressions are submitted to the server and how the server accesses the database or cube to return result sets. See: SQL Profiler Database Monitoring (on page 69)	x
• Test connection to SQL server. See: ODBC SQL Connection Test (on page 51)	x
• Event Logs	x
• Netstat Usage to Check Open Ports by uniFLOW Service (see "Netstat Usage to Check Open Ports by uniFLOW Services" on page 47)	x

3.5 Installation Issues

To analyze errors during installation, the following information can be useful:

Recommended Logs and Data for Analyzing Purposes	Priority
• An extract of the NT-ware Windows registry hive See: Windows Registry Hive (Registry Keys) Extraction (on page 61)	xxx
• Database backup as bak-file Depending on the database in use, there are different backup modes. See: DsPcDb Database Backup (see "Database Backup" on page 21)	xx
• Process Monitor Tool Log Generation (on page 57)	xx
• MPS Reporting Tool Report Creation	xx
• Event logs	xx
• Screenshots Only send a screenshot if the information in the screenshot is really useful, mostly only when visible bugs in the user interface need to be reported. Do not copy screenshots into a WORD or RTF document as this leads to huge file sizes!	xx
• uniFLOW snapshot The uniFLOW snapshot tool makes a backup of the database (only if a local MSDE or SQL 2005 Express database is in use!), a snapshot of the registry keys and runs the Print Migrator Tool to create a backup of all system printers.	xx
• A system image It is possible to create a system image of the full system by using the VM-ware Converter. See: System Image Creation (on page 72)	x

3.6 Internet Gateway Issues

If errors occur that are related to the Internet gateway, the following information might be useful:

Recommended Logs and Data for Analyzing Purposes	Priority
• Log files of the Internet Gateway Activate logging on the administrator site of the IG under Internet Gateway Settings. The path to the error log files is *[mainIG folder]/logfiles*.	xxx
• Apache logs The Apache Logs contain information about the communication between the Apache web server and connected clients. The Apache logs can be found in your Apache folder, for instance /apache/logs/.	xx
• Information on the web server Information on the web server and the php version in use.	xx
• Screenshots of the Internet Gateway configuration.	x
• Customization When customization of the Internet Gateway has taken place, this information can be found in the original project checklist.	x

3.7 Kernel Issues (uniFLOW/RPS)

Recommended Logs and Data for Analyzing Purposes	Priority
• uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3) (on page 80) • uniFLOW Technical Support Interface Log Export (uniFLOW >= V5.4) (on page 81)	x
• Process Monitor Tool Log Generation (on page 57)	x
• Windows Registry Hive (Registry Keys) Extraction (on page 61)	x
• Dump Creation with DebugDiag (Manual Dump) (on page 29)	x
• MPS Reporting Tool Report Creation	x
• uniFLOW Snapshot Creation (on page 80) or System Image Creation (on page 72)	x

3.8 MEAP/MIND/CMFP Issues

For errors that are related to MIND, miniMIND/MEAP applets or installed identification devices the following information might be of use:

Recommended Logs and Data for Analyzing Purposes	Priority
• Telnet log Via Putty it is possible to generate a log of the MIND communication as a text file. See: Telnet Log Generation for MIND / LM / SSP / microMIND V2 (on page 73)	xxx
• Type of reader and firmware version of the reader	xx
• Device type and firmware Including the relevant settings on the device.	xx
• Configuration uniFLOW Snapshot of the uniFLOW configuration or a database backup if this is on a separate server. See: uniFLOW Snapshot Creation (on page 80) and: MSDE / SQL 2005 Express / SQL 2008 Express (see "Microsoft SQL Server 2008 R2 Express" on page 21)	x
• Troubleshoot device connection issues: See: Troubleshooting Device Connection Issues with GetIPInfo.js (on page 74)	x
• uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3) (on page 80) • uniFLOW Technical Support Interface Log Export (uniFLOW >= V5.4) (on page 81)	x
• Wireshark Log Generation (on page 84)	x
• Process Monitor Tool Log Generation (on page 57)	x
• HTTP Access Logging (on page 38)	x
• Netstat Usage to Check Open Ports by uniFLOW Service (see "Netstat Usage to Check Open Ports by uniFLOW Services" on page 47)	x

3.9 Mobile Print / iSend / Email

Recommended Logs and Data for Analyzing Purposes	Priority
• SMTP Log (on page 67)	xxx
• Workflow Diagnostic Interface (on page 89)	xx

Recommended Logs and Data for Analyzing Purposes	Priority
• uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3) (on page 80) • uniFLOW Technical Support Interface Log Export (uniFLOW >= V5.4) (on page 81)	x
• Screenshots	x
• Wireshark Log Generation (on page 84)	xx
• XML Export (uniFLOW Configuration / IIS Backup Creation (on page 43) / Statistics Problem Check (on page 70))	x
• File Copy	x
• Netstat Usage to Check Open Ports by uniFLOW Service (see "Netstat Usage to Check Open Ports by uniFLOW Services" on page 47)	xx
• MPS-report There are 8 different versions of the MPS report tool, each gathering different types of information. In this case especially, the event logs are of importance. See: MPS Reporting Tool Report Creation	xx

3.10 Network Issues

Recommended Logs and Data for Analyzing Purposes	Priority
• Communication trace With the Netmon tool or the Wireshark tool, it is possible to capture all network communication. Obviously, this can lead to huge amounts of data, so this information should be filtered, for instance, by narrowing down the time frame in which the error occurs. See: NetMon Network Trace Generation (on page 47) See: Wireshark Log Generation (on page 84)	xxx
• Network structure description Normally this is already documented as part of the Project Checklist.	xx
• Telnet Logging (on page 73)	x
• Event Logs	x

Recommended Logs and Data for Analyzing Purposes	Priority
• XML Export (uniFLOW Configuration / IIS Backup Creation (on page 43) / Statistics Problem Check (on page 70))	x
• Netstat Usage to Check Open Ports by uniFLOW Service (see "Netstat Usage to Check Open Ports by uniFLOW Services" on page 47)	x
• MPS Reporting Tool Report Creation	x
• Route Print	x
• ipconfig /all	x
• Visible error as screenshot	x

3.11 Print Job Handling Issues

There is a huge variety of errors that have to do with print job handling. They can be Windows, driver, device, firmware or uniFLOW related. For this reason, the kind of information that might be relevant can vary a lot.

Recommended Logs and Data for Analyzing Purposes	Priority
• Spool files There are different methods for capturing spool files. They are described in the related paragraph. See: Spool File Capturing (on page 68)	xxx

Recommended Logs and Data for Analyzing Purposes	Priority
• Techsupport.log One of the "hidden websites" of uniFLOW is the Tech Support Interface. You can use this web site to create different kinds of logs, for instance on general errors, print job handling or on every activity ("flow"). As the techsupport.log entries are stored into the database and the intensive logging might slow down the system, it is highly recommended to change the error level back to "Error" after providing the log files to NT-ware. See: uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3) (on page 80) uniFLOW Technical Support Interface Log Export (uniFLOW >= V5.4) (on page 81)	xxx
• Printer Workflows The printer workflow can be exported to XML from within the Advanced Configuration of the printer under the workflow tab. The Advanced Workflow Editor may need to be enabled: http://www.nt-ware.com/mom/5.3/HTML/EN/index.htm#15060.htm (http://www.nt-ware.com/mom/5.3/HTML/EN/index.htm#15060.htm) If it is not possible to access the advanced configuration due to licensing restrictions, a database backup will suffice. See: DsPcDB Database Backup (see "Database Backup" on page 21)	xxx
• Printer driver (type and version) It is always best to provide the original driver in use.	xx
• Settings in the operating system Check Group policy, file, folder and printer permission; also check whether the printer is installed locally or mapped.	x
• Workflow Diagnostic Interface (on page 89)	x
• Process Monitor Tool Log Generation (on page 57)	x
• Device type and settings Provide an exact description of the device type, including Firmware version and relevant user and service mode settings	x
• Event Logs	x
• Printer Export (on page 54)	x
• XML Export (uniFLOW Configuration / IIS Backup Creation (on page 43) / Statistics Problem Check (on page 70))	x

3.12 RPS Issues

Recommended Logs and Data for Analyzing Purposes	Priority
• Techsupport log Techsupport log of the uF server set to flow. See:	xxx

Recommended Logs and Data for Analyzing Purposes	Priority
uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3) (on page 80) uniFLOW Technical Support Interface Log Export (uniFLOW >= V5.4) (on page 81)	
• Extract of NT-ware Windows registry hive on RPS See: How to make an extract of the Windows registry hive	xxx
• Dump.htm of RPS You can create a dump.htm of your RPS installation to check if the configuration on the RPS is correct. See: RPS dump.htm Activation (on page 64)	xxx
• Momaps log (set to flow) How to enable logging on the RPS is described in the related paragraph. See: RPS Logging (on page 64)	xxx
• HTTP Access Log on the uniFLOW RPS for Windows See: HTTP Access Logging (on page 38)	xx
• MPS-report Use the "alliance" version of the MPS-report tool on the RPS. See: MPS Reporting Tool Report Creation	xx
• Configuration uniFLOW Use the Snapshot tool or make a database backup. See: MSDE / SQL 2005 Express / SQL 2008 Express (see "Microsoft SQL Server 2008 R2 Express" on page 21) and: uniFLOW Snapshot Creation (on page 80)	x
• In case you have to query the SQL Lite DB on the RPS refer to the following chapter: See: RPS SQL Query Website Activation (on page 65)	x
• Netstat Usage to Check Open Ports by uniFLOW Service (see "Netstat Usage to Check Open Ports by uniFLOW Services" on page 47)	x

3.13 Scanning Issues

Recommended Logs and Data for Analyzing Purposes	Priority
• Scan Processing Server Log Activation (on page 66)	xxx
• Screenshots	x
• Workflow Diagnostic Interface (on page 89)	x
• Telnet Logging (on page 73)	x
• Wireshark Log Generation (on page 84)	x
• Process Monitor Tool Log Generation (on page 57)	x

Recommended Logs and Data for Analyzing Purposes	Priority
• XML Export (uniFLOW Configuration / IIS Backup Creation (on page 43) / Statistics Problem Check (on page 70))	x
• File Copy	x

3.14 Services (General) / Configuration Issues

Errors that include the services can be analyzed with the following tools:

Recommended Logs and Data for Analyzing Purposes	Priority
• MPS-report There are eight different versions of the MPS report tool, each one gathering different types of information. In this cases like this, the event logs are of special importance. See: MPS Reporting Tool Report Creation	xx
• Configuration of uniFLOW Snapshot of the uniFLOW configuration. See: uniFLOW Snapshot Creation (on page 80)	xx
• Extract of the NT-ware Windows registry hive See: Windows Registry Hive (Registry Keys) Extraction (on page 61)	xx
• Poolmon Poolmon creates a snapshot of the system memory every 60 minutes and stores the log files. See: Poolmon Log Generation (on page 53)	x
• Print Migrator The Print Migrator Tool reproduces all system printers, drivers and ports. See: Printer Export (on page 54)	x
• System image It is possible to create a system image of the full system by using the VM-ware Converter. See: System Image Creation (on page 72)	x
• Crash dump It is possible to create a crash dump in case the kernel or service of uniFLOW terminates or crashed unexpectedly. See: Internal Exception Handling and Dump Creation (on page 28) See: Dump Creation with DebugDiag (Manual Dump) (on page 29) See: Dump Creation with DebugDiag (Automatic Dump) (on page 31)	x

3.15 uniFLOW Client Issues

Recommended Logs and Data for Analyzing Purposes	Priority
• uniFLOW Client for Windows Logging (on page 76)	xxx
• Screenshots	x
• Telnet Logging (on page 73)	x
• Wireshark Log Generation (on page 84)	x
• IIS Log	x

3.16 uniFLOW SmartClient Issues

In uniFLOW SmartClient environments the print infrastructure can be configured much more flexible than in a normal server print environment because services/components that are usually located on a server can be distributed to uniFLOW SmartClient PCs and MEAP devices.

Therefore, in case of print issues in uniFLOW SmartClient environments, it is essential to check the communication between the server(s) and all endpoints i.e. all peers concerned in order to see what component causes the problem.

For checking the communication paths of all components involved, you can make use of the logging features described below.

If you send the logging data to our support team, you should also attach screenshots of all tabs of the uniFLOW SmartClient Configuration, a description of the configured uniFLOW SmartClient use case and of the scenario the customer originally wanted to achieve.

Recommended Logs and Data for Analyzing Purposes	Priority
• uniFLOW SmartClient Logging The logging of the uniFLOW SmartClient can be enabled on the Management Server (uniFLOW server or RPS). If it is enabled on the Management Server, it will track all uniFLOW SmartClient logs from **all** computers. On the uniFLOW server the uniFLOW SmartClient log can be activated in ***Server Config > General Settings > uniFLOW***, on the RPS it can be activated via registry key. For a detailed information see uniFLOW SmartClient Logging (on page 78).	xxx
• *Techdisppeers* website Via https://localhost:8443/techdisppeers.asp on the uniFLOW server and on the RPS all endpoints that are connected to the server can be seen.	xxx

Recommended Logs and Data for Analyzing Purposes	Priority
• Wireshark Log Generation (on page 84) Note that this communication takes place via HTTPS. Therefore, uniFLOW and Wireshark require some special preparations in order to be able to view the underlying communication in plain text.	xxx
• Telnet Logs of all MFPs Perform a telnet log on port 53213 of the MFP. This telnet log provides similar information as the uniFLOW SmartClient log, but from the perspective of the printer. For more information see Telnet Logging (on page 73).	xxx
• Screenshots of all tabs of the uniFLOW SmartClient Configuration under ***Connections > Client > SmartClient Configuration***.	xxx
• Description of the configured use case.	xx
• Description of the customer requirements.	x

3.17 Data Collection Methods for Error Analysis

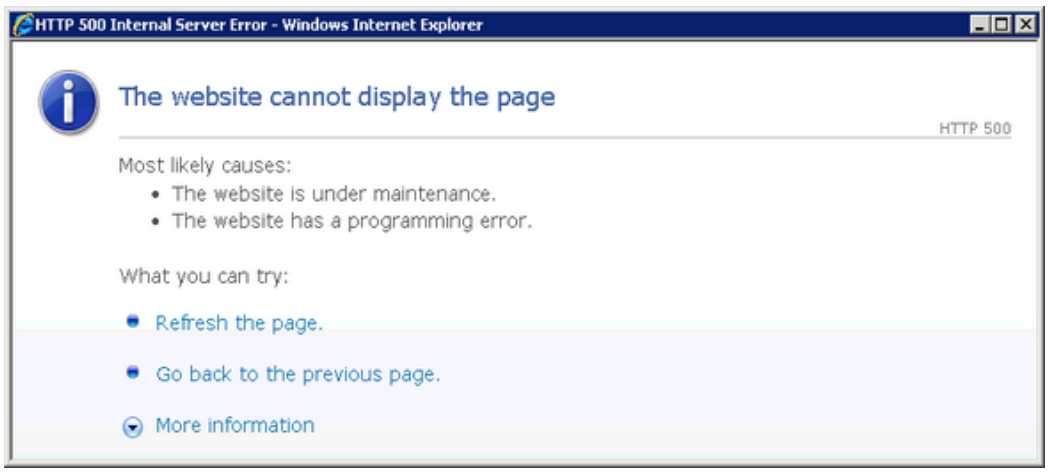
There are a variety of uniFLOW specific and third party tools that can be used for collecting data for analyzing purposes. In this chapter you'll find an overview of the most important tools, how and where they can be obtained and a description of how to use them.

3.17.1 Browser Error Message Check

Issue

If you receive HTTP error messages in your browser, these are generally displayed in a "friendly HTTP error message" format.

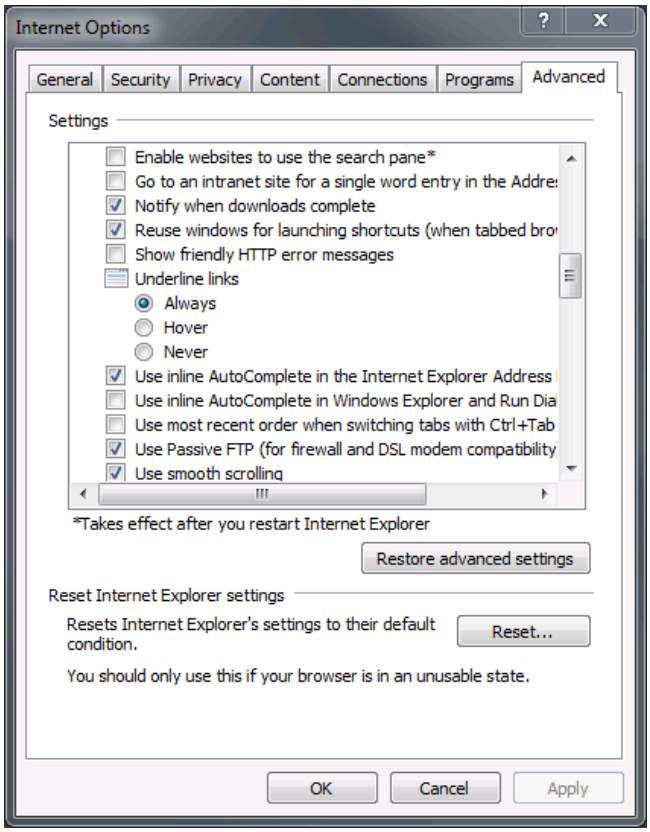
This message does not give you much detail on where exactly the error happened.



Resolution

To get more information, you can turn off the ***Show friendly HTTP error messages*** feature of the Internet Explorer browser.

To do so, open the ***Internet Options > Advanced*** menu of the Internet Explorer and disable ***Show friendly HTTP error messages***.

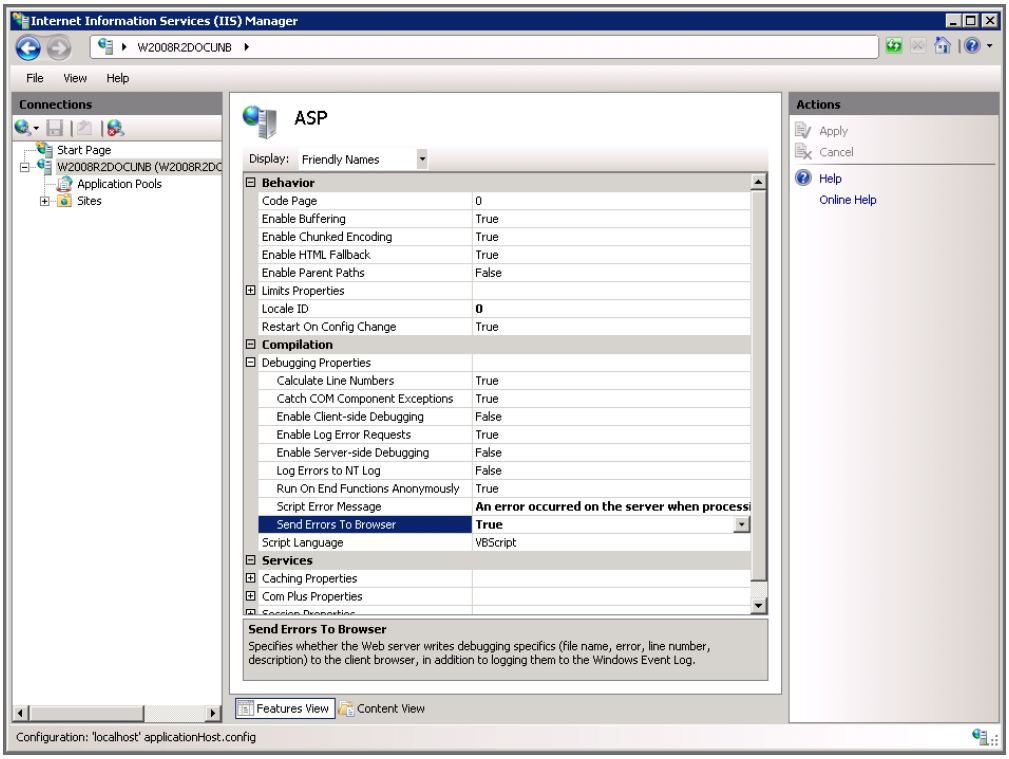


Different Internet Information Services

With IIS6, further information about the errors are available by default. For IIS7 this must be activated first.

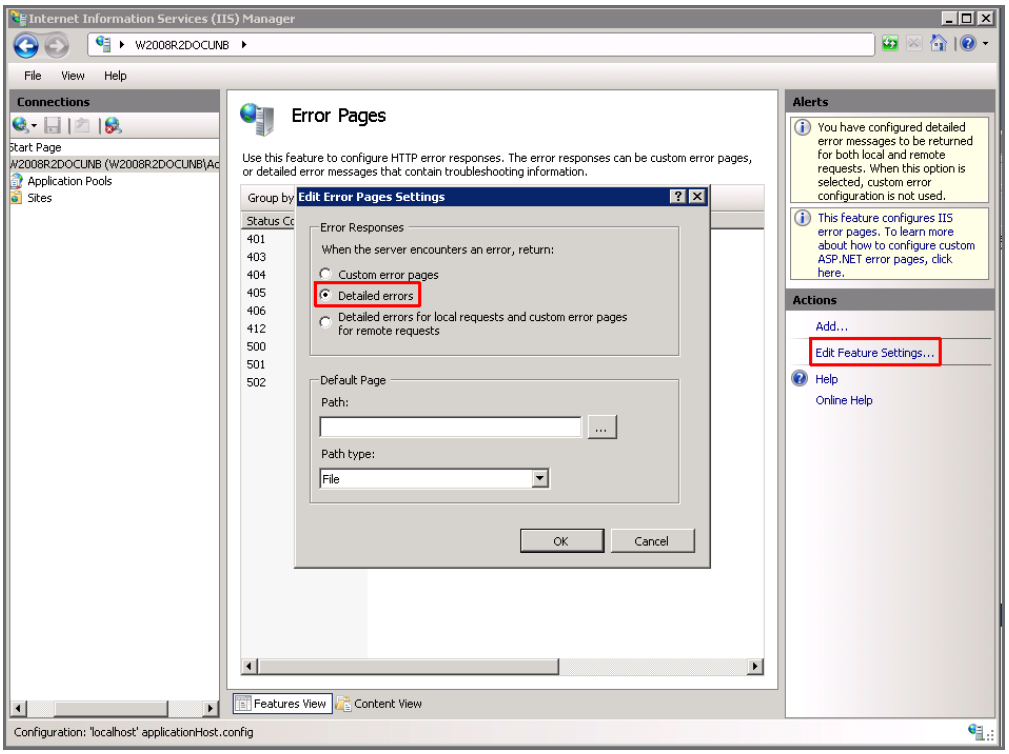
1. To enable the same behavior as with IIS6, simply run the following command:
   `%windir%\system32\inetsrv\appcmd set config -section:asp -scriptErrorSentToBrowser:true`
   Alternatively, you can do this manually in the IIS Manager:
   a. Open the IIS Manager.
   a. Navigate to ***ASP > Debugging Properties > Send Errors to Browsers*** and set the value to ***True***.

b. Click ***Apply.***

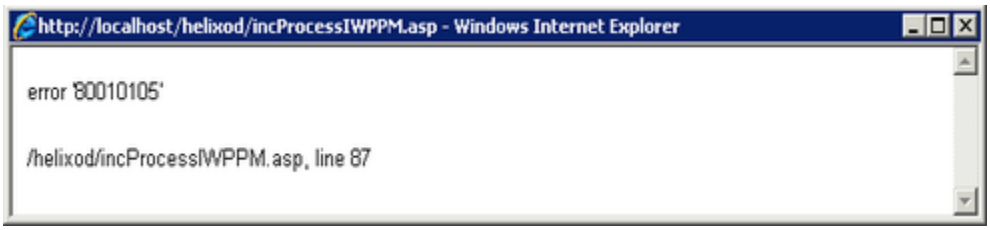


2. If this is required, you also have to configure the IIS custom-error to allow detailed errors to be sent to remote clients.
   `%windir%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpErrors -errorMode:Detailed`
   (default is DetailedLocalOnly)
   Alternatively, you can do this manually in the IIS Manager:
   a. Open the IIS Manager.
   b. Navigate to ***Error Pages > Edit Feature Settings... > Error Responses*** and select the radio button ***Detailed Errors***.

c. Click ***OK***.



Note that you most probably would never want to do the last step on a production server.



3.17.2 CPCA Logging

To enable CPCA logging:

1. Click on ***Start***.
2. Type *regedit* into the input field.

Windows Registry Settings

uniFLOW server:

Data Type: ***REG_SZ*LogFilePath**	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom\Device*Agents\CpCaLogReader 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\DeviceAgents\CpCaLogReader*
Value Name:	*LogFilePath*
Value Type:	*REG_SZ*
Value Data:	e.g. *c:\temp*

RPS:

LogFilePath	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom\MomAps\CpCaLogReader* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomAps\CpCaLogReader*
Value Name:	*LogFilePath*
Value Type:	*REG_SZ*
Value Data:	e.g. *c:\temp*

Set this key to a local directory on the server, and the CPCA Log Reader will store log extracts from the device in binary form and log files for each device in text file format (<Device IP-Address>.log). Binary files can be analyzed by our technical support in order to detect changes in the CPCA implementation of the devices. Text log files are to be analyzed with notepad.

This is a system wide key and each device configured in uniFLOW will log the CPCA communication from each device into the directory entered in the above Windows registry key. After checking, please deactivate this key (delete) and restart the service again.

Changed settings require a restart of the uniFLOW services.

3.17.3 CRQM Logging

To enable the advanced logging functionality for CRQM you need to add the following Windows registry key on the respective server.

Enable CRQM Logging on a uniFLOW Server

Registry Settings:

LogFilePath	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\NT-ware\Mom\CRQM* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\CRQM*
Value Name:	*LogFilePath*
Value Type:	*REG_SZ*
Value Data:	*C:\CRQMLogs\crqmlog.txt*

The folder must exist. A restart of the uniFLOW Server service is necessary. The log/txt file *crqmlog.txt* will be created in the folder defined in the registry key.

Enable CRQM Logging on an RPS

Registry Settings:

LogFilePath	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\NT-ware\Mom\MomAPS\CRQM* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomAPS\CRQM*
Value Name:	*LogFilePath*
Value Type:	*REG_SZ*
Value Data:	*C:\CRQMLogs\crqmlog.txt*

The folder must exist. A restart of the RPS service is necessary. The log/txt file *crqmlog.txt* will be created in the folder defined in the Windows registry key.

3.17.4 Database Backup

If uniFLOW runs with an external database (DsPcDB), the database server or database has to be backed up separately. For database backups see also chapter Microsoft SQL Server Data Engine (MSDE) (on page 22).

When backing up a Microsoft SQL 2008 R2 Express Edition or SQL Server please follow Microsoft's best practice. The following chapters serve as examples.

For more information about the uniFLOW database, please refer to white paper *Database Structure of uniFLOW and HelixPW* in the NT-ware Knowledgebase.

Before you start any backup, please ensure there is sufficient storage space.

3.17.4.1 Microsoft SQL Server 2008 R2 Express

There are several ways to make a complete backup of the uniFLOW Database with Microsoft SQL Server 2008 R2 Express. The easiest way is to use the OSQL commands as follows:

Backup

Please start the following command in the command line:

osql -S (server) -E -Q "BACKUP DATABASE <databasename> TO DISK = '<name of backupfile>'"

e.g.

osql -S (local) -E -Q "BACKUP DATABASE DsPcDb TO DISK = 'C:\backup\dspcdb.bak'"

With this you can backup the local database DsPcDb into the file ***C:\backup\dspcdb.bak***.

Restore

To restore the database from this file just type:

osql -S (server) -E -Q "RESTORE DATABASE <databasename> FROM DISK = 'name of backupfile'"

e.g.

osql -S (local) -E -Q "RESTORE DATABASE dspcdb FROM DISK = 'C:\backup\dspcdb_bak'"

Further possibilities to backup the database with Microsoft SQL Server 2008 R2 Express

- You can install the Microsoft SQL Server Management Studio Express to make backups with the help of a GUI (Graphical User Interface). Microsoft SQL Server

2008 R2 Management Studio Express (SSMSE) is an integrated environment for accessing, configuring, managing, administering, and developing all components of SQL Server Express and can be downloaded under the following link:

http://www.microsoft.com/en-us/download/details.aspx?id=22985
(http://www.microsoft.com/en-us/download/details.aspx?id=22985)

- Use the SnapShotTool.exe for a complete database backup or restore.

3.17.4.2 Microsoft SQL Server 2008

1. Open the Microsoft SQL Server Management Studio from ***Start > All Programs > Microsoft SQL Server 2008***.
2. Connect to the server database module with server type, server name, authentication method, user name and password.
3. Extend the folder tree on the left hand side of the window by clicking on the server name.
4. Extend the folder tree on the left hand side of the window by clicking on the database folder.
5. Choose the database which you want to backup (in our case DsPcDb).
6. Right click on the chosen database / Tasks / Backup.
7. In the upcoming wizard verify that the right database is displayed.
8. Set backup type to ***Full Backup***.
9. Set target to the correct storage path on the disk.
10. With a click on ***OK*** the backup will start.
11. After having finished you will find the database backup in the chosen folder (the default folder is: `%ProgramFiles%\Microsoft SQL Server\MSSQL.nn` (nn depends on the installed instances) `\Backup\`)

In some cases the database transaction log file DsPcDb_log.LDF can grow to a huge size and slow down the SQL server. In the Microsoft SQL Server Management Studio we have the possibility to create a maintenance task that backups the database and clears the log file.

For more information go to the Microsoft Knowledgebase article How to stop the transaction log of a SQL Server database from growing unexpectedly (http://support.microsoft.com/kb/873235/en-us).

3.17.4.3 Microsoft SQL Server Data Engine (MSDE)

Before you decide to make major changes in uniFLOW, it can make sense to export the uniFLOW database to a test system to check, if the desired changes are done correctly.

Sometimes, it can also be helpful to provide a uniFLOW database to the NT-ware support for a deeper analysis of a problem without touching the system of the user.

MSDE Database Backup

The MSDE database includes a command-line utility named *Osql.exe* that can be used to back up and restore a Microsoft Data Engine (MSDE) database on a disk or tape.

How to back up an MSDE database to a disk or tape drive

- **Step 1**
  At a command prompt on the MSDE database server, type the following and press ENTER.
  `osql -Usa -Ppassword`

  The switches/parameters for Osql.exe are case sensitive and have to be entered as shown above. Replace "sa" and "password" with the "sa" account name and the belonging password.

Backup to disk drive:

- **Step 2**
  To back up the MSDE database on a disk, at the OSQL's prompt, type the following and press ***ENTER***.
  BACKUP DATABASE DsPcDb TO DISK = 'C:\DsPcDb.bak'

  If you use *BACKUP DATABASE DsPcDb TO DISK = 'DsPcDb.bak'* **the backup is stored in the subfolder called backups of the MSSQL installation path (usually located at C:\MSSQL.1\MSSQL\Backup).**
  Note that write access to C:\ directly may be restricted for certain user accounts.

- **Step 3**
  At the 2> prompt, type *GO* and press ***ENTER***.

Backup to tape drive

- **Step 2**
  To back up the MSDE database on a tape device, type the following and press ***ENTER***.
  BACKUP DATABASE DsPcDb TO TAPE = tape_device
- **Step 3**
  At the 2> prompt, type *GO* and press ***ENTER***.

If the backup has been done, you will get an info text about the backup process. To exit the OSQL command prompt, type *EXIT* and press ***ENTER***.

MSDE Database Restoration

- It is possible to restore a database backup from a SQL 2000 to a SQL 2005/2008 database. The database will be converted to the new database format.
- It is impossible to restore a SQL 2005/2008 or SQL Express 2005/2008 (R2) backup to a SQL 2000 or MSDE 2000 database. If doing so, you will receive the following error messages:
  `Msg 3205, Level 16, State 2, Server <SERVERNAME>, Line 1 Too many backup devices specified for backup or restore; only 64 are allowed.`
  `Msg 3013, Level 16, State 1, Server <SERVERNAME>, Line 1 RESTORE DATABASE is terminating abnormally.`
- Before restoring a uniFLOW database, make sure the uniFLOW server is not running. It is sufficient to stop the uniFLOW Server service. If you try to restore a database and uniFLOW is still running and connected to the database, you will receive the following error messages:
  `Msg 3101, Level 16, State 1, Server <SERVERNAME>, Line 1 Exclusive access could not be obtained because the database is in use.`
  `Msg 3013, Level 16, State 1, Server <SERVERNAME>, Line 1 RESTORE DATABASE is terminating abnormally.`

1.1.1.1.1.1 Same Database Server

The following describes how to restore an MSDE database to the database from where you have created the backup.

- **Step 1**
  At a command prompt on the MSDE database server, type the following and press ***ENTER***.
  osql –Usa –Ppassword
  The password for a uniFLOW MSDE database installation is by default ***ntwsapwd***

  The switches/parameters for Osql.exe are case sensitive and have to be entered as shown above. Replace "sa" and "password" with the "sa" account name and the belonging password.

Restore from disk drive

- **Step 2**
  To restore the MSDE database from a disk, at the OSQL's prompt, type the following and press ***ENTER***.
  RESTORE DATABASE DsPcDb FROM DISK = file_path
  where *file_path* is a full path to an existing backup file enclosed in single quotation marks (for example, 'C:\DsPcDb.bak').
- **Step 3**
  At the 2> prompt, type *GO* and press ***ENTER***.

Restore from tape drive

- **Step 2**
  To restore the MSDE database from a tape device, type the following and press ***ENTER***.
  RESTORE DATABASE DsPcDb FROM TAPE = tape_device
  where *tape_device* is the device name of your tape drive (for example, \\.\tape0).
- **Step 3**
  At the 2> prompt, type *GO* and press ***ENTER***.

To exit the OSQL command prompt, type *EXIT* and press *ENTER.*

1.1.1.1.1.2 Existing but Different uniFLOW Database

The following describes how to restore an MSDE database to an already existing uniFLOW database whereas the backup has not been made from that system.

Execute the steps 1. to 3. from the topic Same Database Server (Restoring to an MSDE Database to the Same Database Server). Afterwards execute the following:

- **Step 4:**
  If you restore a database on a system where a different uniFLOW database already exists, the user pbaip will have a different OID after the restore procedure. Type the following OSQL command to fix this problem:
  ```
  sp_change_users_login 'auto_fix',pbaip
  sp_change_users_login 'auto_fix',uFReader
  ```
- **Step 5:**
  At the 2> prompt, type *GO* and press ***ENTER***.

1.1.1.1.1.3 DB Server Where No uniFLOW DB Exists Yet

The following describes how to restore an MSDE database to a database server where no uniFLOW database exists yet.

Execute the steps 1. to 3. from the the topic Same Database Server.

- **Step 4:**
  After restoring the database, you have to type the following statements in OSQL (MSDE) or into the Query Analyzer (SQL Server 2000 / 2005):

```
USE Master
GO
if not exists (select * from master.dbo.syslogins where loginname
= N'uFReader')
BEGIN
   declare @logindb nvarchar(132), @loginlang nvarchar(132)
select @logindb = N'DsPcDb', @loginlang = N'us_english'
   if @logindb is null or not exists (select * from
master.dbo.sysdatabases where name = @logindb)
         select @logindb = N'master'
   if @loginlang is null or (not exists (select * from
master.dbo.syslanguages where name = @loginlang) and @loginlang
<> N'us_english')
         select @loginlang = @@language
   exec sp_addlogin N'uFReader', N'NtwR3adPwd', @logindb,
@loginlang
END
GO
if not exists (select * from dbo.sysusers where name = N'uFReader'
and uid < 16382)
   EXEC sp_grantdbaccess N'uFReader', N'uFReader'
GO
exec sp_addrolemember N'db_datareader', N'uFReader'
GO
USE DsPcDb
GO
exec sp_change_users_login 'auto_fix',uFReader
GO
```

3.17.4.4 Database Restoration

If you restore your database on a different or a new system, this will cause a problem. The new database user has a different GUID than the old one and accessing the database is not possible anymore. After the restore procedure has been completed it is necessary to repair the database user in order to gain access to the database for uniFLOW.

3.17.5 Dump Generation

A memory dump consists of the recorded state of the working memory of a computer program at a specific time, generally when the program has terminated abnormally (crashed). Sometimes it is necessary to create a memory dump of a specific process or NT service that crashed, in order to analyze the cause of the crash.

In most cases, the dump file created via the Internal Exception Handling and Dump Creation of uniFLOW is sufficient for analyzing most problems:

- Internal Exception Handling and Dump Creation (on page 28)

Sometimes, however, dump creation with the DebugDiag tool is necessary for a complete memory dump of the process in question.

If the time and action that cause a process to crash can be reproduced and the server is monitored during the crash, a manual dump can be initiated:

- Dump Creation with DebugDiag (Manual Dump) (on page 29)

If the specific time and action that causes the process to crash is unknown, an automatic dump can be configured:

- Dump Creation with DebugDiag (Automatic Dump) (on page 31)

3.17.5.1 Internal Exception Handling and Dump Creation

Software

uniFLOW server ≥ V5.0

uniFLOW RPS ≥ V5.0

uniFLOW Scan Processing Server

Description

In order to catch so-called exceptions originating from programming mistakes and abnormal program termination (crashing), uniFLOW has been enhanced with an internal exception handling mechanism.

This internal exception handling mechanism basically sits idle and only comes to life if an exception occurs. Before terminating the program a crash dump file (minidump) is written to the server's hard disk and an entry is made in the *techsupport.log*, detailing the problem that occurred and the name of the file written.

The dump file is usually very small and can easily be uploaded to NT-ware. Even though it is small, it contains a lot of important information, including the cause of the problem. Most of the errors that occur can be located in this way.

How to find the Log Entries and the Dump File

In case of a crash, the dump file and the corresponding XML file are stored under:

C:\Program Files\Common Files\NT-ware Shared\Data

The XML file is called *SysLog_<servername>_<username>.XML*. It contains an export of the *techsupport.log* and contains a section like the following:

```
<Entry>
<EntryTime>2010-04-01 00:00:02</EntryTime>
<EntryType>0</EntryType>
<JobID>{00000000-0000-0000-0000-000000000000}</JobID>
<Description>critical error 0xE06D7363 occurred, dump file written to C:\Program Files\Common Files\NT-ware Shared\Data\\ddd7fc4e-c6b6-4e8c-b83a-8657b11b0c1f.dmp</Description>
</Entry>
```

Here you will find the respective name of the dump (.dmp) file that is stored in the same folder.

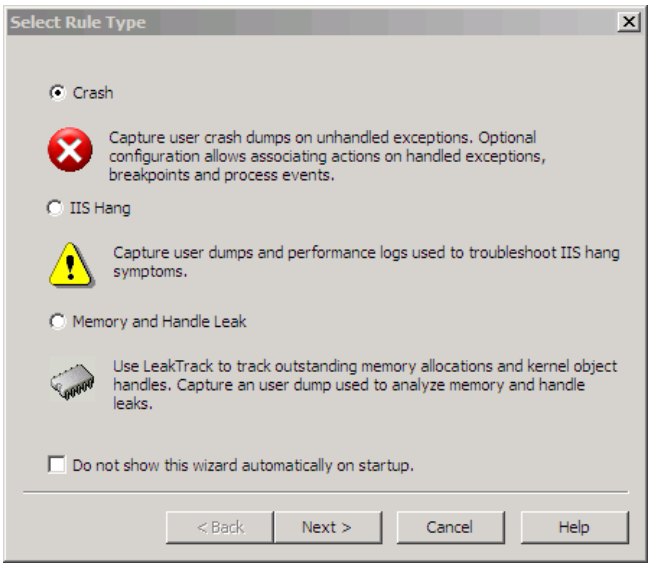
Send the .dmp file together with the corresponding .xml file to NT-ware for further analysis.

3.17.5.2 Dump Creation with DebugDiag (Manual Dump)

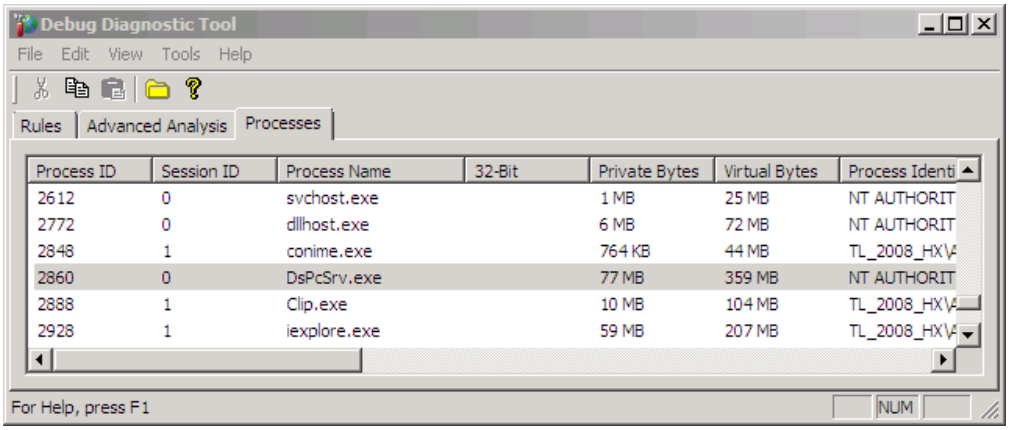
Download the Debug Diagnostic Tool V2.2 here (https://www.microsoft.com/en-us/download/details.aspx?id=49924).

1. Install the tool on the uniFLOW server or RPS that is on the server that tends to crash from time to time.
2. After the installation, start the tool under ***Start > All Programs > Debug Diagnostic Tool2 > DebugDiag 2 Collection***.

3. Cancel the wizard that is starting up.



4. Now go to the ***Processes*** tab.
5. When the error is visible (for instance, if *DsPcSrv.exe* or *MomAps.exe* are hanging or not responding), right-click on the affected process and click on ***Create*** full user dump.



6. This dump can be found in the following folder:
   C:\Program Files\DebugDiag\Logs\Misc

Recommendation

- In case the memory usage of the process is unexpectedly high, one manual dump file is required for further analysis.
- In case the process reacts slow or uses a high amount of CPU time, multiple dump files are required for further analysis. Please create at least three manual dump files in one minute intervals.

Sending Dump Files

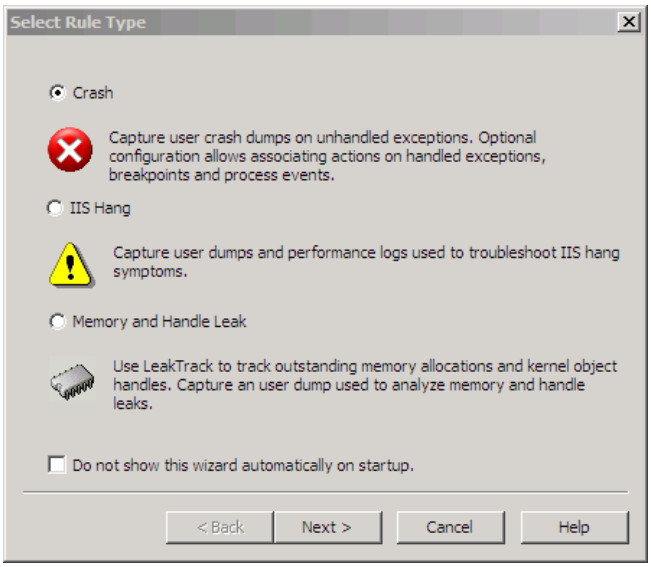
Please zip the dump file and send it to NT-ware for deeper analysis.

The best way to do this is via NT-ware's "File Exchange Interface". Please contact NT-ware support for further details.

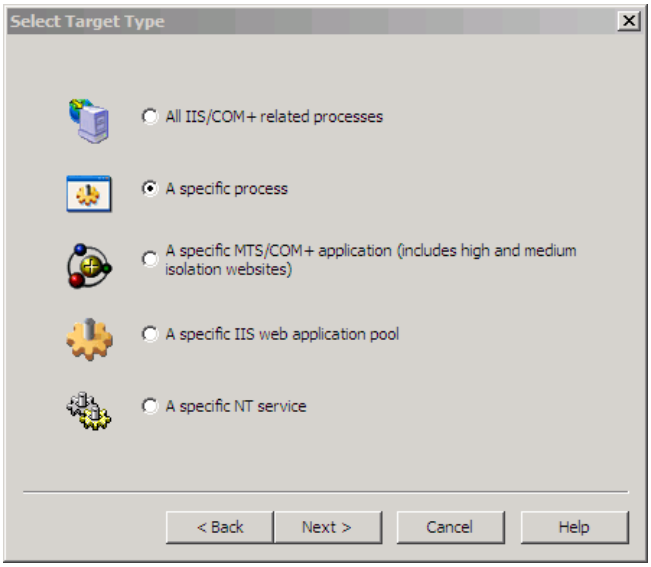
3.17.5.3 Dump Creation with DebugDiag (Automatic Dump)

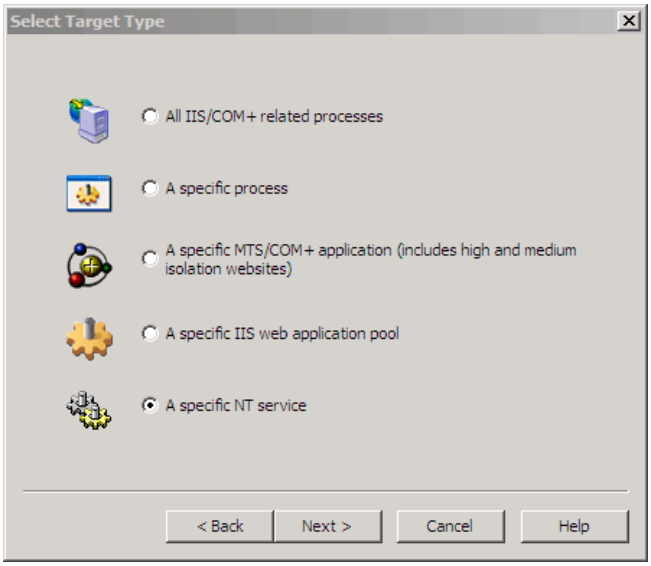
Download the Debug Diagnostic Tool V2.2 here (https://www.microsoft.com/en-us/download/details.aspx?id=49924).

1. Install the tool on the uniFLOW server or RPS that is on the server that tends to crash from time to time.
2. After the installation, start the tool under ***Start > All Programs > Debug Diagnostic Tool2 > DebugDiag 2 Collection***.
3. In the starting wizard please choose ***Crash*** and click on ***Next***.

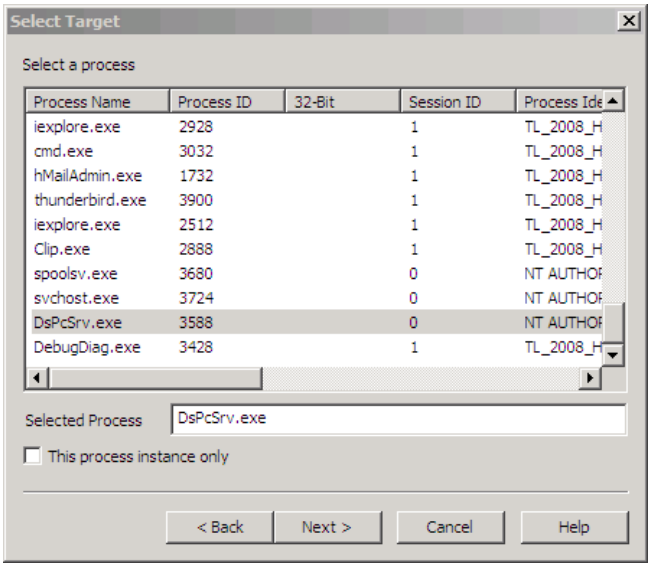


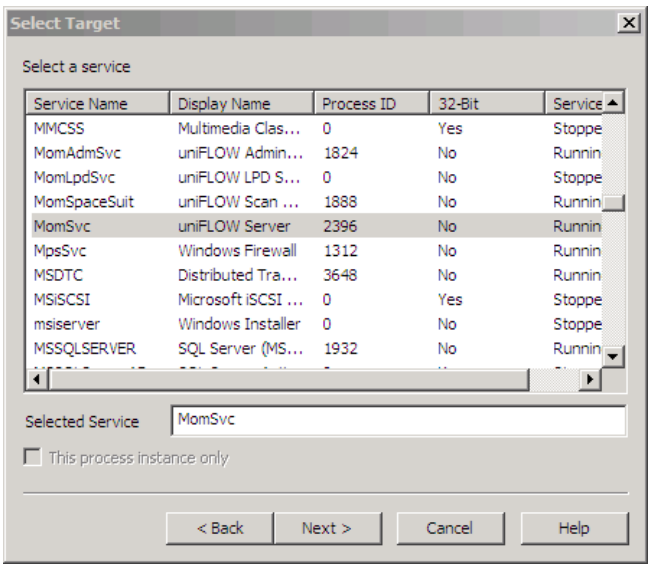
4. Select ***A specific process*** or ***A specific NT service*** depending on what you want to capture and click ***Next***.





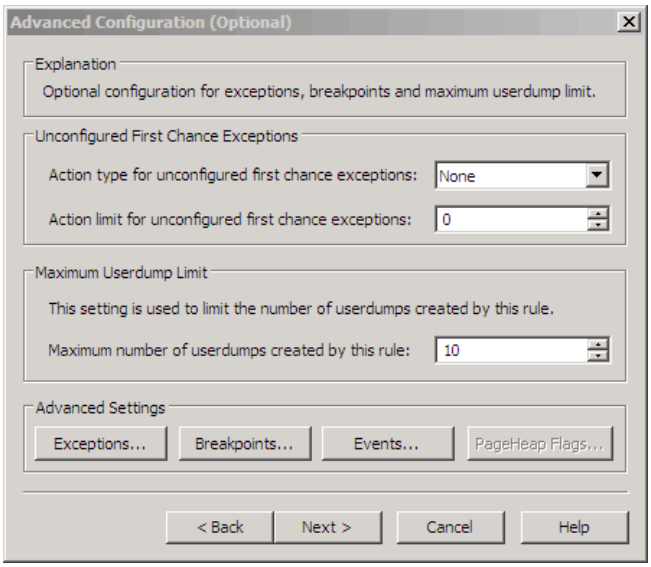
5. Select the process or service that is expected to crash (*DsPcSrv.exe* or *MomSvc* etc.) and click ***Next***.



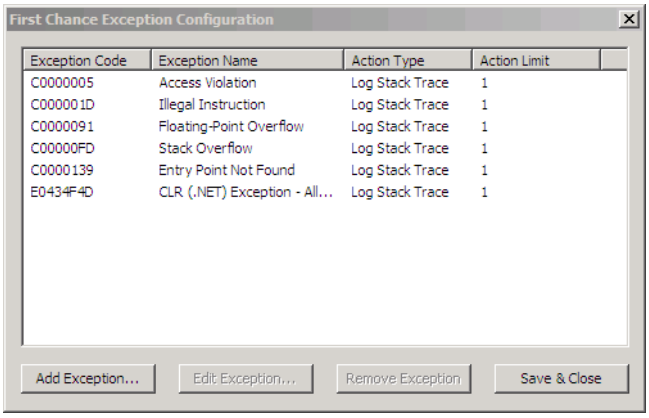


6. In the ***Advanced Configuration*** select ***None*** under ***Action type for unconfigured first chance exceptions***.

7. Set the ***Action limit for unconfigured first chance exception***s to 0.

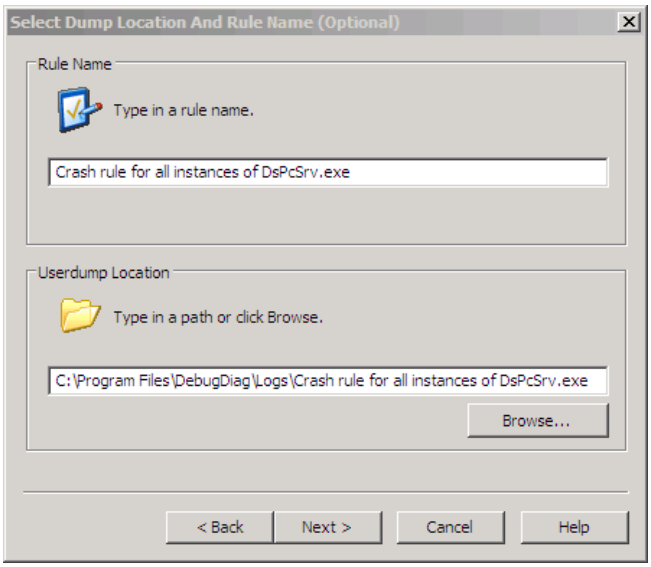


8. Click on ***Exceptions***.
9. Click on ***Add Exception...*** and add the following exceptions:
   - ***Access Violation***
   - ***Illegal Instruction***
   - ***Floating-Point Overflow***
   - ***Stack Overflow***
   - ***Entry Point Not Found***
   - ***CLR (.NET) Exception***

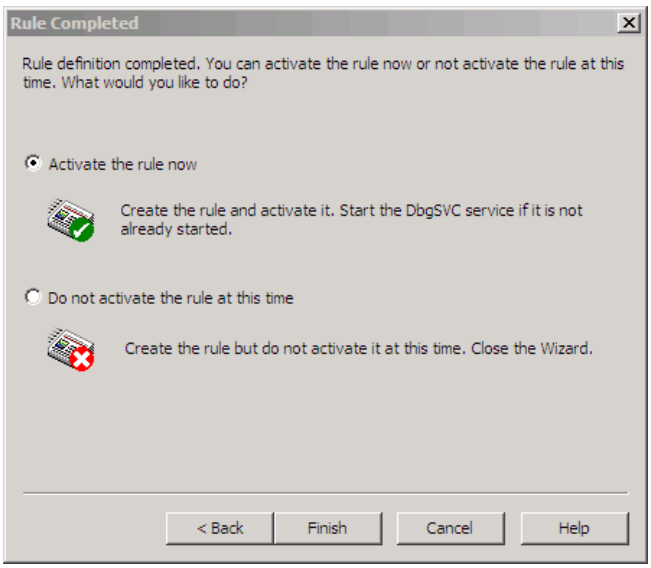


10. Confirm with ***Save & Close***.
11. Click ***Next***.

12. Type in a name for the rule, modify the path if necessary and click ***Next***.



13. Activate the rule in the next window and click on ***Finish***.



If the crash occurs again, please navigate to the dump folder.

Please zip the dump file and send it to NT-ware for a thorough analysis.

The best way to do this is via our "File Exchange Interface". Please contact our support for further details.

3.17.6 EAI Logging

To enable EAI logging:

1. Click on ***Start***.
2. Type *regedit* into the input field.

Windows Registry Settings

uniFLOW server:

EAI_LogFilePath	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\NT-ware\Mom* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom*
Value Name:	*EAI_LogFilePath*
Value Type:	*REG_SZ*
Value Data:	e.g. *c:\temp*

RPS:

EAI_LogFilePath	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\NT-ware\Mom* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom*
Value Name:	*EAI_LogFilePath*
Value Type:	*REG_SZ*
Value Data:	e.g. *c:\temp*

Set this key to a local directory on the server. There are two types of log files that are written:

- One log file in XML format for each device configured.
  EAI_<manufacturer>_<serialnumber>_<server-name>_<date>_<time>.log
- One single log file that comprises all device capabilities for all EAI devices found on the network.
  EAI_Discover_DeviceCapabilities_<server-name>_<date>_<time>.log

After each service restart there will be a new set of the above files.

This is a system wide key and each device configured in uniFLOW will log the EAI communication from each device into the directory entered in the above Windows registry key. After checking, please deactivate this key (delete) and restart the service again.

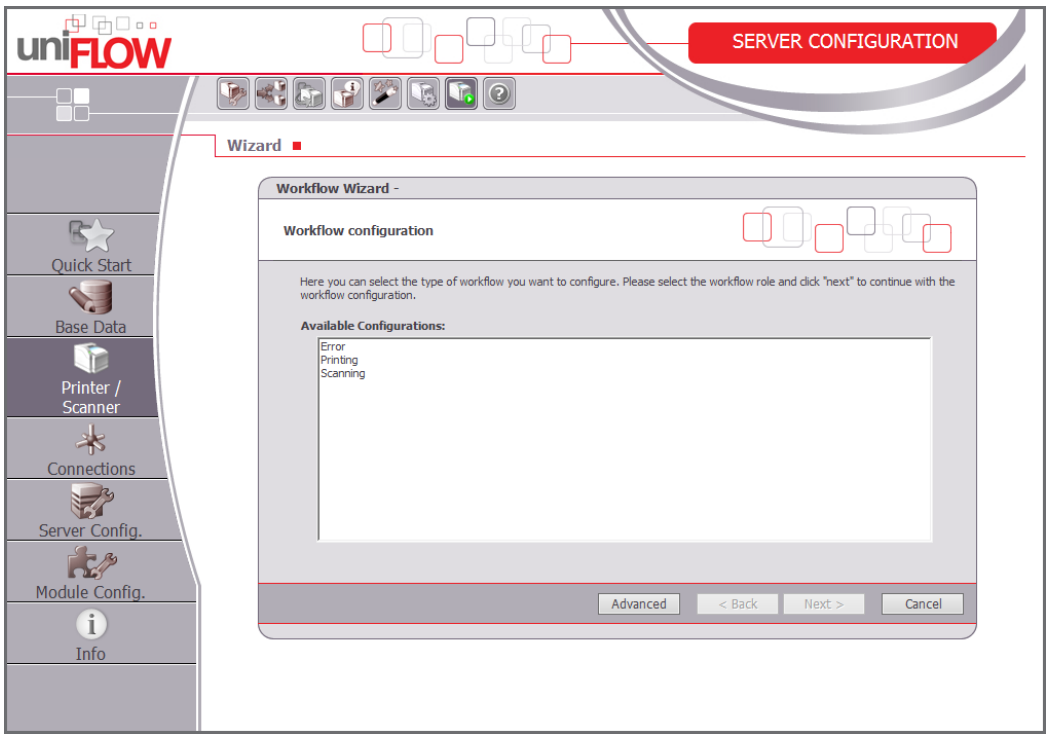
Changed settings require a restart of the uniFLOW services.

3.17.7 Error Role

In case an error occurs in a uniFLOW workflow, the error workflow engine is triggered. This can be used to write an error workflow log automatically and to send an appropriate email.

The ***Error*** workflow that can be configured with the ***Workflow Wizard*** can be used to ensure a consistent behavior for workflow errors in uniFLOW. The error workflow can be configured in such a way that the administrator is sent an error notification. There will be error logs for a later evaluation of the errors, and it is possible to automatically delete all jobs that produced a workflow error.

To configure a (default) Global Workflow for the ***Error*** role, click the ***New*** icon on the ***Global Workflows*** overview page and select ***Error***.



The wizard will guide you through all necessary settings.

Make sure the log files folder exists: *C:\logfiles\error*

If you would like to change the default parameters, you can add or delete tokens.

The final step of the wizard is the ***Save Workflow*** page. This page allows you to either tick the ***Default Global Workflow*** checkbox, in order to save the configured error workflow as a ***Default Global Workflow,*** or to give the error workflow a name and save it as a named Global Workflow.

Note that you can also tick the ***Default Global Workflow*** checkbox if a Default Global Workflow already exists, you will in that case overwrite the settings of the existing Default Global Workflow with the current configuration settings.

Clicking on the ***Finish*** button will complete the configuration of the error workflow and guide you back to the overview page of ***Global Workflows***. On that page you should now also see the error workflow you have just completed.

3.17.8 HTTP Access Logging

To enable further HTTP logging on the uniFLOW server or the uniFLOW RPS for Windows, the following Windows registry key needs to be added.

Windows Registry Settings

HttpAccessLogPath	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\NT-ware\Mom* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom*
Value Name:	*HttpAccessLogPath*
Value Type:	*REG_SZ*
Value Data:	e.g. *c:\logs\httpaccesslog.log*

The "System" and "Everyone" user needs full access to this folder. The file will be created automatically.

Changed settings require a restart of the uniFLOW services.

Please keep in mind that you need to delete this key after the logging has been done.

3.17.9 HTTP Error Codes

Client Errors

- 400 Bad Request:
  The server cannot or will not process the request due to something that is perceived to be a client error.
- 401 Unauthorized:
  Similar to 403 Forbidden, but specifically for use when authentication is required and has failed or has not yet been provided. The response must include a WWW-Authenticate header field containing a challenge applicable to the requested resource. See Basic access authentication and Digest access authentication.

- 402 Payment Required:
  Reserved for future use. The original intention was that this code might be used as part of some form of digital cash or micropayment scheme, but that has not happened, and this code is not usually used. YouTube uses this status if a particular IP address has made excessive requests, and requires the person to enter a CAPTCHA.
- 403 Forbidden:
  The request was a valid request, but the server is refusing to respond to it. Unlike a 401 Unauthorized response, authenticating will make no difference.
- 404 Not Found:
  The requested resource could not be found but may be available again in the future. Subsequent requests by the client are permissible.

Server Errors

- 500 Internal Server Error:
  A generic error message, given when an unexpected condition was encountered and no more specific message is suitable.

3.17.10 HTTPS Communication

uniFLOW provides the option of enforcing HTTPS communication on the internal web server.

If you select this option during the installation or an update, the option ***ForceHTTPS*** is enabled in the Windows registry.

This setting can have a negative impact if set unintentionally where components that are not updated, e.g. uniFLOW MEAP Applets, Scan Processing Server(s) or uniFLOW clients, will stop communicating.

- Enabling the ***Enforce HTTPS*** option requires components which communicate with the internal HTTP server to support communication via HTTPS. HTTP requests are not accepted.
  Therefore, make sure that the following components have at least been upgraded to the required minimum version in order to fully support HTTPS communication:
  - uniFLOW MEAP Client / Universal Login Manager requires V4.2 or higher.
  - Scan Processing Server requires *MomSpaceSuit* from uniFLOW V5.3 or higher.
  - Remote Print Server (RPS) requires uniFLOW V5.3 or higher.
  - uniFLOW Client for Windows requires uniFLOW V5.3 or higher.
  - uniFLOW Universal Driver requires uniFLOW V5.3 or higher.
- EAI mobile and uniFLOW Embedded Applets (Multi-Vendor Support) are not affected by this setting and are still able to communicate on the HTTP port.

For disabling the HTTPS enforcement configure ***ForceHTTPS*** as follows on the uniFLOW server.

Windows Registry Settings

ForceHttps	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\NT-ware\Mom\MomTcpServer* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomTcpServer*
Value Name:	*ForceHttps*
Value Type:	*REG_DWORD*
Value Data:	*0*

3.17.11 ICARUS Server for Web

Logs

There are three log files that can be analyzed.

The log file names, paths and sizes can be configured in the section log4net of the XML file named Web.config which can be found in the installation folder of ICARUS Server for Web.

The log folder configured here has to be writable by IIS.

For information on log4net see https://logging.apache.org/log4net/

- *application_lifecycle.log*
  This file contains log data on start-up and shut-down of the application.
- *application.log*
  This file contains log data on the normal operation. The majority of entries concern connection issues from and to the ICARUS Clients for Web.
- *remoteclient.log*
  This log is filled with data only if the value of the key *ClientLogger* in the file Web.config is set to "Remote". The default setting is "Console".
  The log contains timestamps, IP data and other useful information from the ICARUS Client for Web.
  The log level can be changed by editing the numeric value of the key *ClientLogLevel* in the file Web.config:
  - *0*
    None:
    No logging
  - *1*
    Error:
    Only Error messages.

- *2*
  Warn:
  Only error and warning messages.
- *3*
  Info (default):
  Verbose logging.
- *4*
  All:
  Debug level.

Keep in mind that setting *ClientLogger* to "Remote" creates high network traffic and should only be active when really needed.

Network Traffic Analysis

1. uniFLOW to ICARUS Server for Web: CUI communication protocol
   This can show whether uniFLOW actually sends out the correct commands for configuring a device or loading a UI.

For testing this, the ICARUS Server for Web should be configured in the Network Configuration section via its HTTP address and not via HTTPS.
Tools like Wireshark do not support capturing of traffic that is sent via localhost communication, for instance, when ICARUS Server for Web and uniFLOW are installed on the same machine.

2. ICARUS Server for Web to uniFLOW: UI loading and ICARUS request relaying.
   This can show whether an ICARUS UI definition (XML and Script) could be loaded and whether the proxying of requests works and actually reaches the correct server.

For testing this, the MomTcpServer should be configured without an HttpsPort and with disabled ForceHttps.
Tools like Wireshark do not support capturing of traffic that is sent via localhost communication, for instance, when ICARUS Server for Web and uniFLOW are installed on the same machine.

3. Web client to ICARUS Server for Web: Web page and image retrieval, ICARUS requests and real-time updates.
   This can show what platform configuration is contained in the initial starting page, what requests are transferred to uniFLOW (via the proxy) and what real-time updates (UIs, events, commands) the ICARUS Server for Web sends to the client.

For easily testing this access the ICARUS Server for Web on its HTTP URL and disable static/dynamic content compression on IIS to avoid *unreadable .gzip* encoding.

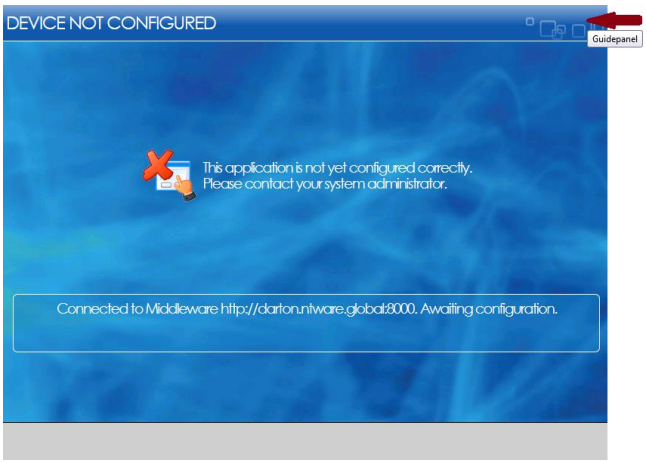
4. Web client or scan device to uniFLOW
   Depending on the device type, this could trace autonomous scan image uploads to uniFLOW.

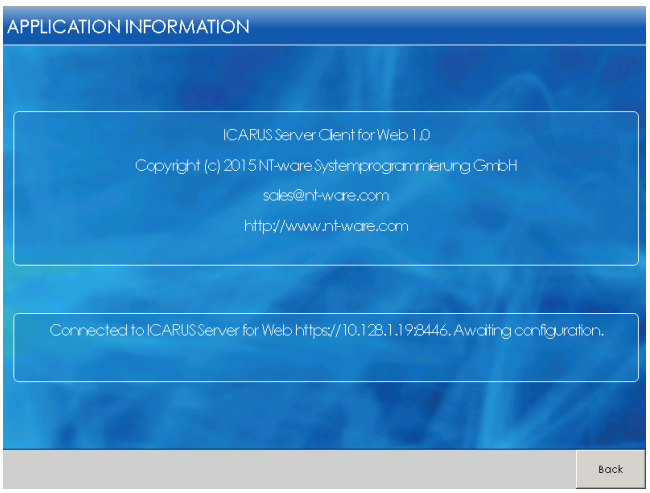
For easily testing this, the MomTcpServer should be configured without an HTTPS port and with disabled ForceHttps setting.

Application Information

On the ICARUS Client for Web, information on the application, version and network parameters can be shown by clicking/tapping on the logo in the right upper corner.

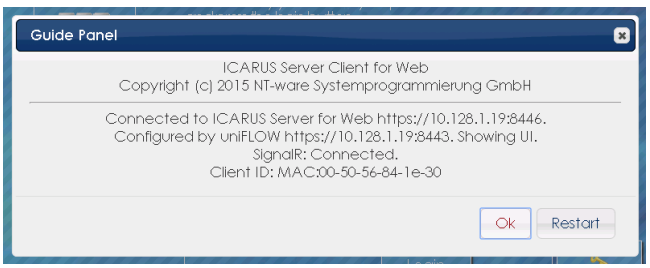
- As long as the client is not configured, the ***APPLICATION INFORMATION*** window opens and shows basic information.





As long as the ***APPLICATION INFORMATION*** window is shown, the client does not try to connect to the ICARUS Server for Web and therefore can not be configured.

- As soon as the client is configured, the ***Guide Panel*** with more detailed information is shown when you click/tap the logo in the right upper corner.



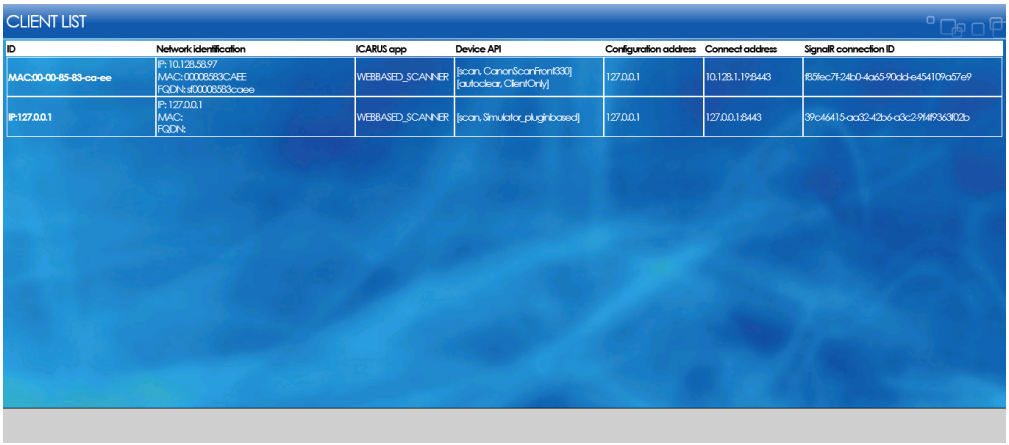
Client List

A list of all connected clients can be shown by opening the status page of the ICARUS Server for Web:

<ICARUS Server for Web base URL>/Status.aspx

or directly

<ICARUS Server for Web base URL>/Status.aspx/ClientList



The table shows the following details:

- ***ID***:
  ID/Serial number of the client.
- ***Network identification***:
  All identified network information that is made available to uniFLOW for matching a client.
- ***ICARUS app***:
  The assigned ICARUS app from the DIF (see MOM-17956).
- ***Device API***:
  All device APIs that are to be loaded based on the DIF (see MOM-17945).
- ***Configuration address***:
  IP from the interface that uniFLOW/RPS uses to contact the ICARUS Server for Web.
- ***Connect address***:
  IP/FQDN and port that was sent by uniFLOW/RPS via the *CUI CONNECTION CONNECTADDRESS[HTTPS]* parameter. HTTPS has precedence here.
- ***SignalR connection ID***:
  Internal ID that indicates an existing real-time connection and that might be used for logging in certain cases.

3.17.12 IIS Backup Creation

The IIS Backup is a built-in function of the Internet Information Services (IIS) that is used to create a backup of the IIS configuration. You can use this to check if the IIS configuration of uniFLOW is correct.

How to use the IIS-Backup

1. In the IIS snap-in on the local computer right-click on the computer icon under ***Internet Information Services***.

2. Click ***Action*** and select ***Backup > Restore Configuration***.
3. Click on ***Create Backup***, choose a name for the backup file and set a password for the file! Setting a password is actually very important as it is not possible to restore this file on another computer if the backup file is not encrypted.

The default location for the backup is the folder *%SystemRoot%\system32\inetsrv\MetaBack*. Please note that this backup procedure only saves the configuration of the IIS and not the contents or websites that are configured within the IIS.

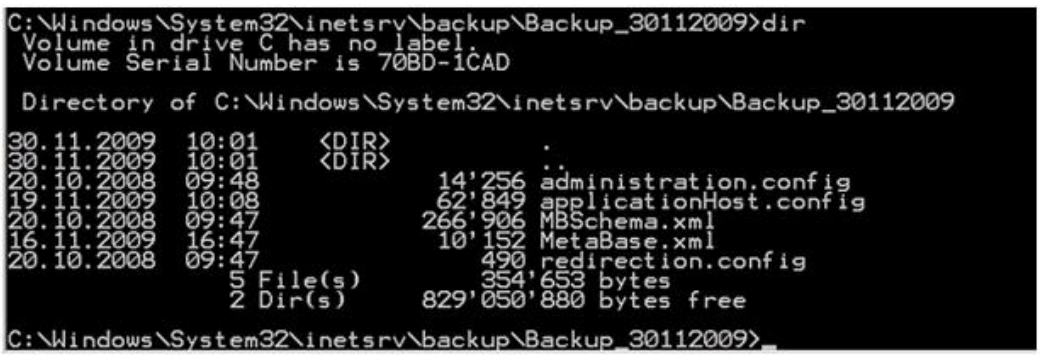
3.17.12.1 Backup of the IIS Configuration on a Windows Server 2008

If you use a Windows Server 2008, please follow the steps below to backup the IIS configuration.

1. Open a command prompt window (*cmd.exe*).
2. Navigate to *\%system_drive%\windows\system32\inetsrv*
3. Type the following command line: *appcmd add backup MyBackup*

The backup is located in

\%system_drive%\windows\system32\inetsrv\backup



3.17.13 IIS Log Analysis

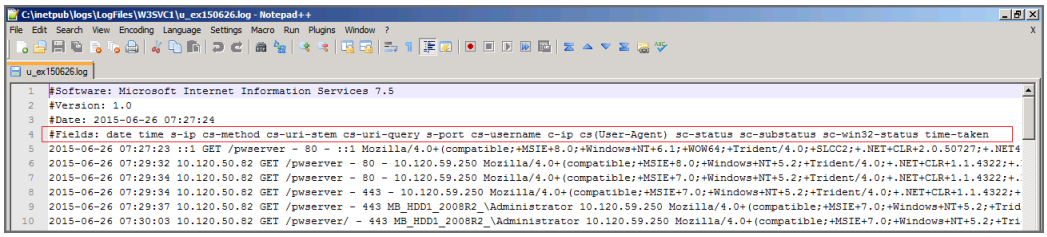
Activation

Please follow this link for a detailed description on how to enable IIS logging:
https://technet.microsoft.com/en-us/library/cc754631(v=ws.10).aspx
(https://technet.microsoft.com/en-us/library/cc754631(v=ws.10).aspx)

Structure

The fourth line (***#Fields***) of the IIS log file describes all the columns each log entry consists of.

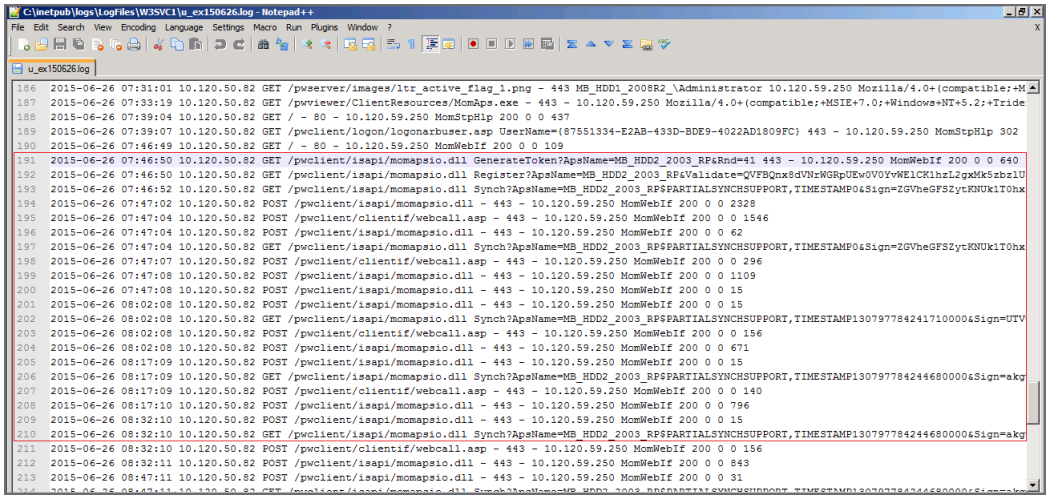
See the example below:



Relevant Keywords

Depending on the problem, the IIS log can be filtered for specific keywords which are used by uniFLOW. Be aware that the log only contains files that are used by the IIS and not the files which are used by the internal MomTCPServer. This includes all the websites like pwserver, pwclient and the connection from the RPS.

The log below shows the connection from an RPS:



You can read from this log that an RPS with the IP 10.120.50.82 and the DNS name MB_HDD2_2003_RP connects to the uniFLOW server. Afterwards a partial synchronization takes place.

The following columns are important for troubleshooting:

- ***time-taken:***
  This column describes how long it took the IIS to generate the feedback to provide it to the client computer. This does not include the time it takes to transfer to the client. This is important for example in case that a website takes a very long time to generate, so you can check if this is down to the network or if the problem already occurred on the server during content generation.
- ***sc-status:***
  All sc-status codes are described on the website https://support.microsoft.com/en-us/kb/943891

(https://support.microsoft.com/en-us/kb/943891). The most important status codes are:

- ***202:***
  Accepted – all okay.
- ***404:***
  File not Found – A file which was tried to access does not exists on the server.
- ***500:***
  Internal Server error – Please deactivate the friendly error messages to check for the root cause of this problem during the website generation.
- ***401:***
  Logon failed – a Login / Authorization failed on the website.

- ***s-port:***
  Describes the port which is used on the server like e.g. 443 or 80 to connect from the client.
- ***c-ip:***
  The ip of the client computer to find out from which client the request to the IIS was made.
- ***cs-uri-stem:***
  The path to the file which was requested from the client computer.

3.17.14 MomRptServer.exe (Reports/Statistics) Log Activation

To enable the advanced logging functionality for the report server (used for the creation of reports and statistics) you need to add the following Windows registry key on the respective server.

Enable Report Server Logging on a uniFLOW Server

Windows Registry Settings:

ReportServerLogPath	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\NT-ware\Mom* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom*
Value Name:	*ReportServerLogPath*
Value Type:	*REG_SZ*
Value Data:	e.g. *c:\logs*

The folder must exist. A restart of the uniFLOW Server service is necessary. The log/txt file 'Report.log' will be created in the folder defined in the Windows registry key.

3.17.15 NetMon Network Trace Generation

With NetMon you can capture all network communication. Try to filter this information, for instance, by selecting a particular time frame you are interested in or by running the tool until you have captured the error.

Download the Tool NetMon from:

ftp://ftp.microsoft.com/pss/tools/netmon/netmon2.zip

(password to decompress: **trace**)

1. Install NetMon on the selected machine.
2. Start Network Monitor from *Start > All Programs > Administrative Tools > Network Analysis Tools > Network Monitor*.
3. Click ***OK*** on the *Select Default Network* dialog.
4. Expand the Local Computer and select the network interface that does NOT state it is a Dial-up connection or VPN.
   If the machine has more than one network card, use *ipconfig /all* to determine the correct MAC address to select.
5. Select ***Capture > Buffer Settings***.
6. Change the buffer size to 20 mb (minimum). DO NOT change the Frame Size of the default value of ***FULL***.
7. Select ***Capture > Filter***.
8. Double-click the ***INCLUDE *ANY <-> *ANY*** line.
9. In the Station 1 Window (left hand side) select ***LOCAL***.
   If the machine has more than one network card use *ipconfig /all* to determine the correct MAC address to select.
10. Click ***OK***.
11. Select ***Capture > Start***.
12. Reproduce the problem.
13. Select ***Capture > Stop and View***.
14. Select ***File > Save As...***.

Please name the file *MOM-nnnn.cap* (MOMPS-nnnn) to relate it to the relevant ITS-issue.

3.17.16 Netstat Usage to Check Open Ports by uniFLOW Services

Netstat is a very useful tool for checking the network connections in use by the uniFLOW services.

It can be used to:

1. Ensure a certain port is listening: e.g. 8000, 8001, 8002, 53213.
2. Ensure the process that is listening on the port is the correct process.
3. Check the number of connections the uniFLOW process is maintaining.

Syntax

Netstat Syntax (http://technet.microsoft.com/en-us/library/ff961504.aspx)

```
netstat -ano
```

Parameter	Description
a	Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
n	Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
o	Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager.

The above command will display all connections, sometimes this can be many pages. Therefore, if you know what you are looking for, e.g. a specific port number (8000) or a specific process ID (from the Windows Task Manager), the results can be piped through the FIND command:

```
netstat -ano | find "8000"
```

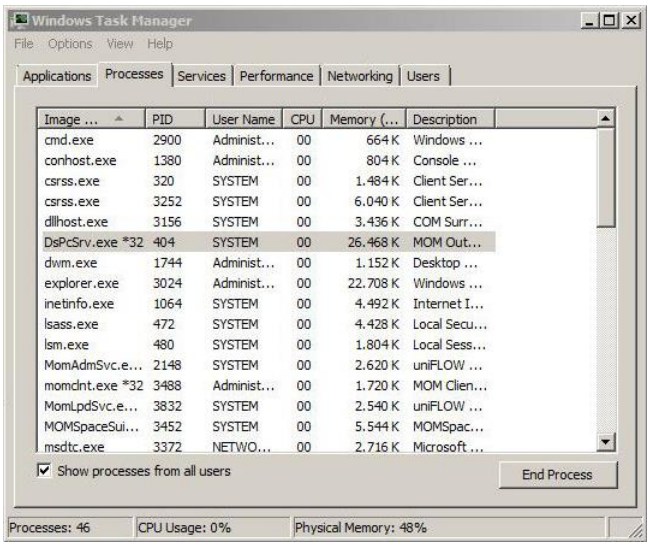
The result of this example is only rows containing 8000 will be displayed.

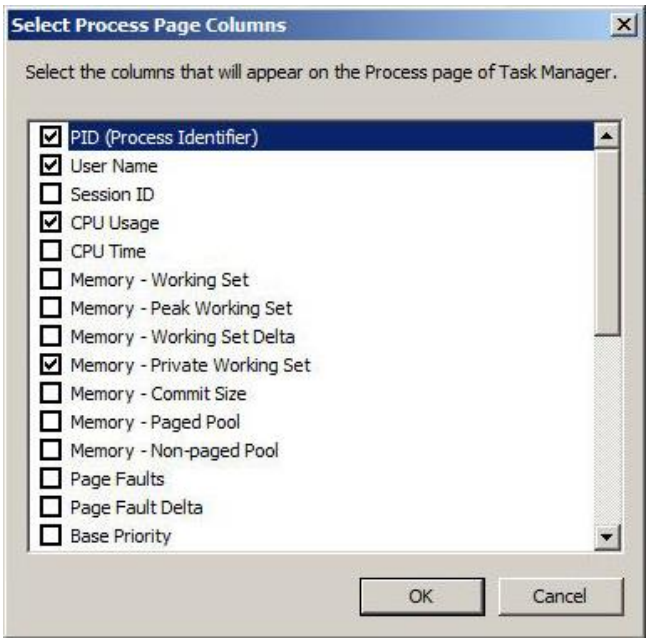
The results can be saved to file using the following syntax:

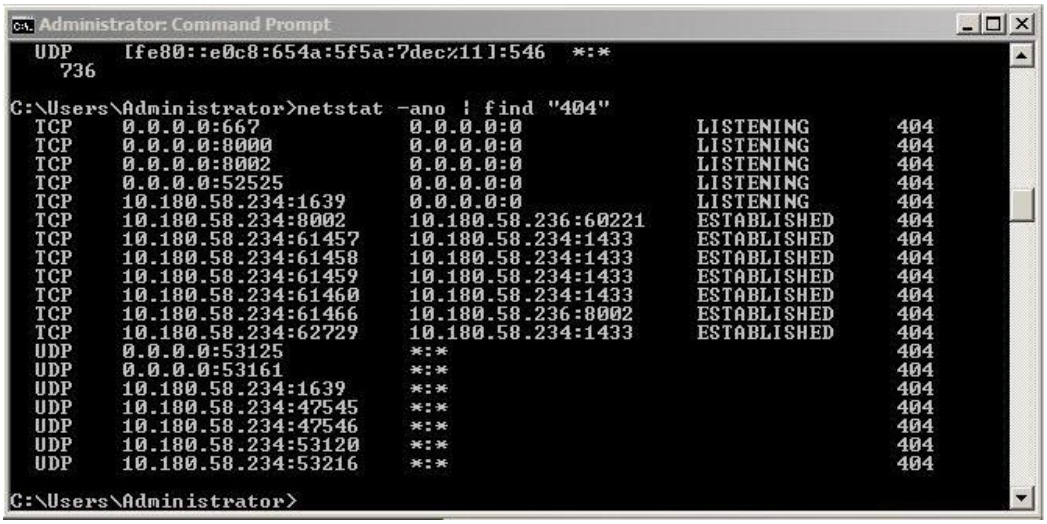
```
netstat -ano | find "8000" > fullpath\filename.log
```

Below are screenshots where the PID column has been added to the task manager (***View*** > ***Select Columns***). This way, it can be determined that the PID of the uniFLOW service is 404. Afterwards, Netstat was run to show all open connections belonging to the uniFLOW process.

In the screenshots, it can be seen that the uniFLOW process is **NOT** listening on 53213, therefore MEAP connections would be failing.







Further information about TCP and UDP ports used by uniFLOW can be found in the *WHITE PAPER - TCP/UDP Ports of uniFLOW and Canon equipment* which can be found in the NT-ware Knowledgebase (see MOMKB-99 (http://its.nt-ware.net/browse/MOMKB-99)).

3.17.17 Océ PRISMAdirect logging

Océ PRISMAdirect supports two logging methods.

mom Tech Support Interface

All errors and informational messages are logged in the ***mom Tech Support Interface***. Each entry will start with the prefix ***PRISMA_DIRECT_IF:***

On the uniFLOW server the uniFLOW ***mom Tech Support Interface*** can be reached via the following URL:

http(s)://<uniFLOW_server>/pwserver/techsupport.asp You can choose between different logging levels. If required, you can export the log for support cases.

Note that the ***mom Technical Support Interface*** logs will automatically be deleted from the uniFLOW database after seven days.

Logging to a File

You should only enable this logging method in case of issues or when advised to do so by NT-ware. As this logging method logs all messages, it will grow very quickly. Furthermore, it is a very technical log that is only useful for uniFLOW experts.

In order to enable this logging method, set the following Windows registry key:

LEO_LogFilePath	
Key:	*HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom*
Value Name:	*LEO_LogFilePath*
Value Type:	*REG_SZ*
Value Data:	directory where the log file shall be created in Example: c:\

3.17.18 ODBC SQL Connection Test

The easiest way to test a connection to an SQL server from the uniFLOW server is via ODBC. In the absence of any other tools such as SQL Management Studio, oSQL or SQLCMD, ODBC is always available on a Windows Server.

The tool ODBC can be used to setup a basic connection to the SQL server, local or remote and test connectivity.

The test confirms the following:

- The SQL server is accessible from the uniFLOW server.
- The credentials used by uniFLOW to connect to the DB as defined in the connection string registry values are valid and working (pbaip and ufreader).
- Permissions to access the DsPcDb database using the above user credentials are confirmed.

ODBC Data Source Test Connection

1. Click on ***Windows > Start > Control Panel.***
2. Click on ***Administrative Tools.***
3. Double click on ***Data Sources (ODBC).***
4. Click the ***System DSN*** tab.
5. Click the ***Add...*** button.
6. Select ***SQL Server.***
7. Click the ***Finish*** button.
8. Enter a name and description for the test in the ***Name*** and ***Description*** field.
9. In the ***Server*** field, type the IP address of the computer where SQL Server (MSDE) is running.
10. Click the ***Next*** button.
11. Click the ***With SQL Server authentication using a login ID and password entered by the user.*** option.
12. Click the ***Client Configuration*** button.
13. Click ***TCP/IP*** option for the ***Network libraries.***
14. Make sure the ***Server alias*** and ***Server name*** fields have the IP address of your server.
15. Click the ***OK*** button.
16. Click the ***Connect to SQL server to obtain default settings for the additional configuration options.*** option.
17. Enter *pbaip* for the user name and *Ntw5qlPwd*. Alternatively you can test the connection with the user *ufreader* and the password *NtwR3adPwd*.
18. Click the ***Next*** button.
19. Click on ***Change the default database to:*** option.
20. Click the database drop down list and select ***DsPcDb.***
21. Click the ***Next*** button.
22. Click the ***Finish*** button.
23. Click the ***Test Data Source...*** button.

3.17.19 PBAIP-User Repair after Database Restoration

After "restore Database" you have to type the following statements in OSQL (MSDE) or Query Analyzer (SQL Server 2000/2005/2008):

Prior to uniFLOW V5.1

```
USE Master
GO
If not exists (select * from master.dbo.syslogins where loginname =
N'PbaIp')
BEGIN
	declare @logindb nvarchar(132), @loginlang nvarchar(132) select
@logindb = N'DsPcDb', @loginlang = N'us_english'
	if @logindb is null or not exists (select * from
master.dbo.sysdatabases where name = @logindb)
		select @logindb = N'master'
	if @loginlang is null or (not exists (select * from
master.dbo.syslanguages where name = @loginlang) and @loginlang <>
N'us_english')
		select @loginlang = @@language
	exec sp_addlogin N'PbaIp', N'Ntw5qlPwd', @logindb, @loginlang
END
GO
if not exists (select * from dbo.sysusers where name = N'PbaIp' and uid
< 16382)
	EXEC sp_grantdbaccess N'PbaIp', N'PbaIp'
GO
exec sp_addrolemember N'db_owner', N'PbaIp'
GO
USE dspcdb
GO
exec sp_change_users_login 'auto_fix',pbaip
GO
```

Since uniFLOW V5.1

1. Run the OSQL command **Prior uniFLOW V5.1** (see above) first.
2. Run the OSQL command **Since uniFLOW V5.1** (see below).

```
USE Master
GO
if not exists (select * from master.dbo.syslogins where loginname =
N'uFReader')
BEGIN
	declare @logindb nvarchar(132), @loginlang nvarchar(132) select
@logindb = N'DsPcDb', @loginlang = N'us_english'
```

```
	if @logindb is null or not exists (select * from
master.dbo.sysdatabases where name = @logindb)
		select @logindb = N'master'
	if @loginlang is null or (not exists (select * from
master.dbo.syslanguages where name = @loginlang) and @loginlang <>
N'us_english')
		select @loginlang = @@language
	exec sp_addlogin N'uFReader', N'NtwR3adPwd', @logindb, @loginlang
END
GO
if not exists (select * from dbo.sysusers where name = N'uFReader' and uid
< 16382)
	EXEC sp_grantdbaccess N'uFReader', N'uFReader'
GO
exec sp_addrolemember N'db_datareader', N'uFReader'
GO

USE dspcdb
GO

exec sp_change_users_login 'auto_fix',uFReader
GO
```

3.17.20 Poolmon Log Generation

Poolmon displays data that the operating system collects with regard to memory allocation from the system's paged and non-paged kernel pools and on the memory pools used for Terminal Services sessions. The data is grouped by pool allocation tag. This information can be used by NT-ware to find kernel mode memory leaks. A memory leak is caused by an application or by a process that allocates memory for use, but that does not free the memory when the application or process has finished. Therefore, available memory is completely used up over time. Frequently, this condition causes the system to stop functioning correctly.

1. Copy the Poolmon directory to your hard disk and alter the *poolmon.bat* file.
2. You will find a set timer=10800 value at the top of the file. Please change 10800 to a value NT-ware suggests. If the value has been set to 86400 for example, the Poolmon tool will run for 24 hours.
3. After saving the file, start the Poolmon tool using the *poolmon.exe* in your folder. Poolmon will create a memory snapshot every 60 minutes and will store the log files in your Poolmon folder.
4. As soon as the defined time period has elapsed, please copy the accumulated log files together into one file. To do so, open a command prompt and browse to the folder containing the *.txt* log files and type:
   copy file1.txt + file2.txt + file3.txt full.log
   Note that in this example you have 3 log files.
5. Afterwards, zip the *full.log* file and send it to NT-ware for further analysis.

Availability

Poolmon is available from a number of different sources.

- The Windows NT 4.0 Resource Kit
- The *\Support\Tools* folder of Windows 2000, Windows XP, and Windows Server 2003 CD-ROMs.
- Integrated into the MS Windows Driver Kit (WDK) as one tool out of many, downloadable here (http://www.microsoft.com/whdc/DevTools/WDK/default.mspx).
  The WDK works on Windows Server 2008, Server 2008 R2, Server 2003, XP, Vista, and Windows 7.

As a standalone tool, Poolmon only works on server operating systems like Windows 2000/2003.

3.17.21 Printer Export

Printers are exported either with the Print Migrator Tool or with the Print Migration Wizard. Both tools are provided by Microsoft. The differences between these tools are outlined in the table below.

Tool	Print Migrator 3.1	Printer Migration Wizard, Printbrm.exe command-line tool
Supported systems	Supports migration to **Windows Server 2003** from all previous Windows operating systems.	**Windows Vista** - Supports all migrations to Windows Vista. **Windows Server 2008 R2** - You cannot migrate directly from older operating systems (Windows NT Server 4.0, Windows 2000 Server) to Windows Server 2008 R2. Instead, you must migrate from the older operating system to a computer running Windows Vista, then migrate from Windows Vista to Windows Server 2008 R2.
Unsupported systems	Does not work with Windows Vista and later operating systems.	Does not support migrations from Windows 2000 Server and older systems.
Support for x64-Systems and drivers	**No.** 64-bit drivers or systems are not supported.	**Yes.** The Printer Migration Wizard is the only Microsoft-supported migration tool that works with 64-bit systems and drivers.
Availability	Available online. Print Migrator 3.1 was also shipped in resource kits for Windows 2000 Server and Windows Server 2003.	Available through the Print Management snap-in or through the command line by using Printbrm.exe on computers running Windows 7 Enterprise, Windows 7 Ultimate, and Windows Server 2008 R2.

3.17.21.1 Windows Server 2003 - Print Migrator Tool

The Microsoft Print Migrator automates the backup and restore of print configuration data on print servers running Microsoft Windows Server operating systems. The created .cab file can be used to recreate a customer's environment.

You can download the Microsoft Print Migrator Tool here (http://www.microsoft.com/WindowsServer2003/techinfo/overview/printmigrator3.1.mspx).

On this site you can also download a document that gives an elaborate description on how to use this tool.

3.17.21.2 Windows Server 2008 - Print Management

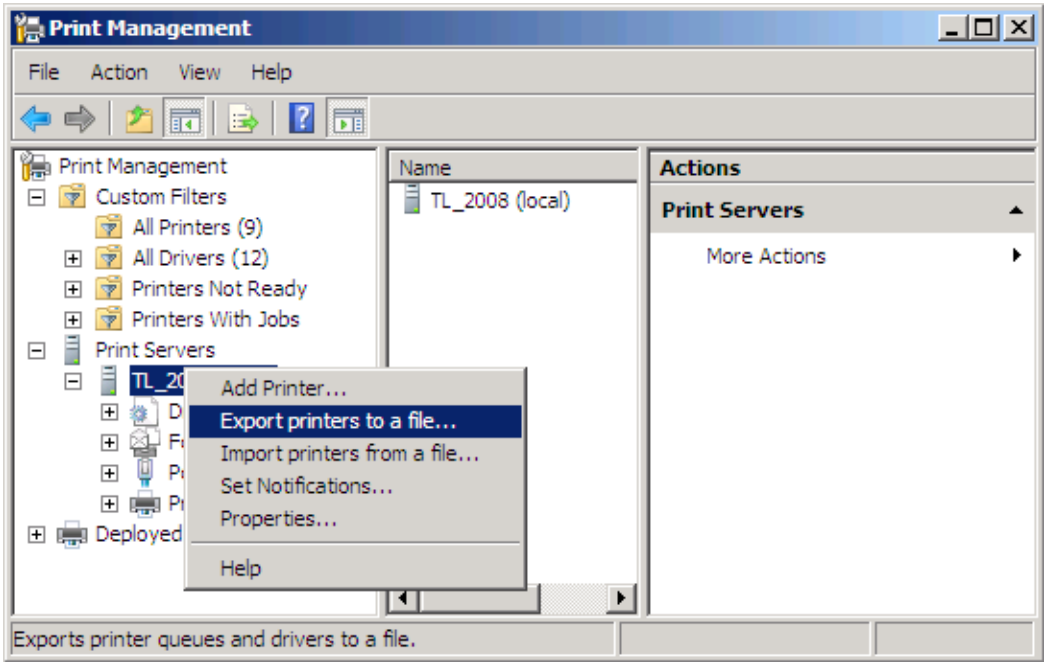
The Print Management console of the Windows Server 2008 provides an Export/Import interface to migrate printers to a different system. You can easily export the whole printer configuration into one single file. The **Printer Migration Wizard** then

exports the Print Queues, the Printer Drivers, the Print Processors and the Printer Ports.

The created *.printerExport* file can be used to recreate a customer's environment.

Export

- Open the ***Print Management*** console under ***Windows > Start > Administrative Tools.***
- Open the context menu of the desired Print Server and select ***Export printers to a file...***



Note that the Print Management console will be installed as part of the Print Services role. In case the print Management console is not yet available on your Windows Server 2008, you can install it by adding the role Print Services.

3.17.22 Problem Steps Recorder

Windows 7 and Windows Server 2008 R2 provide a ***Problem Steps Recorder***. This program is basically a tool to record screenshots every time the mouse is clicked. When stopped it creates a zipped MHTML document with all the screenshots inside. Use this tool to report certain problems that require screenshots.

You can start the ***Problem Steps Recorder*** by clicking on Windows ***Start*** and typing ***PSR*** or search for Problem Steps Recorder.

Please refer to the following links for more information.

- Microsoft Technet Description (http://blogs.technet.com/b/askperf/archive/2009/10/21/windows-7-windows-server-2008-r2-problem-steps-recorder.aspx)
- Microsoft Technet Video (http://technet.microsoft.com/en-us/windows/dd320286)

3.17.23 Process Monitor Tool Log Generation

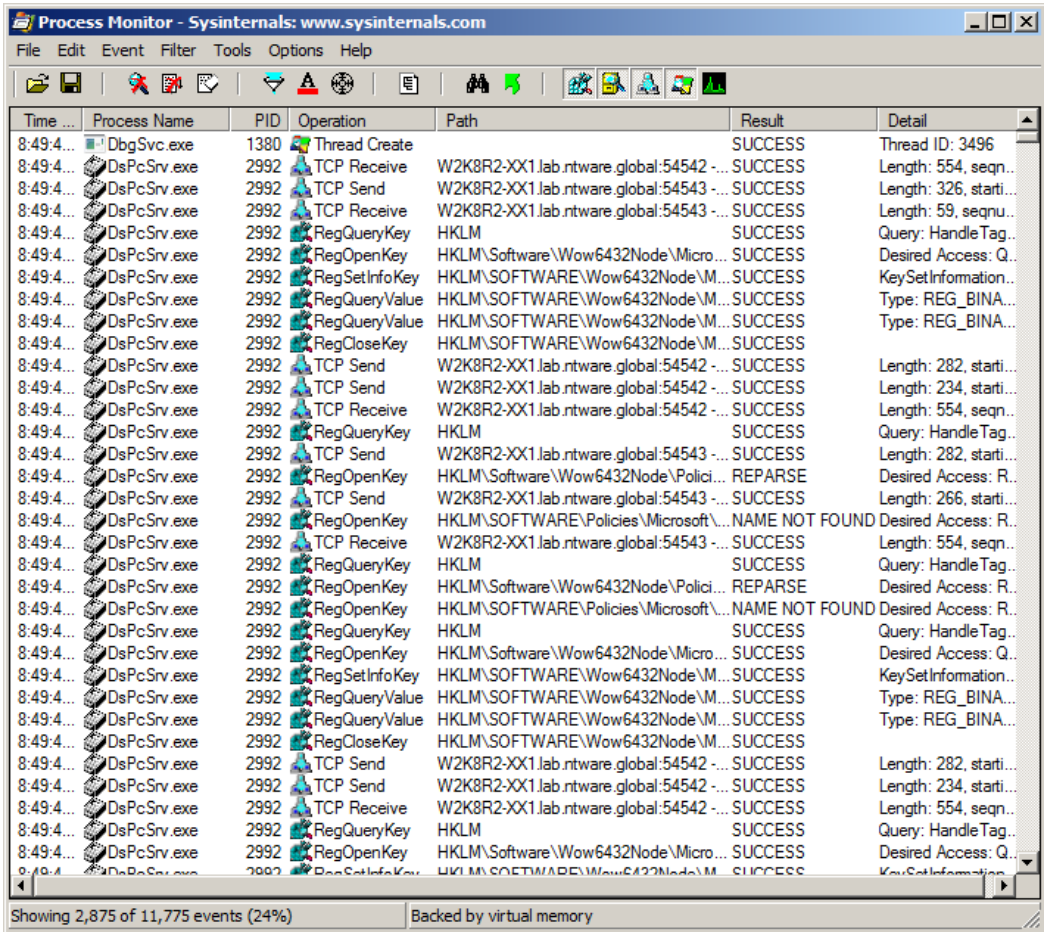
The free Process Monitor published by Microsoft is a real-time monitoring tool for file, Windows registry and process activities on a Windows system.

Click here (http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx) for download and further information like system requirements etc.

In a uniFLOW environment the logs created by Process Monitor can be used, among other things, to analyze file access problems, for instance, when a spool file is not/cannot be deleted after printing.

General View

After starting Process Monitor the program immediately begins capturing events. A list of process events is shown containing information like time, process name, path etc.



Main Control Elements

On the start screen you will find buttons for easy access to the main functions. For support purposes you will only need the following:

- File access: ***Open***/***Save***
- Capture controls
  - ***Capture***: Starts/Stops capturing.
  - ***Autoscroll***
  - ***Clear***: Clears current list.
- Filter options
  - ***Filter***: Create and manage filters.
- Activity Filters: These show or hide details concerning the following:
  - ***Registry***
  - ***File System***
  - ***Network***
  - ***Process and Thread***
  - ***Profiling events***

The functions listed above can also be used via the menus.

Useful Settings

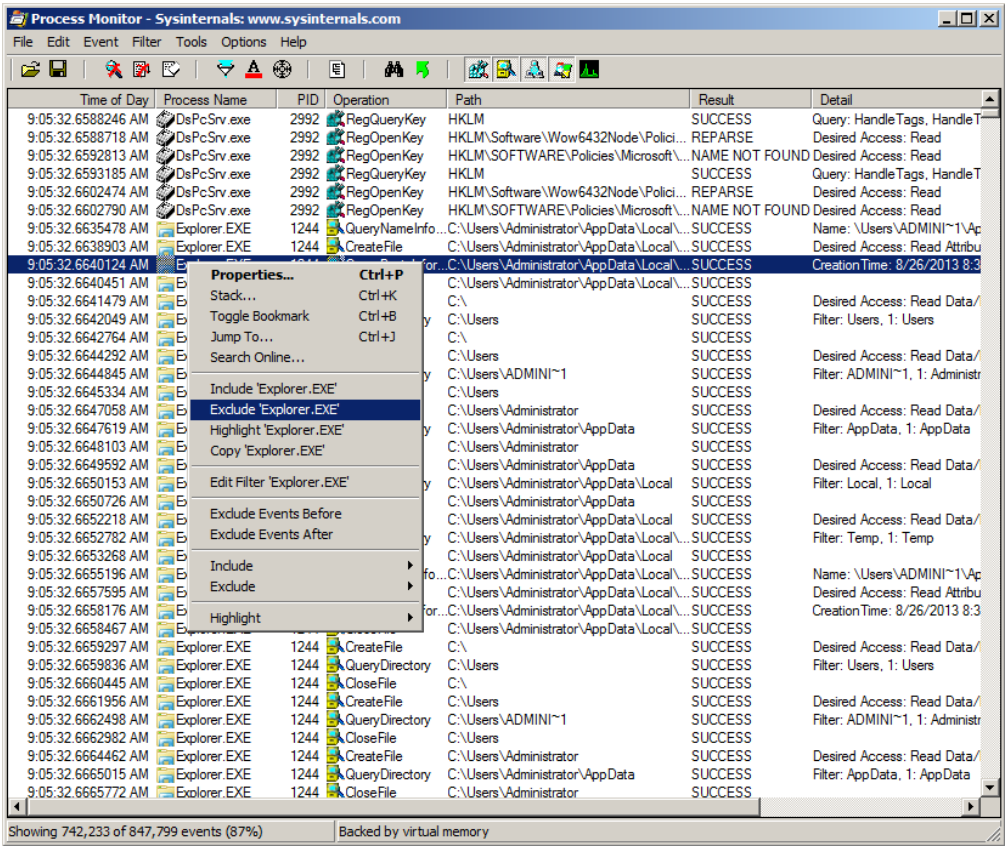
In order to allow effective analysis of problems, certain settings should be used.

- Activate ***Capture*** only when you want to start logging. Otherwise, the log files can get very large and cause problems.
- ***Autoscroll*** should be turned off, otherwise you can quickly loose overview.
- Under ***Filter***, check ***Drop Filtered Events***. This way, events that do not meet the filter criteria are not added to the log, resulting in a smaller log size.

Creating a Log

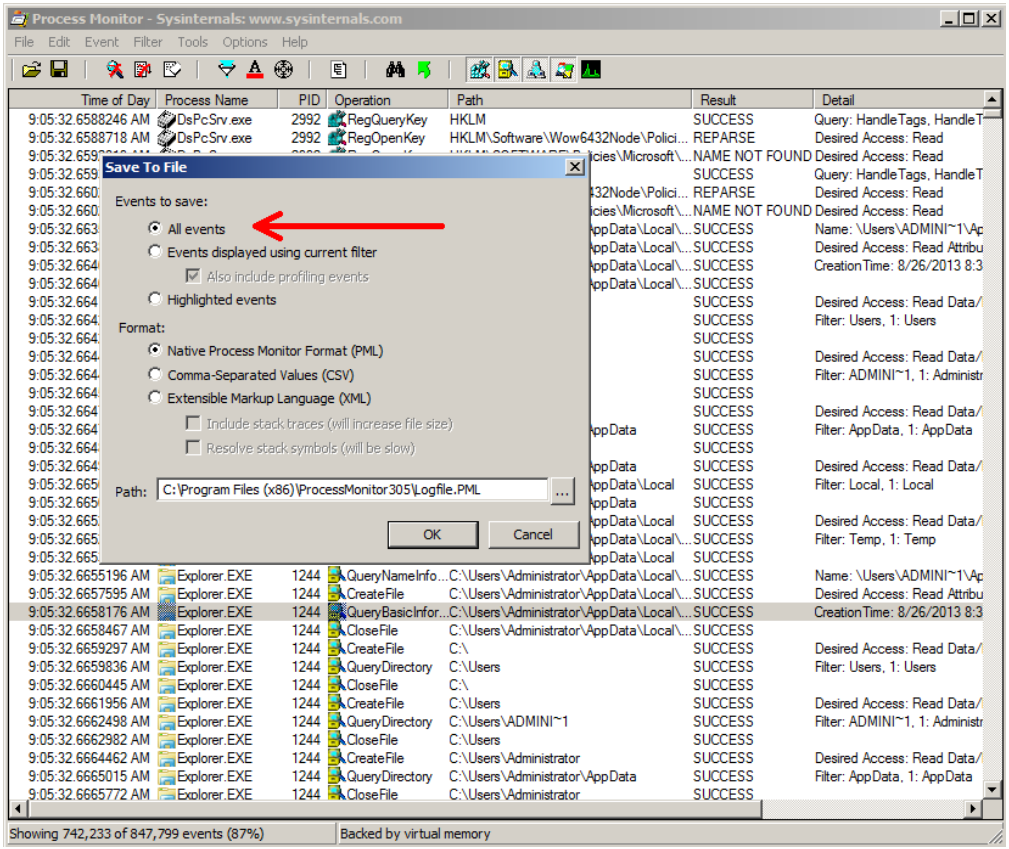
The filter options allow filtering for processes, paths and other event properties. Thus, it is easier to reproduce a problem and see if the relevant entries are captured in the log.

1. First you want to exclude all events/processes that are not involved in your problem, for instance *Explorer.EXE*. Right-Click on any instance of Explorer.EXE in the list. Click on the menu item ***Exclude 'Explorer.EXE'***. Now all entries of *Explorer.EXE* are hidden. Do this for all events/processes that are irrelevant to the problem.



2. You can add filters for paths. For instance, if you want to see events concerning the spool folder you would create a new filter with the following settings (depending on your operating system):
   Column: ***Path***
   Relation: ***contains***
   Value: *C:\Windows\System32\spool\PRINTERS*
   Action: ***Include***

3. Start capturing and try to reproduce the problem. For instance, if you have problems with spool jobs not being deleted you would print a new print job.
4. With the settings from above there should be entries for the spool folder that either show ***SUCCESS*** or an error message in the column ***Result***. In the case of undeleted spool files the error message could be ***ACCESS DENIED***.
5. If there was an error message indicating that you reproduced the problem stop capturing and open the ***Save*** dialog. Select the radio button ***All events*** and save the log file to your file system. That way all filters are turned off for saving and the supporters can analyze the complete list of events.



6. If there was no error message, stop capturing and clear the list. Then, restart capturing and try to reproduce your problem. Repeat these steps until you can reproduce the problem successfully.
7. After saving the log compress the file and send it to the NT-ware support

When you send data to NT-ware, please keep the following in mind.

- Keep the logs small. If you have an error that is not reproducible for each, try clear the list before trying again. That way the log does not contain unnecessary information.
- Send only unfiltered data to NT-ware. Select "All Events" in the file dialog when saving to a file. That way, the log file contains all data.

3.17.24 Windows Registry Hive (Registry Keys) Extraction

To create an extract of the NT-ware Windows registry entries:

1. Open the Windows registry.
2. Navigate to:
   - System Key on a 32-bit Operating System:
     HKEY_LOCAL_MACHINE\Software\NT-ware
   - System Key on a 64-bit Operating System:
     HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware
3. Right click on ***NT-ware*** and choose ***export***.

Example

In the following you see a Windows registry export from a Windows Server 2008 of a standard uniFLOW V5.0.5 installation with an installed and activated uniFLOW Scan Processing Server.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware]
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\LicenseManager]
"2-E163V-PEO4A-D2C50-39UF0-B2U2H"="3-742YG-X47AG-KM5NQ-CGT2G-0JP1M 1.0
953580 0000 00 00"
"0-2EUQX-L2OZ0-3D15T-PRS3N-HM1VA"="3-1M2P8-I2HQG-KOETV-CG32N-D3DN2
5.0.5 534388 0000 00 00"
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom]
"ARCHPREVIEWFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\WebAnon\\PdfArch\\"
"ARCHPRINTFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\PrintArchive\\"
"CLIENTPDFFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\WebAnon\\Pdf\\"
"CONNECTIONSTRING"="Provider=SQLOLEDB.1;Persist Security Info=True;User
ID=pbaip;Password=Ntw5qlPwd;Initial Catalog=DsPcDb;Data
Source=(local);Use Procedure for Prepare=1;Auto Translate=True;Packet
Size=4096"
"DATAFOLDER"="C:\\Program Files\\Common Files\\NT-ware Shared\\Data\\"
"DIFPATH"="C:\\Program Files\\Common Files\\NT-ware Shared\\Dif\\"
"DRQMSPOOLERPATH"="C:\\Program Files\\uniFLOW\\DRQMSpool\\"
"IGDATAFILEPATH"="C:\\Program Files\\Common Files\\NT-ware
Shared\\IGData\\"
"IGV2PORTDRIVERMSIPATH"="C:\\Program
Files\\uniFLOW\\IgV2PortDriverMsi.Exe"
"JAWSENGINEPATH"="C:\\Program Files\\Common Files\\NT-ware Shared\\"
"JTPROFILEFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\JtProfiles\\"
"LDAPPROFILEFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\LdapProfiles\\"
"MINDFWPKGDIR"="C:\\Program Files\\uniFLOW\\MindFw\\"
"MOMCLNTMSIPATH"="C:\\Program Files\\uniFLOW\\MomClntMsi.Exe"
"MOMISSPATH"="C:\\Program Files\\Common Files\\NT-ware
Shared\\MomISS.exe"
```

```
"MOMJTXPATH"="C:\\Program
Files\\uniFLOW\\WebClient\\jobevents\\jobtickets\\MOMJTX\\"
"PCLXLENGINEPATH"="C:\\Program Files\\Common Files\\NT-ware Shared\\"
"PDFFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\WebAuth\\Pdf\\"
"POSJTCONFIGFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\PosJtConfigs\\"
"POSPATH"="C:\\Program Files\\Common Files\\NT-ware Shared\\POS.EXE"
"REPORTSERVERPATH"="C:\\Program Files\\Common Files\\NT-ware
Shared\\MomRptServer.Exe"
"SCRIPTFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\Scripts\\"
"SHAREDWEBANON"="C:\\Program Files\\Common Files\\NT-ware
Shared\\WebAnon\\"
"SPLOTPROXY"="C:\\Program Files\\Common Files\\NT-ware
Shared\\MomxPlot.exe"
"VERSION"="Suite"
"WEBCLIENTPATH"="C:\\Program Files\\uniFLOW\\WebClient\\"
"WEBQUEUEMANPATH"="C:\\Program Files\\uniFLOW\\WebQueueMan\\"
"WEBSERVERPATH"="C:\\Program Files\\uniFLOW\\WebServer\\"
"XPDLIBFOLDER"="C:\\Program Files\\Common Files\\NT-ware
Shared\\XPDLIB\\"
"ProductFamily"=dword:00000001
"MomLanguage"="EN"
"CountryCode"="GB"
"FoundSpoolFolder"="C:\\Windows\\system32\\spool\\PRINTERS\\"
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\DemoLicSet]
"LicenseInfo"=hex:
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\DeviceAgents]
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\DeviceAgents\CpCaLogReader]
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\DeviceAgents\CpCaLogReader\Ti
meStamps]
"{10B30457-1B72-4D2E-813D-B45B74680FFE}-1"=hex:80,a9,86,75,f7,0f,cc,01
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\Icarus]
"ICARUSPATH"="C:\\Program Files\\uniFLOW\\WebClient\\Icarus\\"
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomAdmSvc]
"HTMLRESOURCEFILES"="C:\\Program Files\\Common Files\\NT-ware
Shared\\MomAdmSvc\\"
"AccessMask"=hex(7):00,00
"HttpPort"=dword:0000c1ac
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomAdmSvc\ServiceMonitor]
"IgnoreDependencies"=dword:00000000
"MaxPercentalMemoryIncrease"=dword:0000000a
"WatchMemoryUsage"=dword:00000001
"CrashProtectServices"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomAdmSvc\ServiceMonitor\Main
tenanceRestart]
"ExecutionMonthWeekDay"=dword:00000001
"ExecutionMonthWeekNumber"=dword:00000001
"ExecutionDayOfMonth"=dword:00000001
"ExecutionMonthInterval"=dword:00000000
"ExecutionMonthMask"=dword:00ffffff
"ExecutionWeekInterval"=dword:00000001
```

```
"ExecutionDayMask"=dword:00000040
"ExecutionDayInterval"=dword:00000001
"ExecutionEnd"=hex:00,00,00,00,00,00,00,00
"ExecutionBegin"=hex:00,78,ba,4a,04,54,bf,01
"RepeatInterval"=dword:00000002
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomAdmSvc\ServiceMonitor\Memo
ryRestart]
"ExecutionMonthWeekDay"=dword:00000001
"ExecutionMonthWeekNumber"=dword:00000001
"ExecutionDayOfMonth"=dword:00000001
"ExecutionMonthInterval"=dword:00000000
"ExecutionMonthMask"=dword:00ffffff
"ExecutionWeekInterval"=dword:00000001
"ExecutionDayMask"=dword:000000ff
"ExecutionDayInterval"=dword:00000001
"ExecutionEnd"=hex:00,00,00,00,00,00,00,00
"ExecutionBegin"=hex:00,78,ba,4a,04,54,bf,01
"RepeatInterval"=dword:00000002
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomSpaceSuit]
"LoggerDest"=hex(7):46,00,69,00,6c,00,65,00,00,00,00,00
"HttpPort"=dword:00001f41
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomSpaceSuit\Logger]
"LogFile"="C:\\Program Files\\uniFLOW Scan Processing
Server\\Log\\MomSpaceSuit.log"
"LoggingLevel"=dword:00000002
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomSpRec]
"UPLOADPATH"="C:\\Program Files\\Common Files\\NT-ware
Shared\\PrintArchive\\"
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomTcpServer]
"HttpPort"=dword:00001f40
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\MomUpload]
"UPLOADPATH"="C:\\Program Files\\Common Files\\NT-ware
Shared\\WebAuth\\Upload\\"
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\PrintManager]
"LOCALACTIVEJOBSPATH"="C:\\Program Files\\Common Files\\NT-ware
Shared\\ActiveJobs\\"
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\PrintProcs]
"CANON IR C4080/C4580 PCL6"="WinPrint"
"CANON IR-ADV C5045/5051 PS3"="WinPrint"
"CANON IR-ADV C7055/7065 PS3"="WinPrint"
"CANON IR-ADV C9060/9070 PS3"="WinPrint"
"CANON IR5075 PS3"="WinPrint"
"MICROSOFT XPS DOCUMENT WRITER"="WinPrint"
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\uniFLOW]
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\uniFLOW\1.00.000]
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\uniFLOW Scan Processing Server]
[HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\uniFLOW Scan Processing
Server\1.00.0000]
```

3.17.25 RPS dump.htm Activation

The dump.htm enables one to check the configuration file of the RPS. The dump.htm makes the information contained in the Objectsspace.dat available in clear text. The availability of the dump.htm page is controlled by a Windows registry key that will be checked each time the page is requested, so no restart will be necessary.

The URL of the dump.htm is the following:

http://<uniflowRPSserver>:8000/dump.htm

Windows Registry Settings

EnableDump	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom\MomAps* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomAps*
Value Name:	*EnableDump*
Value Type:	*REG_DWORD*
Value Data:	e.g. *1*

If set to 0 (default) no dump is possible. Set this key to 1 to enable the dump page, no restart necessary.

To enable the dump, type "dump.htm" behind the address of the RPS.

3.17.26 RPS Logging

RPS V4.0 or Lower

The RPS logs for versions up to V4.0 are saved as text files on the RPS in the following folder *…\Program Files\uniFLOW Remote Print Server\Data*. Here you will find the file: *MomAps.log*.

Windows Registry Settings

LOGGINGLEVEL	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom\MomAps\SystemLogger* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomAps\SystemLogger*
Value Name:	*LOGGINGLEVEL*
Value Type:	*REG_DWORD*
Value Data:	e.g. *0*

This key is active after a service restart. Set to 0 (FLOW) it will ensure an extended logging on the RPS.

Afterwards, you can set it back to its standard value 2 (ERROR).

RPS V4.1 or Higher

From V4.1 the logs can be accessed through the RPS Techsupport page, see chapter RPS (on page 100).

3.17.27 RPS SQL Query Website Activation

The website is now available at http://localhost:8000/sqlquery.htm and can be used to drop SQL statements on the newly introduced RPS SQL Lite database.

Note that for security reasons only ***SELECT*** commands are possible.

Windows Registry Settings

EnableSqlQuery	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom\MomAps* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomAps*
Value Name:	*EnableSqlQuery*
Value Type:	*REG_DWORD*
Value Data:	*1*

Set this value to 1 to enable the *SQLquery.htm* website.

To disable this website, please set the value to 0 or delete the key.

This is only available with uniFLOW V4.1 or higher and does not require a restart of the services.

3.17.28 Scan Processing Server Log Activation

To generate a Scan Processing Server log (MOMSpaceSuit) please proceed as follows:

Windows Registry Key

LoggingLevel	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom\MomSpaceSuit\Logger* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomSpaceSuit\Logger*
Value Name:	*LoggingLevel*
Value Type:	*REG_DWORD*
Value Data:	*0* (default *2* = Error)

The log file will be saved under:

C:\Program Files\uniFLOW Scan Processing Server\Log

The following URL shows the current number of processing files in the IRIS (MomSpaceSuit) engine.

http://localhost:8001/ufwkp/status.htm

The Scan Processing Server has to be restarted after changing the Windows registry key.

3.17.29 SiteAudit Logging

To enable the logging for SiteAudit on the uniFLOW server, set the Windows registry key listed below.

It logs information about the SiteAudit readout and the communication with the devices. Note that the log file will not be deleted automatically nor overwritten. Please use it only for the debugging period.

LogFilePath	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom\MomSiteAudit* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomSiteAudit*
Value Name:	*Ignore No PF*
Value Type:	*REG_SZ*
Value Data:	*C:\logs\siteaudit.log (EXAMPLE)*

3.17.30 SMTP Log

To add the ability to log SMTP communication on the uniFLOW/RPS server the following key needs to be added.

Windows Registry Settings

SmtpLogFileName	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom*
Value Name:	*SmtpLogFileName*
Value Type:	*REG_SZ*
Value Data:	*c:\UF_logging\smtp.log* (example)

The "SYSTEM" user needs write permissions on this folder. If the value is empty or does not exist no SMTP logging will proceed.

Changed settings require a restart of the uniFLOW services.

Please keep in mind that you need to delete this key after the logging has been done.

3.17.31 Special Characters in Usernames and Passwords

In uniFLOW there are a number of different areas where user names and passwords can be entered/stored. These are, for example, identities, network folder user names and passwords, certain Device Agent configurations, SMTP Server connections etc.

In general there is no limitation to the character sets that can be used for either user names or passwords, all is UNICODE and everything can be stored.

There are however different areas in the software, for example certain Device Agent configurations, where the current user interface (uniFLOW V5.1.x and older) uses a separator ('$') to separate arguments. There may be other areas in the software using different separators.

So in the instance where a user name / password combination is failing, a good troubleshooting step would be to ensure there are no uniFLOW reserved characters contained within:

{}$%;, etc.

3.17.32 Spool File Capturing

- If you want to capture spool files, the most convenient way to do this is to insert the Workflow Element Backup Spool file in the workflow of the printer in question in uniFLOW.
- In the ***Advanced Configuration*** of this Workflow Element you can choose whether the spool file should be deleted after print or not and you can enter the path for the backup folder.
- Files are saved as .bak.

The spool folder on a clustered system will be different to the folder mentioned in this chapter. Please check your cluster configuration to figure out which is the right spool folder.

3.17.33 SQL Express 2005 Network Access Activation

SQL 2005 Express works just fine with uniFLOW. Management tools installed on the same server can administer SQL 2005 Express just fine. However, when you try to connect to SQL 2005 Express via the network, it could fail. Not even the Enterprise Manager can access the SQL 2005 EXPRESS via the network.

Starting with MSDE/SQL Server 2000 SP3, the installation default is to disable all network protocols for security reasons. By disabling the network protocols, the

MSDE/SQL Server will not answer any network requests, thus it is invulnerable to any network viruses, for instance SQL Slammer. When creating the uniFLOW setup scripts, we opted to maintain this high level of security, thus we disabled the network protocols on the SQL 2005 Express. This means, however, that you cannot maintain or administer the SQL 2005 Express remotely.

You can re-enable the network support in the SQL 2005 Express by using the SQL Server Configuration Manager Utility. The steps below describe how this is done.

1. Open the start menu and navigate to ***Programs > Microsoft SQL Server 2005 > Configuration Tools***.
2. Click on ***SQL Server Configuration Manager***.
3. On this tool, please select ***SQL Server Network Configuration***, then select ***Protocols for MSSQLSERVER***.
4. On the right, choose ***TCP/IP*** and right click.
5. Now you can enable TCP/IP access for the SQL 2005 Express, which will be activated after a restart of the service.
6. Restart services by using the uniFLOW Admin services web site. Open a web browser and type the following address: http://uniFLOW_Server_IP:49580
7. Click on stop for SQL Server (MSSQLSERVER). All the services will stop except the Print Spooler. After a successful stop of services you can restart all the services by clicking on Start for the uniFLOW server.

Now SQL 2005 Express should be accessible from the network.

Enabling the SQL 2005 Express network protocols makes it vulnerable to network attacks - therefore, we suggest disabling network support after you have finished with maintenance.

3.17.34 SQL Profiler Database Monitoring

Microsoft SQL Server Profiler is a graphical user interface to SQL Trace for monitoring an instance of the Database Engine or Analysis Services. You can capture and save data on each event to a file or table for later analysis. For example, you can monitor a production environment to see which of the stored procedures affect performance by executing too slowly.

SQL Server Profiler shows how SQL Server resolves queries internally. This allows administrators to see exactly what Transact-SQL statements or Multi-Dimensional Expressions are submitted to the server and how the server accesses the database or cube to return result sets.

Using SQL Server Profiler, you can do the following:

1. Create a trace that is based on a reusable template.
2. Watch the trace results as the trace runs.
3. Store the trace results in a table.
4. Start, stop, pause and modify the trace results as necessary.

5. Replay the trace results.

Use SQL Server Profiler to monitor only the events in which you are interested. If traces become too large, you can filter them based on the information you want, so that only a subset of the event data is collected. Monitoring too many events adds overhead to the server and the monitoring process and can cause the trace file or trace table to grow very large, especially when the monitoring process takes place over a long period of time.

The Microsoft SQL Server Profiler is available with:

- SQL Server 2005 Standard Edition
- SQL Server 2005 Enterprise Edition
- SQL Server 2008 Datacenter Edition
- SQL Server 2008 Enterprise Edition
- SQL Server 2008 Standard Edition
- SQL Server 2008 Web Edition
- SQL Server 2008 Workgroup Edition

Please refer to the following Microsoft article to learn more about the SQL Server Profiler (http://msdn.microsoft.com/en-us/library/ms181091.aspx).

3.17.35 Statistics Problem Check

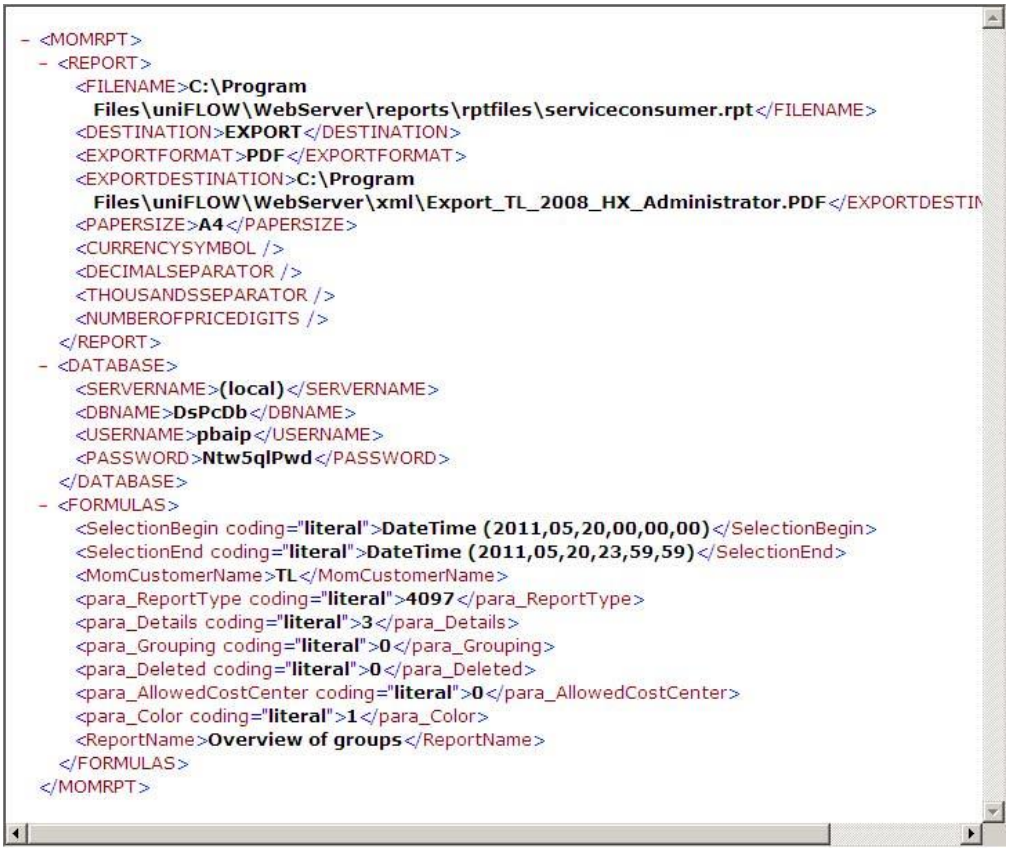
If you encounter problems creating statistics or reports in uniFLOW, please follow the steps described here to gather further information about the problem.

If you create a statistic in uniFLOW, uniFLOW creates an XML file in background containing all selected settings. The *MomRptServer.exe* will then be started with this XML file to create the final statistic in PDF, XLS or RTF format.

If a statistic is not created, you can check the following:

1. Create the desired statistic in uniFLOW.
2. Open the folder:
   C:\Program Files\uniFLOW\WebServer\xml

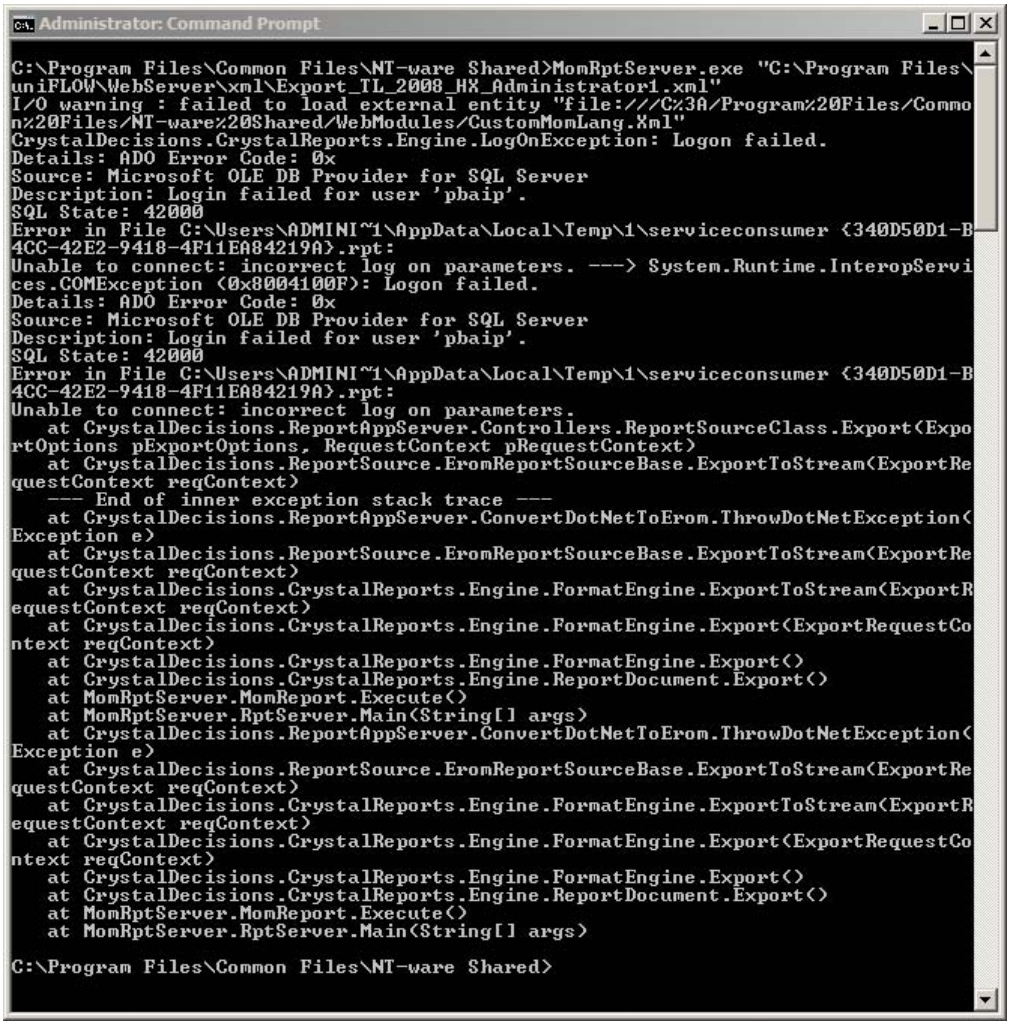
3. In general, you will find an XML file and the created statistics PDF/XLS/RTF in this folder.
   The XML file contains information about the export format, the export folder, the paper size, details about the database connection etc.



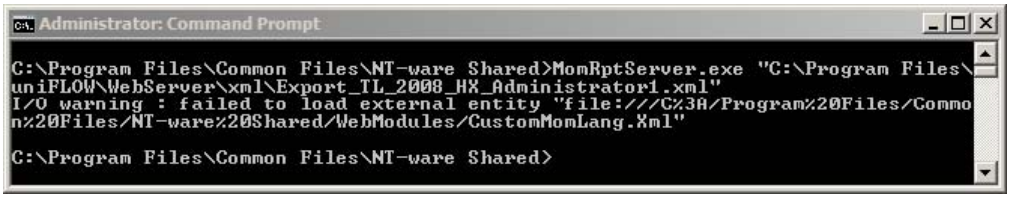
```
- <MOMRPT>
  - <REPORT>
      <FILENAME>C:\Program
        Files\uniFLOW\WebServer\reports\rptfiles\serviceconsumer.rpt</FILENAME>
      <DESTINATION>EXPORT</DESTINATION>
      <EXPORTFORMAT>PDF</EXPORTFORMAT>
      <EXPORTDESTINATION>C:\Program
        Files\uniFLOW\WebServer\xml\Export_TL_2008_HX_Administrator.PDF</EXPORTDESTIN
      <PAPERSIZE>A4</PAPERSIZE>
      <CURRENCYSYMBOL />
      <DECIMALSEPARATOR />
      <THOUSANDSSEPARATOR />
      <NUMBEROFPRICEDIGITS />
    </REPORT>
  - <DATABASE>
      <SERVERNAME>(local)</SERVERNAME>
      <DBNAME>DsPcDb</DBNAME>
      <USERNAME>pbaip</USERNAME>
      <PASSWORD>Ntw5qlPwd</PASSWORD>
    </DATABASE>
  - <FORMULAS>
      <SelectionBegin coding="literal">DateTime (2011,05,20,00,00,00)</SelectionBegin>
      <SelectionEnd coding="literal">DateTime (2011,05,20,23,59,59)</SelectionEnd>
      <MomCustomerName>TL</MomCustomerName>
      <para_ReportType coding="literal">4097</para_ReportType>
      <para_Details coding="literal">3</para_Details>
      <para_Grouping coding="literal">0</para_Grouping>
      <para_Deleted coding="literal">0</para_Deleted>
      <para_AllowedCostCenter coding="literal">0</para_AllowedCostCenter>
      <para_Color coding="literal">1</para_Color>
      <ReportName>Overview of groups</ReportName>
    </FORMULAS>
  </MOMRPT>
```

4. In the event that there is only an XML file in the folder, the PDF/XLS/RTF could not be created for some reason.
5. To check why this happened and to get some more information about this error, you can start the creation of the statistic manually by using this XML file.
6. To do so, open a command prompt and change to the folder:
   C:\Program Files\Common files\NT-ware Shared
7. Run the *MomRptServer.exe* with the XML file.

8. The next screenshot gives an example of a failed statistic creation. If you check the messages in the example screenshot, you can see that the logon failed. This means that the password for user pbaip of the database is wrong.



9. The next screenshot is an example of a working statistic creation. The I/O warning is not a problem, as it appears in the event that a *CustomMomLang.xml* should be used and is in place. In a standard installation you can simply ignore this message as it does not cause any problems.



3.17.36 System Image Creation

The "VMware Converter" Tool can be downloaded from the VM-ware website. This VMware Converter enables the creation of a VM-ware image of the complete system.

- Simply execute the VMware Converter and follow the steps of the wizard.

3.17.37 Telnet Logging

In some cases it is necessary to generate a Telnet log. This can be achieved with the standard Windows Telnet client or with the more versatile Putty software.

To use Telnet, you first should ensure that the Telnet Client is installed on your computer. On a Windows Server 2008 (R2) you can add it as a feature if not yet installed.

Installing Putty

1. Please download the file *putty-0.60-installer.exe* (or newer).
2. Run *putty-0.60-installer.exe.*
3. Click on Next.
4. Select ***Additional tasks***, then click on ***Next*** (options selected by default are OK).
5. Click on ***Next***.
6. After completion, click on ***Finish***.

Now Putty is ready for usage.

3.17.37.1 Telnet Log Generation for MIND / LM / SSP / microMIND V2

The Telnet log can be used in situations where communication with the MIND box, LM, SPP or microMIND V2 needs to be analyzed. To generate a Telnet log please proceed as follows:

Putty

1. Run Putty from the program list on the start menu.
2. On the session tab, enter the device IP address and the port number (see below).
3. Then, on Connection type, choose ***RAW***.
4. Navigate to the Logging tab, and select All session output on Session logging options.
5. Choose a log file name and click on ***Browse*** to choose a path for the log file.
6. Navigate back to the Session tab and click on ***Open*** in the bottom. The telnet session will open.
7. To stop the logging, click on the cross at the top right hand corner of the telnet window.
8. The file will automatically be created on the given path.

Use the following Ports:

SPP: 53213

LM: 53214

Mind: IP and the default port (23)

microMIND V2: 53215

For microMIND V2 use the following login data:

Username: ntware

Password: dwarf

Possible Error Messages

- ***IDRESULT_KNOWN 0***:
  User/ID is known.
- ***IDRESULT_OK 0***:
  User/ID is known.
- ***IDRESULT_FAILURE 1***:
  General failure.
- ***IDRESULT_UNKNOWN 2***:
  User/ID is unknown.
- ***IDRESULT_BLOCKED 3***:
  User is known but access is blocked for instance because his budget has expired.
- ***IDRESULT_DEVICEOFFLINE 4***:
  User is known and would have access, but the status control shows that the device is offline, therefore no login is possible.
- ***IDRESULT_SERVERBUSY 5***:
  Server is currently busy (most likely because of a CPCA read out) so logon is temporarily not possible.

Telnet

1. To use Telnet open a command prompt in Windows.
2. Type: *telnet <IP-address> <Port>*
3. Type *HELP* and confirm with enter to view a list of supported commands.

You could start Telnet session with logging from the command window with the following line:

telnet 192.168.110.100 53213 -f C:\Logs\TelnetFile.txt

3.17.38 Troubleshooting Device Connection Issues with GetIPInfo.js

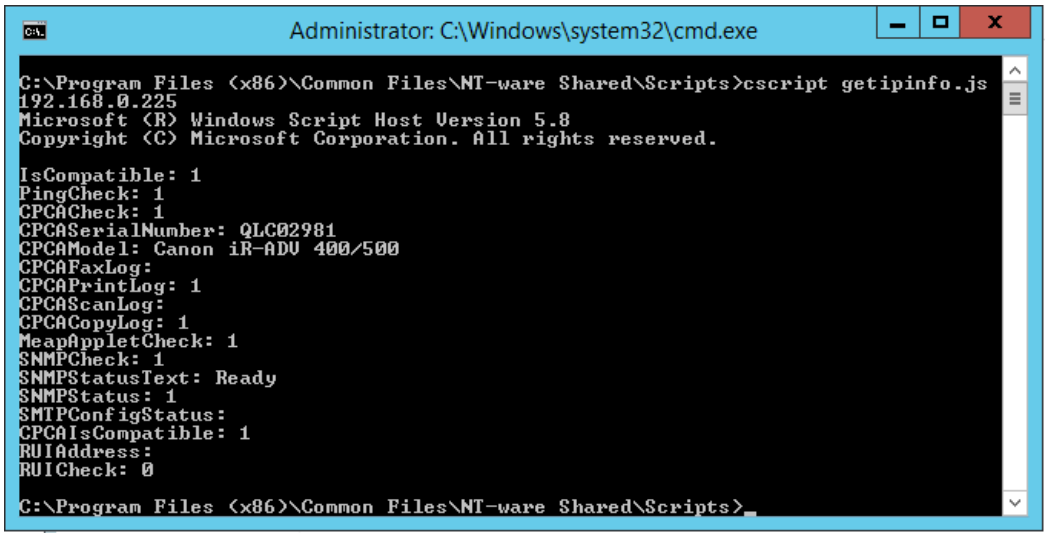
The *getipinfo.js* script is a useful tool in troubleshooting device connection issues.

The script is shipped with uniFLOW and located in *C:\Program Files (x86\Common Files\NT-ware Shared\Scripts*.

It is run on the uniFLOW server using he following command syntax:

cscript getipinfo.js <device ip>

The output looks as follows:



- ***IsCompatible:***
  Confirms a DIF is available for this device.
- ***PingCheck:***
  Confirms the device is reachable in the network via PING.
- ***CPCACheck:***
  Confirms the device is a CPCA device.
- ***CPCASerialNumber:***
  Device serial retrieved via a CPCA call.
- ***CPCAModel:***
  Device model retrieved via CPCA call. This should match the model name in the corresponding DIF.
- ***CPCAFaxLog:***
  This log is accessible.
- ***CPCAPrintLog:***
  This log is accessible.
- ***CPCAScaLog:***
  This log is accessible.
- ***CPCACopyLog:***
  This log is accessible.
- ***MeapAppletCheck:***
  The MEAP applets are reachable.
- ***SNMPCheck:***
  SNMP is reachable.
- ***SNMPStatusText:***
  The current SNMP status text.
- ***SNMPStatus:***
  The current SNMP status value.
- ***SMTPConfigStatus:***
  Always shows an empty value as this check is no longer performed.

- ***CPCAIsCompatible:***
  Confirms a DIF is available for this device.
- ***RUIAddress:***
  Always shows an empty value as this check is no longer performed.
- ***RUICheck:***
  Always shows value 0 as this check is no longer performed.

3.17.39 uniFLOW Client for Windows Logging

Method 1 (Print Audit mode .ini file)

1. Edit the *momclnt.ini* file.
2. Add the following line: *LoggingEnabled=1*.
3. Restart the uniFLOW Client for Windows.
4. The log file will be created in *\%system_drive%\temp* (as *MomClient_username.txt*).

Method 2 (Via ApjPrint/MomPort)

Add the following regkey:

LoggingEnabled	
Key:	32-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Nt-ware\Mom\MomClient* 64-bit Operating System: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\NT-ware\Mom\MomClient*
Value Name:	*LoggingEnabled*
Value Type:	*REG_DWORD*
Value Data:	1

- Restart the uniFLOW Client for Windows
- The log file will be created in *\%system_drive%\temp* (as MomClient_username.txt)

Note to disable the logging after troubleshooting.

3.17.40 uniFLOW Service for Google Cloud Print Logging

The uniFLOW Print Service for Google Cloud Print (CloudPrintSvc) logs informational and error messages into a log file.

In order to diagnose any problem, it is best to set the registry key *LogLevel* to value 1 or 2. This causes the service to log more information in a log file placed in the installation folder. The value data of the *LogLevel* registry key defines the depth of log information required.

The log file is named *CloudPrintSvc.log* and can be found in the same location as the service executable.

A service restart of the uniFLOW Service for Google Cloud Print is required to apply the change.

LogLevel	
Key:	32-bit system: *HKEY_LOCAL_MACHINE\Software\Nt-ware\CloudPrintSvc* 64-bit system: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\Nt-ware\CloudPrintSvc*
Value Name:	*LogLevel*
Value Type:	*REG_DWORD*
Value Data:	• *0*: Means normal service information. Should be default and used whenever the service is running normally. • *1*: Should be used to log any errors that might occur. • *2*: Log messages important for development analysis. Should be set only when really required. Otherwise it might produce big log files unnecessary. The service will trace the response messages from the Cloud Print endpoints into a log file named *CloudPrintSvc.log*. The logging information related with the XMPP connection is written into a separate log file named *jingle.log* (naming comes from the libjingle open source library which is used to connect to the XMPP Google Talk server).

Other Debugging & Support Measures

The uniFLOW Print Service for Google Cloud Print first tries to connect to the XMPP server on port 5222 with auto-detected proxy settings. If the connection fails, it will try to connect to the fallback port 443 with auto-detected proxy settings. This behavior is built into the service, but can also be influenced from within the registry when required from the support team.

AutoDetectProxy	
Key:	32-bit system: *HKEY_LOCAL_MACHINE\Software\Nt-ware\CloudPrintSvc* 64-bit system: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\Nt-ware\CloudPrintSvc*
Value Name:	*AutoDetectProxy*
Value Type:	*REG_DWORD*
Value Data:	• *0:* Disables proxy server detection. • *1:* Enables proxy server detection.

UseFallbackPort	
Key:	32-bit system: *HKEY_LOCAL_MACHINE\Software\Nt-ware\CloudPrintSvc* 64-bit system: *HKEY_LOCAL_MACHINE\Software\Wow6432Node\Nt-ware\CloudPrintSvc*
Value Name:	*UseFallbackPort*
Value Type:	*REG_DWORD*
Value Data:	• *0:* Uses the standard XMPP port 5222 first. • *1:* The service will first connect to the fallback port 443.

These keys are not created by the service. They have to be created manually.

3.17.41 uniFLOW SmartClient Logging

In ***Server Configuration > General Settings > uniFLOW SmartClient*** you can configure the general settings and logging settings for the uniFLOW SmartClient network.

- ***Maximum age of peer cache (days)*** (default: 0)***:***
  Entering a value does only make sense in case the device(s) / uniFLOW SmartClient(s) are continuously online.
- ***Logging Level:***
  The uniFLOW SmartClient(s) will receive the information which logging level has been set and only upload entries of the selected logging level.

- ***None*** (default)
- ***Errors***
- ***Critical:***
  Only critical errors will be logged.
- ***Flow***

The logging level ***Flow*** will result in a large amount of data. Please observe to set the ***Maximum log file size*** to an appropriate value. The Logging Level ***Flow*** should only be used for short periods of time for diagnostic purposes!

- ***Log Directory:***
  If a ***Logging Level*** is enabled, enter the path to the Log Directory in this field.
  There are three possibilities for the destination folder of the log file, listed according to their priority:
  - Windows registry entry:
    HKEY_LOCAL_MACHINE\SOFTWARE\NT-ware\Mom\SmartClientLogPath
    If set, this setting has the highest priority. It is useful for overwriting the Global Config setting of the uniFLOW Server, in case the path does not exist on the RPS file system. It expects an absolute path.
  - The Global Config Log Directory:
    If no Windows registry path is configured, then this log directory will be used. It expects an absolute path.
  - If none of the above two is set, than the path: *%DataFolder%\SmartClient\Logs* will be used.
- ***Log Type:***
  - ***Separate File for each peer*** (default)
  - ***Common file for a peer group***
- ***Maximum log file size (KB)*** (default: 0)***:***
  The default is 0, as by default logging is not enabled. In case you want to enable logging, specify a maximum file size in KB here. As a result, the logging file will never exceed the entered size. Once the log file has reached this limit, with every new entry the oldest entry in the log is deleted.
- ***Number of days to keep log*** (default: 0)

Local Logs

- Local logs on the uniFLOW SmartClient PCs are enabled if the Windows registry key ***LoggingEnabled*** is set to ***1*** on the uniFLOW SmartClient PC. For this purpose proceed as follows:
  - On the uniFLOW SmartClient PC open the Windows registry.
  - Go to *HKLM\SOFTWARE\NT-ware\Mom\MomSmartClient.*
  - Create a ***REG_DWORD*** item called *LoggingEnabled* and set it to *0x00000001 (1)*.
  - Restart the uniFLOW SmartClient.
  - In folder *%APDATA%\NT-ware\SmartClient\DATA*
    a logfile momsmartclnt_[machinename]_YYYY-MM-DD_HHMISS.log will be

created.

Example:

In Windows 7, for the *Administrator* user this would for instance be the folder *C:\Users\Administrator\AppData\Roaming\NT-ware\SmartClient\DATA*

- The uniFLOW SmartClient's local log is restricted to 10 MB and 10 days by default. This can be changed in the Windows registry with the Windows registry keys:
  32-bit system:
  `HKEY_LOCAL_MACHINE\Software\NT-ware\Mom\MomSmartClient`
  `DaysToKeepLog` (DWORD) – number of days to keep log
  `MaxLogFileSize` (DWORD) – size in KB
  The log file is located in *%APPDATA%\NT-ware\Smartclient\DATA.*

3.17.42 uniFLOW Snapshot Creation

The uniFLOW SnapShot Tool is included with each uniFLOW installation. With the uniFLOW SnapShot Tool you can create a backup of your uniFLOW installation. With this backup and the corresponding uniFLOW version it is possible to restore a uniFLOW installation. The uniFLOW SnapShot Tool saves the changed uniFLOW files, Windows registry entries and database tables to the hard disk and also runs the Microsoft Print Migration Tool to create a backup of all system printers.

The use of the SnapShot Tool is explained in greater detail in the chapter ***SUPPORT*** in the current uniFLOW User Manual.

The SnapShot Tool works only with the MS Print Migration Tool. It does not work with the MS Printer Migration Wizard which is included in the Windows Server 2008. See also the chapter How to Export Printers (see "Printer Export" on page 54) of this White Paper.

3.17.43 uniFLOW Technical Support Interface Log Export (uniFLOW <= V5.3)

The uniFLOW ***mom Tech Support Interface*** can be reached via the following URLs:

- *http(s)://<uniFLOW_server>/pwserver/techsupport.asp* (uniFLOW server)
- *http(s)://<RPS>:8000/techsupport.asp* (RPS server)

You can choose between different logging levels.

- If an RPS service restart takes place, the logging level will be reset to ***Logging Level - Error***.

An export of the log is possible in case this is required for support cases.

Note that the ***Workflow Diagnostic Interface*** (on page 89) logs and the ***mom Technical Support Interface*** logs will be deleted automatically from the uniFLOW database after seven days.

The techsupport log of the RPS will not be deleted after seven days as the logs will be written into text files. A new text file will be created when one of the following conditions are met:

- RPS service restart.
- The MomAps log size reaches 10 MB.

3.17.44 uniFLOW Technical Support Interface Log Export (uniFLOW >= V5.4)

The uniFLOW ***mom Tech Support Interface*** can be reached via the following URLs:

- **uniFLOW server:**
  http(s)://<uniFLOW_server>/pwserver/techsupport.asp
- **RPS:**
  http(s)://<RPS>:8000/techsupport.asp

You can choose between different logging levels.

- If an RPS service restart takes place, the logging level will be reset to ***Logging Level - Error***.

An export of the log is possible in case this is required for support cases.

- ***Export Log:***
  Clicking this button displays the current active log file in XML format which you can save to an .xml file.

Log File Path

The techsupport logs for uniFLOW and RPS are automatically saved to a text file.

You can find the log files under the following location:

- **uniFLOW server:**
  C:\Program Files (x86)\Common Files\NT-ware Shared\Data\DsPcSrv_<Computer Name>_<Creation Date>_<Creation Time>.log
- **RPS:**
  C:\Program Files (x86)\uniFLOW Remote Print Server\Data\MomAps_<Computer Name>_<Creation Date>_<Creation Time>.log

A new text file will be created when one of the following conditions are met:

- Service restart.
- Log size reaches 10 MB.

If you want to clear the logs, just delete the log files in the aforementioned paths.

Windows Registry Keys

The log rotation scheme can be configured via Windows registry keys (create if not present):

Maximum size of the log file:

- ***Key:***
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NT-ware\Mom\SystemLogger
- ***Value Name:***
  MaxLogFileSize
- ***Value Type:***
  DWORD
- ***Value Data:***
  Enter the maximum size of the log file in bytes (default: 10485760 [= 10 MB]).

Maximum age of the log file:

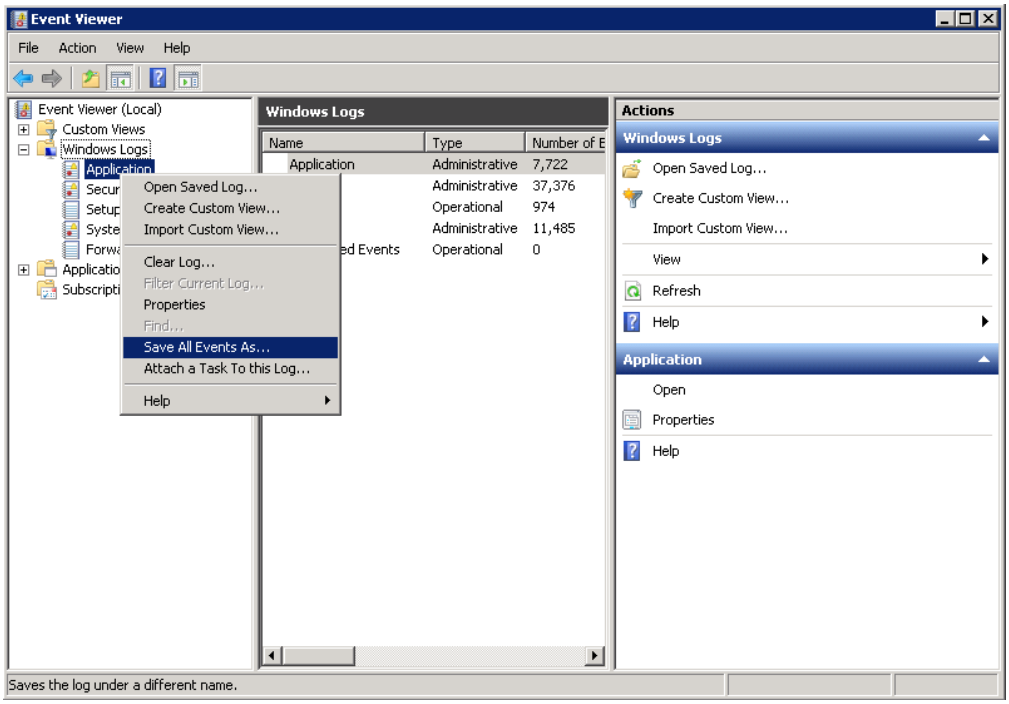
- ***Key:***
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NT-ware\Mom\SystemLogger
- ***Value Name:***
  DaysToKeepInLog
- ***Value Type:***
  DWORD
- ***Value Data:***
  Enter the maximum age of the log file in days (default: 31).

3.17.45 Windows Event Viewer

The Windows Event Viewer (Windows Server 2008 R2 or Higher) collects and shows various information that can be exported for analysis.

- Open the Event Viewer from the ***Administrative Tools*** menu.
- Right-click on the item you were requested to export and select ***Save All Events As...***

  Usually, at least ***Application*** and ***System*** are required.



- Select a target folder, enter a name and click on ***Save***.

- In the window ***Display Information*** select the radio button ***Display information for these languages*** and check ***English (United States)***. That way, the exported file will be in English.
  Press ***OK*** to save the file.

3.17.46 Wireshark Log Generation

Wireshark is the world's foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions. Wireshark has a rich feature set which is far too extensive to explain in this White Paper. For this reason, please refer to the Wireshark website where you can also download the free software.

Download Wireshark (http://www.wireshark.org/).

Please ensure that you work in accordance with data protection law and that you have written consent and permission to trace the network traffic and to send it to NT-ware for support reasons. Please also note that you are using the program at your own risk.

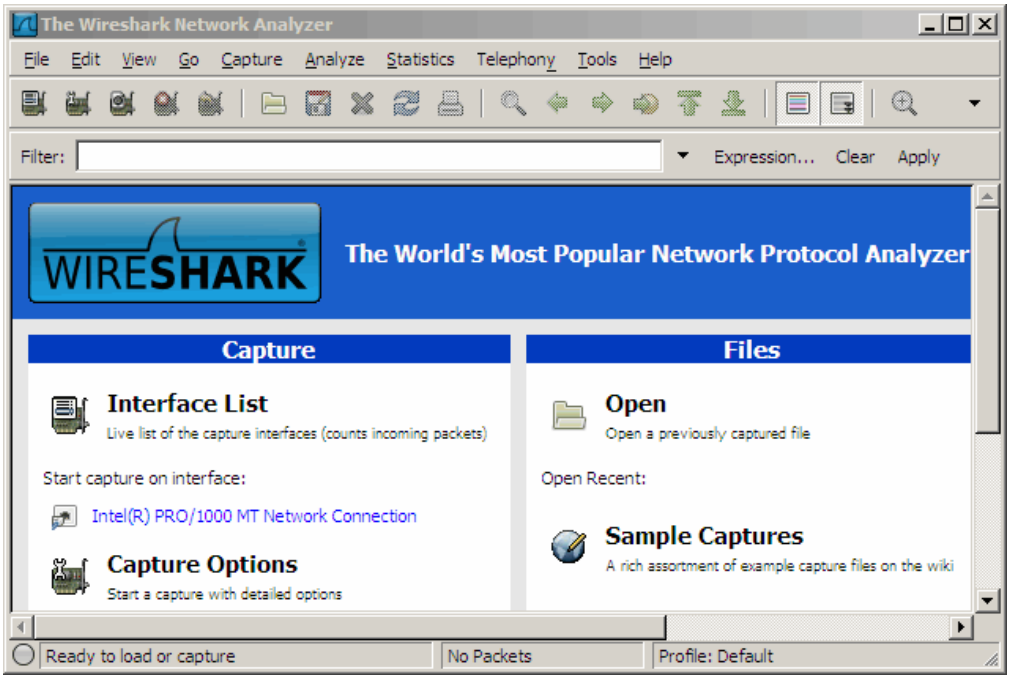
If you want to capture network traffic for support reasons or for the investigation of a software problem, make sure that you start capturing the network traffic and then reproduce the problem from the beginning until the problem appears. This is important in order to provide a complete trace and as much information as necessary.

Wireshark Log Generation

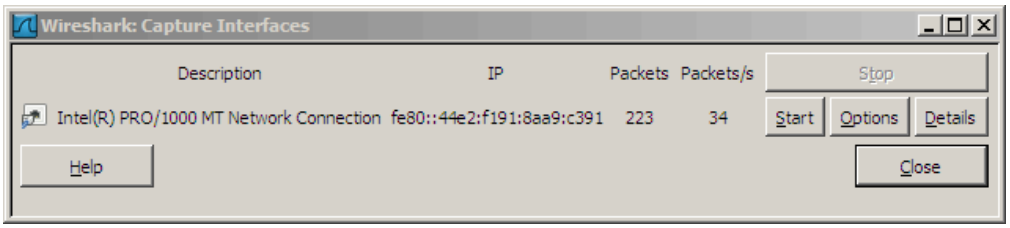
1. Download Wireshark (http://www.wireshark.org/).
2. Install Wireshark on a computer that is involved in the network communication. In most cases, this is the uniFLOW server itself.

If you are in a "switched" network, you can only capture network traffic on devices involved. This means you have to install Wireshark either on the uniFLOW server or RPS.
If this is not possible, you can alternatively connect a network hub between uniFLOW server / RPS and the switched network. Connect your Laptop running Wireshark to this hub as well, and you will be able to see any network communication to and from the uniFLOW server / RPS.

3. In Wireshark, select ***List the available capture interfaces***  from the icon menu bar.



4. You can start capturing by simply clicking the ***Start*** button of the desired interface. As the capture files can grow very fast, we recommend only to capture the communication between the involved computers/devices. To do so, click on ***Options***.



5. Select options and set filter:
In order to keep the file size as small as possible you should always define ***Capture Filters***.
Clicking on ***Capture Filter*** will show you a list with all available filter options. These options can be combined by using ‘and’, ‘or’ or ‘and not’ in the syntax.

Example

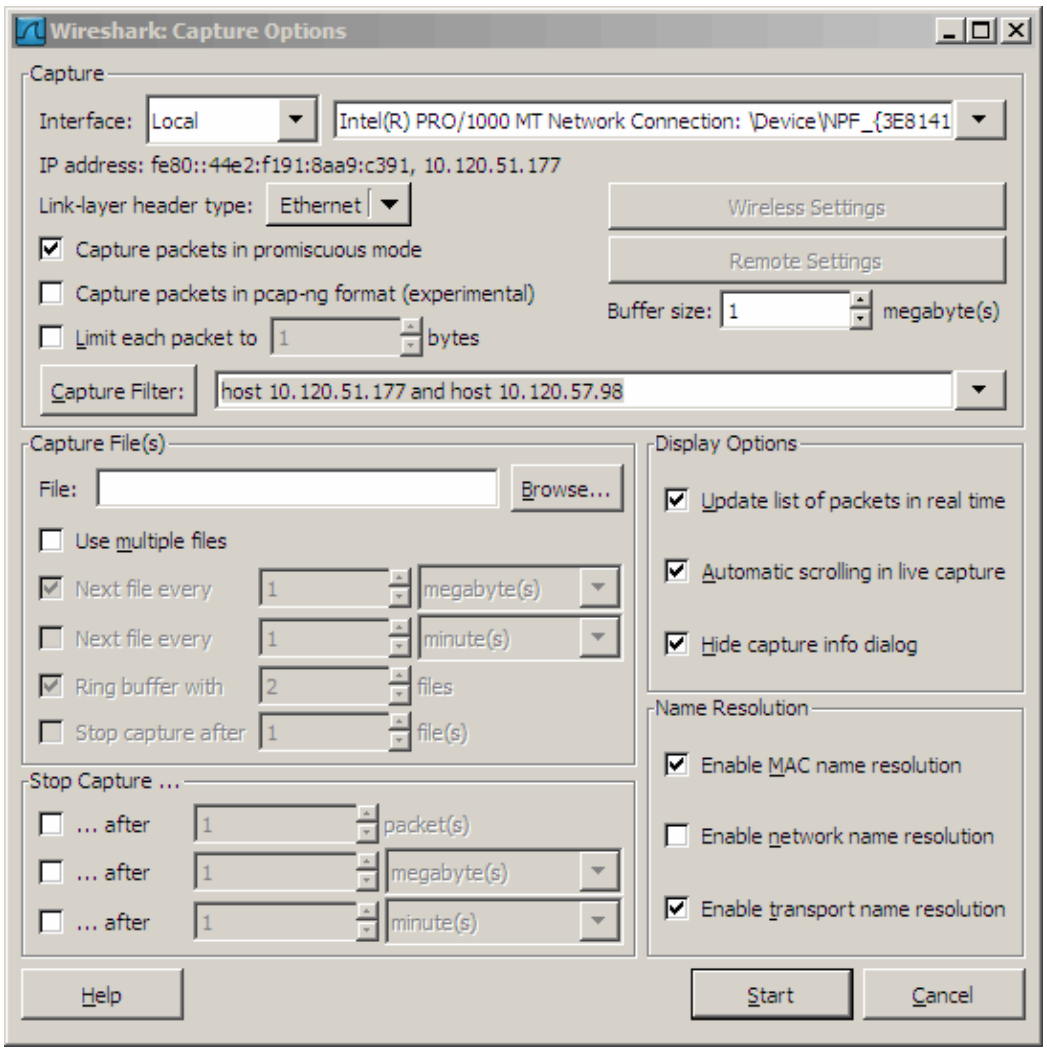
To capture only the traffic between two specific devices you could use:

```
host 10.120.51.177 and host 10.120.57.98
```

To capture only HTTP traffic from a certain computer to the computer you use to capture, you could use:

```
host 192.168.110.3 and tcp port http
```

To avoid your hard disk filling up you can set a ***Stop Capture*** value as capture files grow very large very fast.

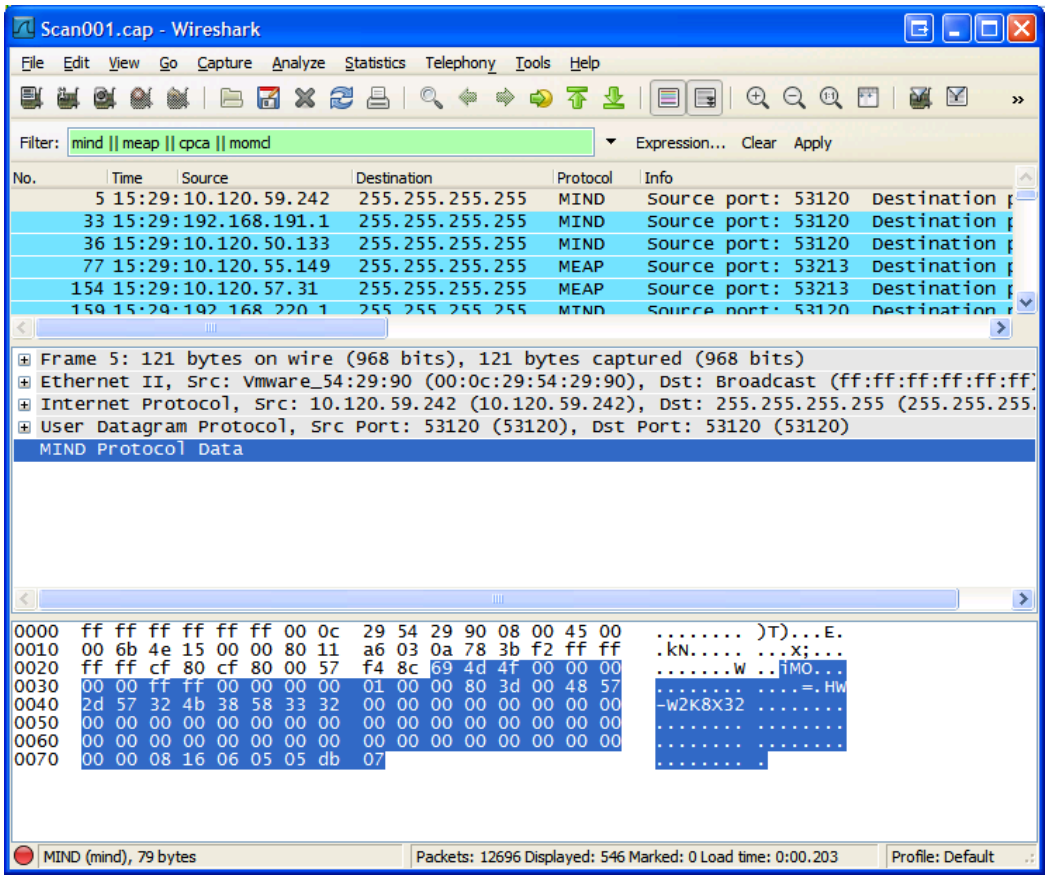


How to use an NT-ware created LUA profile for Wireshark

In case you want to try to investigate by yourself, NT-ware created a LUA profile for Wireshark which makes the reading and interpretation of the network trace easier for you. It highlights the following protocols:

- MOMCL (MomClient)
- MIND (MIND / miniMIND communication)
- CPCA (Common Peripheral Controlling Architecture)

- MEAP (Multifunctional Embedded Application Platform)



You can download the LUA profile created by NT-ware in our ITS under: MOMKB-485 (https://web.nt-ware.net/its/browse/MOMKB-485).

You need to copy the following files in the root folder of your Wireshark installation folder:

- nt-ware-public.lua
- init.lua

Note that the *init.lua* file will be overwritten. So please make a backup of the original file beforehand.

Please name the file *MOM-nnnn.cap* (MOMPS-nnnn) to relate it to the relevant ITS-issue.

Wireshark in an Encrypted Environment

The following only applies to uniFLOW's internal web server.

Communication relating to IIS, MEAP SSL (SSL enabled on the device) or between the uniFLOW SmartClient and MEAP device cannot be decrypted with this approach.

If the uniFLOW installation is configured to use SSL encryption, there are prerequisites to be considered.

1. A new certificate / private key pair has to be created manually.
2. These keys have to be imported into uniFLOW and into Wireshark.

The certificate created by uniFLOW at installation time is lost if replaced by this process. The advantage of the original certificate is that the private key is unknown and inaccessible.

Once any diagnostics is complete, the customer needs to create a new certificate and private key and implement this themselves if they want the private key to be unknown to NT-ware / Canon.

If the customer is happy for the certificate created by this process to be used permanently, ensure the validity period of the certificate is suitable, for instance 10 years.

The uniFLOW / RPS service requires a restart in order for the new certificate to be used.

If the customer agrees to the creation of new keys, follow these steps:

1. Download and install the appropriate version of the Visual C++ 2008 Redistributable and OpenSSL according to the server system.
   http://slproweb.com/products/Win32OpenSSL.html
2. In addition, OpenSSL requires a configuration file. You can create your own or use the file in MOMKB-485 (https://web.nt-ware.net/its/browse/MOMKB-485).
   Copy it to the OpenSSL installation directory.
3. Open a command prompt and navigate to the `\bin` folder in the OpenSSL installation directory.
4. With the following command you create a new private key:
   openssl genrsa -out privatekey.pem 1024
5. With the following command you create a new certificate based on the new private key:
   openssl req -new -x509 -key privatekey.pem -out newcert.pem -days 365
   Enter the required data.

   In case you get this error:
   WARNING: can't open config file: /usr/local/ssl/openssl.cnf
   apply the following command, depending on your Openssl version and retry Step 4:
   set OPENSSL_CONF=c:\OpenSSL-Win32\openssl.cnf
   or
   set OPENSSL_CONF=c:\OpenSSL-Win64\openssl.cnf
6. In uniFLOW open ***Server Config*** > ***Security Settings*** > ***Edit***
7. Add the contents of the private keyfile and certificate file into the respective field. Include the header and footer lines.
8. Click ***Add a Certificate***.
   If required, do the same for any RPS servers and sync the changes.
9. Open Wireshark and open ***Edit/Preferences/Protocols#***
10. Select ***HTTP*** and add 8443 to the ***SSL/TLS Ports*** list.
11. Select ***SSL*** and edit the ***RSA keys list***.
12. Add a new entry with the following values:
    IP address: The address of the server that you want to monitor.
    Port: *8443*

Protocol: *http* (lower case!)

Key File: The private keyfile you created above.

13. Save the changes.

Now you can capture the encrypted network traffic.

3.17.47 Workflow Diagnostic Interface

uniFLOW provides you with a user interface to help solving your workflow problems, the ***Workflow Diagnostic Interface***.

This allows you to display the Workflow Elements that have been used in the uniFLOW system.

The ***Workflow Diagnostic Interface*** is available on the page:

http(s)://<uniFLOW_server>/pwserver/workflowsupport.asp

It can also be accessed via a link on the bottom of the ***mom Tech Support Interface*** page:

http(s)://<uniFLOW_server>/pwserver/techsupport.asp

It is also possible to export the workflow log automatically by using the Workflow Element ***Export Workflow Log (see "***Automatic Workflow Log Export***" on page** 93***).***

For more information on how to create an error role workflow, refer to Error Role (on page 37).

- Note that the *workflowsupport.asp* diagnostics interface is not available on an RPS. However, from uniFLOW V5.3 onwards, similar data can be collected using the ***Workflow Diagnostic Writer***.
- Note that the ***Workflow Diagnostic Interface*** logs will be stored in the uniFLOW database (ServiceUsage_T). For that reason it is possible to gather this information, once a job is successfully completed.

With the help of this interface, individual jobs may be selected and the workflow execution can be displayed. This shows the events processed, the Workflow Elements processing the events, and diagnostic information that goes along with the processing, such as error messages.

The Workflow Diagnostic Interface page is divided into three sections:

- The ***Change Logging Categories*** dialog.
- The ***Active Jobs*** listing.
- The ***Completed Jobs*** listing.

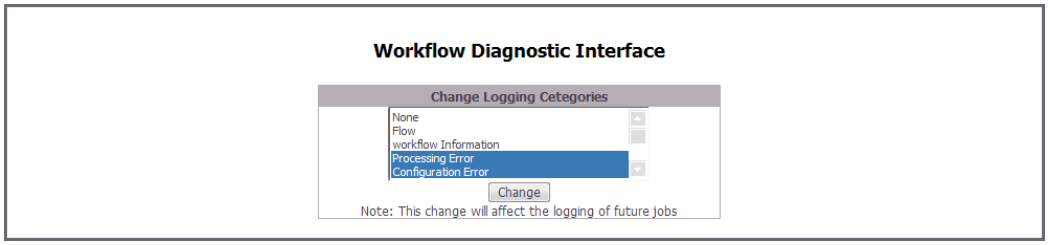
The Change Logging Categories Dialog

The ***Change Logging Categories*** window allows you to select what information or conditions will be logged:

- ***None***
- ***Flow***

- ***Workflow Information***
- ***Processing Error***
- ***Configuration Error***
- ***Licensing Error***
- ***Fatal Error***
- ***Validation Warning***
- ***Validation Error***

Note that the ***Flow*** category will log a huge amount of data. That means that the database is growing very quickly and performance can slow down. For that reason, it is not advisable to leave a production system on ***Flow*** logging for a longer time. It is recommended to leave the default logging level on ***Error*** on a production system.

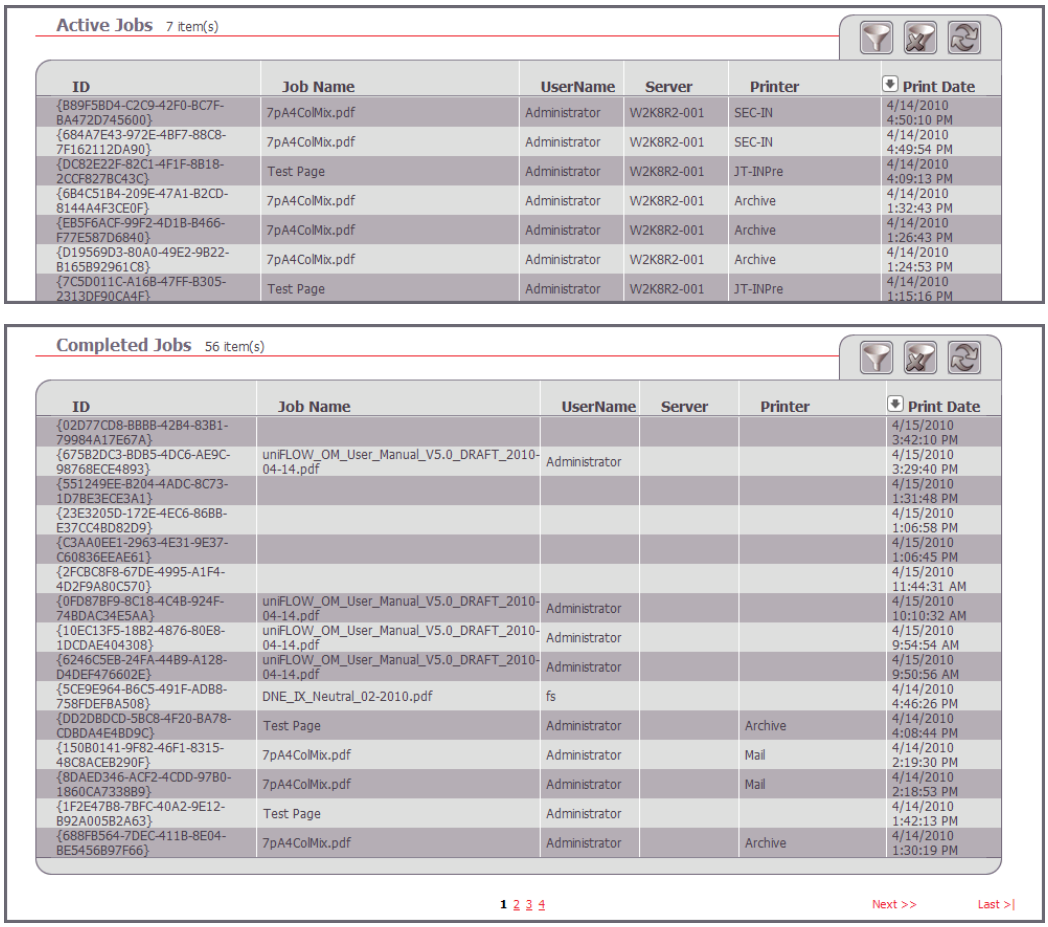


Click the ***Change*** button to apply changes to the selection.

Note that naturally the contents that are to appear within a log need to be configured beforehand. So the changes made in the ***Change Logging Categories*** dialog only apply to jobs that are not yet started. They will not cause changes to the entries that are already in the listings below.

The Jobs Listings

These listings show all jobs that are in the system already. Jobs currently active are shown in the mid section listing, once they are completed they are being moved to the bottom section listing. However, this is not done automatically or periodically, you need to refresh the listings manually, using the refresh button. That way the same jobs are always shown at the same place until you refresh the listing.



Active Jobs 7 item(s)

ID	Job Name	UserName	Server	Printer	Print Date
{B89F5BD4-C2C9-42F0-BC7F-BA472D745600}	7pA4ColMix.pdf	Administrator	W2K8R2-001	SEC-IN	4/14/2010 4:50:10 PM
{684A7E43-972E-4BF7-88C8-7F162112DA90}	7pA4ColMix.pdf	Administrator	W2K8R2-001	SEC-IN	4/14/2010 4:49:54 PM
{DC82E22F-82C1-4F1F-8B18-2CCF827BC43C}	Test Page	Administrator	W2K8R2-001	JT-INPre	4/14/2010 4:09:13 PM
{6B4C51B4-209E-47A1-B2CD-8144A4F3CE0F}	7pA4ColMix.pdf	Administrator	W2K8R2-001	Archive	4/14/2010 1:32:43 PM
{EB5F6ACF-99F2-4D1B-B466-F77E587D6840}	7pA4ColMix.pdf	Administrator	W2K8R2-001	Archive	4/14/2010 1:26:43 PM
{D19569D3-80A0-49E2-9B22-B165B92961C8}	7pA4ColMix.pdf	Administrator	W2K8R2-001	Archive	4/14/2010 1:24:53 PM
{7C5D011C-A16B-47FF-B305-2313DF90CA4F}	Test Page	Administrator	W2K8R2-001	JT-INPre	4/14/2010 1:15:16 PM

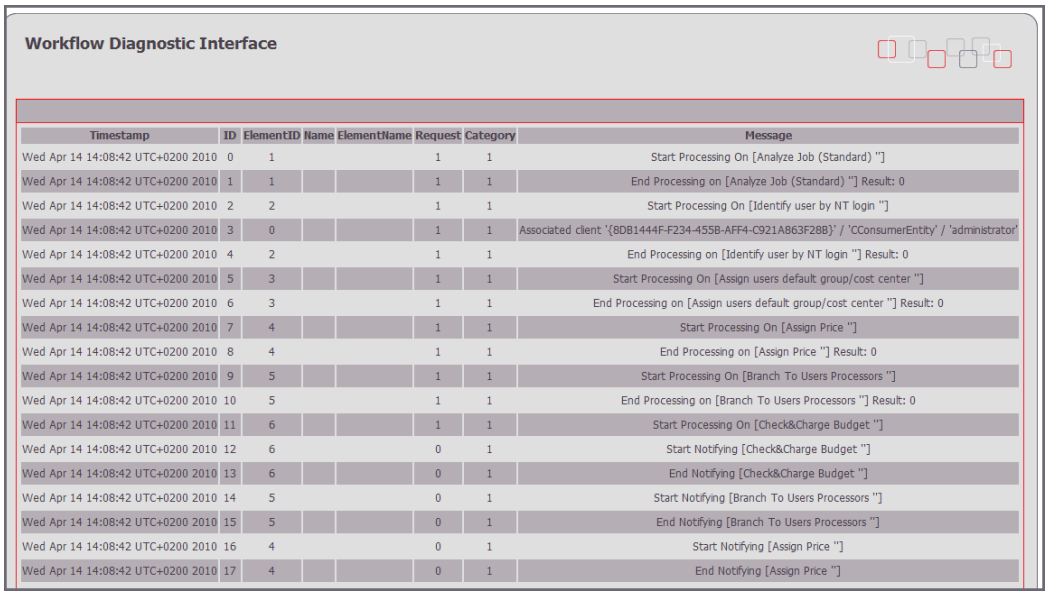
Completed Jobs 56 item(s)

ID	Job Name	UserName	Server	Printer	Print Date
{02D77CD8-BBBB-42B4-83B1-79984A17E67A}					4/15/2010 3:42:10 PM
{675B2DC3-BDB5-4DC6-AE9C-98768ECE4893}	uniFLOW_OM_User_Manual_V5.0_DRAFT_2010-04-14.pdf	Administrator			4/15/2010 3:29:40 PM
{551249EE-B204-4ADC-8C73-1D7BE3ECE3A1}					4/15/2010 1:31:48 PM
{23E3205D-172E-4EC6-86BB-E37CC4BD82D9}					4/15/2010 1:06:58 PM
{C3AA0EE1-2963-4E31-9E37-C60836EEAE61}					4/15/2010 1:06:45 PM
{2FCBC8F8-67DE-4995-A1F4-4D2F9A80C570}					4/15/2010 11:44:31 AM
{0FD87BF9-8C18-4C4B-924F-74BDAC34E5AA}	uniFLOW_OM_User_Manual_V5.0_DRAFT_2010-04-14.pdf	Administrator			4/15/2010 10:10:32 AM
{10EC13F5-18B2-4876-80E8-1DCDAE404308}	uniFLOW_OM_User_Manual_V5.0_DRAFT_2010-04-14.pdf	Administrator			4/15/2010 9:54:54 AM
{6246C5EB-24FA-44B9-A128-D4DEF476602E}	uniFLOW_OM_User_Manual_V5.0_DRAFT_2010-04-14.pdf	Administrator			4/15/2010 9:50:56 AM
{5CE9E964-B6C5-491F-ADB8-758FDEFBA508}	DNE_IX_Neutral_02-2010.pdf	fs			4/14/2010 4:46:26 PM
{DD2DBDCD-5BC8-4F20-BA78-CDBDA4E4BD9C}	Test Page	Administrator		Archive	4/14/2010 4:08:44 PM
{150B0141-9F82-46F1-8315-48C8ACEB290F}	7pA4ColMix.pdf	Administrator		Mail	4/14/2010 2:19:30 PM
{8DAED346-ACF2-4CDD-97B0-1860CA7338B9}	7pA4ColMix.pdf	Administrator		Mail	4/14/2010 2:18:53 PM
{1F2E47B8-7BFC-40A2-9E12-B92A005B2A63}	Test Page	Administrator			4/14/2010 1:42:13 PM
{688FB564-7DEC-411B-8E04-BE5456B97F66}	7pA4ColMix.pdf	Administrator		Archive	4/14/2010 1:30:19 PM

1 2 3 4 Next >> Last >|

With a click on a print job, the job's logging information opens in a pop-up. This basically shows the way the defined workflow of the job is executed. All of the Workflow Elements that have been put together in this printer's workflow, either by yourself or by a printer wizard, are itemized here. Besides that, you will find information about all the error conditions that you previously selected in the ***Workflow Diagnostic Interface***.

Use the ***Save as CSV*** button to save this print job's listed information as comma-separated values and process it in any spreadsheet.



Timestamp	ID	ElementID	Name	ElementName	Request	Category	Message
Wed Apr 14 14:08:42 UTC+0200 2010	0	1			1	1	Start Processing On [Analyze Job (Standard) '']
Wed Apr 14 14:08:42 UTC+0200 2010	1	1			1	1	End Processing on [Analyze Job (Standard) ''] Result: 0
Wed Apr 14 14:08:42 UTC+0200 2010	2	2			1	1	Start Processing On [Identify user by NT login '']
Wed Apr 14 14:08:42 UTC+0200 2010	3	0			1	1	Associated client '{8DB1444F-F234-455B-AFF4-C921A863F28B}' / 'CConsumerEntity' / 'administrator'
Wed Apr 14 14:08:42 UTC+0200 2010	4	2			1	1	End Processing on [Identify user by NT login ''] Result: 0
Wed Apr 14 14:08:42 UTC+0200 2010	5	3			1	1	Start Processing On [Assign users default group/cost center '']
Wed Apr 14 14:08:42 UTC+0200 2010	6	3			1	1	End Processing on [Assign users default group/cost center ''] Result: 0
Wed Apr 14 14:08:42 UTC+0200 2010	7	4			1	1	Start Processing On [Assign Price '']
Wed Apr 14 14:08:42 UTC+0200 2010	8	4			1	1	End Processing on [Assign Price ''] Result: 0
Wed Apr 14 14:08:42 UTC+0200 2010	9	5			1	1	Start Processing On [Branch To Users Processors '']
Wed Apr 14 14:08:42 UTC+0200 2010	10	5			1	1	End Processing on [Branch To Users Processors ''] Result: 0
Wed Apr 14 14:08:42 UTC+0200 2010	11	6			1	1	Start Processing On [Check&Charge Budget '']
Wed Apr 14 14:08:42 UTC+0200 2010	12	6			0	1	Start Notifying [Check&Charge Budget '']
Wed Apr 14 14:08:42 UTC+0200 2010	13	6			0	1	End Notifying [Check&Charge Budget '']
Wed Apr 14 14:08:42 UTC+0200 2010	14	5			0	1	Start Notifying [Branch To Users Processors '']
Wed Apr 14 14:08:42 UTC+0200 2010	15	5			0	1	End Notifying [Branch To Users Processors '']
Wed Apr 14 14:08:42 UTC+0200 2010	16	4			0	1	Start Notifying [Assign Price '']
Wed Apr 14 14:08:42 UTC+0200 2010	17	4			0	1	End Notifying [Assign Price '']

Workflow Diagnostic Interface

Column Name	Description
Timestamp	The timestamp a certain workflow process has taken place.
ID	Simple counter.
Element ID	Always 0.
Name	Generic name of the element, e.g. ***Assign Price***.
Element Name	Specific name of the element set in the workflow editor.
Request	Job request sent to the element, for example: BAJOBREQUEST_STANDARD_DEFAULT_ACTION 0x00000001 BAJOBREQUEST_GENERIC_CONTINUE_WORKFLOW 0x10000400
Event	Job event sent to the element, for example: BAJOBEVENT_WORKFLOW_FINISHED 0x00000007
Category	Category - category of the entry Flow = 0x00000001, These messages are emitted automatically to record the execution flow within a workflow. Information = 0x00000002, These messages are emitted upon request of the Workflow Element to provide information for executing the element. ProcessingError = 0x00000004, These messages are emitted when a processing error, e.g. 'file not found' or 'data in wrong format' occurs. ConfigurationError = 0x00000010, These messages are emitted when the element has detected a configuration error. LicensingError = 0x00000020, Used to record licensing errors. FatalError = 0x00000040,

Column Name	Description
	Any other sort of fatal error. ValidationWarning = 0x10000000, A validation warning entry. ValidationError = 0x20000000 A validation error entry.
Message	Describes the action which has taken place.

3.17.47.1 Automatic Workflow Log Export

The Workflow Element ***Export Workflow Log*** enables automatic export of the workflow log.

See also MOMKB-449 (http://its.nt-ware.net/browse/momkb-449).

Note that the Workflow Element ***Export Workflow Log*** is available since uniFLOW V5.0.4.

General Information

Available in System	• uniFLOW • RPS for Windows
Available in Workflow Role	• Printing • Scanning • Secure Audit • Email • Status Notification • Error • Web Submission Job Order • Web Submission Checkout • Identification
License	• Base
Category	• Output
Useful Before	• No entry
Useful After	• The respective print job entered the error workflow.
Child Connections	• ***Default***

Description

This Workflow Element stores the current workflow log to a file using the given format (e.g. XML or CSV). If no entries are available inside the current workflow log, no file is created.

Parameters

- ***Base Folder:***
  Provides the local or UNC path of the folder to which the log should be stored.
- ***Allow export without login information:***
  - ***Yes*** (default):
    The check is disabled which verifies user identification credentials being available for example if the log should be stored to a local directory which does not need any authentication
  - ***No***
- ***File Name:***
  Allows the beginning of the file name to be specified in which the log file is stored. The respective file type extension is added automatically at the end of the name. The following tokens are replaced:
  - %EXT%
    The standard extension for the file type.

- %DEVICE%
  The device name from which the scan originated.
- %USER%
  The user name.
- %USERLOGIN%
  The user login name.
- %SERVER%
  The uniFLOW server / RPS name.
- For date or time details the following tokens can be used:
  - %H%
    hour
  - %M%
    minute
  - %S%
    second
  - %d%
    day
  - %m%
    month
  - %y%
    year

- ***Behavior for existing files:***
  What to do if the target file name already exists.
  - ***Add unique number*** (default)
  - ***Overwrite***
- ***Export format of the log file:***
  This parameter defines the export format which is for example
  - ***XML*** (default)
  - ***CSV***
- ***Create a log file in the home directory of the following user:***
  This parameter defines whether the log should be stored in the home directory of a given user (login name). If the Base Folder parameter is set this parameter is ignored.

Available Tokens

Token replacement							
These tokens can be used within the parameters of the Workflow Element.							
General Tokens:							
	General	Job	Printer	Session	User		

Specific Tokens:	**Token:**	**Description:**
	%DEVICE%	The device name from which the scan or print originated.
	%EXT%	The standard extension for the file type.
	%SERVER%	The uniFLOW or RPS Server name.
	%USER%	The user name.
	%USERLOGIN%	The user's login name.
Notes:	The %token% tokens are case-sensitive.	
	Unknown %token% tokens are replaced as empty strings.	
	Tip: beware of entering 'path\{token}'; this backslash escapes the '{', so you must enter 'path\\{token}'.	

3.17.47.2 Workflow Diagnostic Writer

The Workflow Diagnostic Interface (on page 89) only collects data on the uniFLOW server, not on RPS or uniFLOW SmartClient. From uniFLOW V5.3 onwards, data can be collected on uniFLOW server, RPS and uniFLOW SmartClient with the Workflow Diagnostic Writer. The Workflow Diagnostic Writer is a service running on the local machine and capable of creating a log file for each workflow job. The logging categories are the same as with the Workflow Diagnostic Interface. However, they have to be configured via a Windows registry key:

Windows Registry Keys

LogPath	
Key:	*HKEY_LOCAL_MACHINE\Software\NT-ware\Mom\WorkflowLog*
Value Name:	*LogPath*
Value Type:	REG_SZ
Value Data:	*C:\Temp Log*
Description:	Absolute path to the directory to store the log files into.

LogCategories	
Key:	*HKEY_LOCAL_MACHINE\Software\NT-ware\Mom\WorkflowLog*
Value Name:	*LogCategories*
Value Type:	*REG_DWORD*
Value Data:	*0xffffffff* (log everything)

LogCategories	
Description:	A bit mask indicating which logging categories shall be logged. The available values are described below. Combinations are possible.

Available Logging Categories

Name	Value
Nothing	0x00000000
Flow	0x00000001
Information	0x00000002
Processing error	0x00000004
Configuration error	0x00000010
Licensing error	0x00000020
Fatal error	0x00000040
Validation warning	0x10000000
Validation error	0x20000000
Log everything	0xffffffff

- The Workflow Diagnostic Writer has to be configured via Windows registry.
- A uniFLOW Server service restart is necessary in order for the Windows registry changes to take effect.
- This function requires uniFLOW V5.3 or higher.
- For a uniFLOW SmartClient that uploads job information to a uniFLOW server, the *LogCategories* value can be used independently of the *LogPath* variable as the workflow log for each uniFLOW SmartClient job will be available within the Workflow Diagnostic Interface (on page 89).

3.18 Web Services / Web Issues

Recommended Logs and Data for Analyzing Purposes	Priority
• W3SVC log files The W3svc.log contains information about communication between the IIS Server and connected clients. The location of your W3SVC logfiles depends on your configuration. For instance, the path could be *C:\Windows\system32\logfiles\w3svc1*.	xxx
• IIS-backup The IIS backup creates a backup of the IIS configuration. See: IIS Backup Creation (on page 43)	x

Recommended Logs and Data for Analyzing Purposes	Priority
• Process Monitor Tool Log Generation (on page 57)	x
• uniFLOW Snapshot Creation (on page 80) or System Image Creation (on page 72)	x
• XML Export (uniFLOW Configuration / IIS Backup Creation (on page 43) / Statistics Problem Check (on page 70))	x
• Customization Possible additional websites on the uniFLOW server. Information on customization can be found in the original project checklist.	x

3.19 WQM (incl. PrePrint) Issues

Especially in WQM / Job Ticketing scenarios the right printer driver is of importance:

Recommended Logs and Data for Analyzing Purposes	Priority
• Information on DIF settings and PPDs Especially when using an unsigned DIF that has been created by yourself using PPDs provided by Canon or other vendors - this information is important.	xxx
• Settings in uniFLOW Snapshot of the uniFLOW configuration. See: uniFLOW Snapshot Creation (on page 80)	xx
• Printer driver (type and version) Provide this for both input and output printer.	xx
• Information on customizations in WQM/Job Ticketing This information can be found in the original project checklist of this customization.	xx
• Configuration of input/output printer A screenshot of the workflow might be enough.	x

4 URLs

This chapter lists the Web Page URLs for the individual product. These URLs will be for the user/administration access and any related support UR's. Where the URL needs to be enabled via a registry entry this will be noted.

This chapter contains URLs that give access to the database or system logging pages. As this is a security risk, it should only be used under advisement by support professionals or expert users.

Do not hand out the present document to any customer directly. The document is intended to be used by support professionals or expert users only.

4.1 Client

PWClient

This is the client (User) web page.

http://<uniflowserver>/pwclient/

4.2 ICARUS Server for Web Ports

uniFLOW Scan Simulator

This is the address of the Scan Simulator

- **Unencrypted:**
  http://<ICARUS server address>:8003
- **Encrypted:**
  https://<ICARUS server address>:8446

4.3 Miscellaneous

IRIS Status Page

This site will show you the current number of jobs being processed by the Scan Processing Server (MOMSpaceSuite). This page will show an error if the scan processing server is offline or not accessible. The default port is used in this example, please change it if your installation has a custom port set during installation.

http://localhost:8001/ufwkp/status.htm

Adding USB ID Readers Key

Install and configure the Login Manager, then use the following URL to upload the relevant config file *.cfg.

http://<iR-IP>:8000/usbidmodule/hidconfig.htm

or

http://<iR-IP>:8000/usbidmodule/base.htm

Canon SMS RUI for the Meap Applet

http://<MFP –IP-Address>:8000/sms

4.4 RPS

RPS Status Page

This page displays the current RPS status and allows you to perform a 'Force Update' and test the SMTP connection. The attached device configurations are visible as well as their device status if monitoring is set.

http://<RPS>:8000/status.htm

RPS Dump Page

This page provides you with a dump of the current RPS database or analysis.

Must be enabled in the Windows registry: *MOMAPS/EnableDump REG_DWORD 0/1*

http://<RPS>:8000/dump.htm

RPS Techsupport Page

This page provides you access to the current techsupport file. This page lists the entry in the currently written to MOM RPD Log file in the Data folder. This page is defaulted to Error only. Ensure you always leave a system on Error only and not Flow mode.

http://<RPS>:8000/techsupport.asp

SQLQuery Page (uniFLOW => 4.1)

This page allows you to run SQL queries against the RPS local database (ObjectSpace.db).

Must be enabled in the Windows registry: *MOMAPS/EnableSqlQuery REG_DWORD 0/1*

http://<RPS>:8000/sqlquery.htm

4.5 Server

uniFLOW Admin Service

This is the uniFLOW Admin Service page where uniFLOW and dependent servers should be controlled.

http://localhost:49580/

PWServer

This is the primary uniFLOW Administrative Web Site.

http://<uniflowserver>/pwserver/

PWRQM

This page provides access to the Release Queue Manager.

http://<uniflowserver>/pwrqm/

uniFLOW Budget Management Web

This page provides a simple and secure user budget management page for a cashier. The budget page must first be enabled under:
Server Config. > General Settings > Budget Management.

http://localhost/pwbudget/

PWWQM (uniFLOW <= 4.1)

This page provides access to the Web Queue Manager for Professional Modules.

http://<uniflowserver>/pwwqm/

4.6 Support URLs

Tech Support Page

This page allows you to access support logs and information regarding the uniFLOW server.

http://<uniFLOW_server>/pwserver/techsupport.asp

Database Viewer

This page allows you to look directly at the uniFLOW SQL database and review the tables.

http://<uniFLOW_server>/pwserver/techdispdb.asp

In order to prevent unauthorized access to this page, a dummy page is installed by default. The real page can be activated by copying the files

- *techdispdb.asp*
- *techdisprecord.asp*

from *C:\<program_folder>\Common Files\NT-ware Shared\Scripts*

to *C:\<program_folder>\uniFLOW\WebServer*

uniFLOW Workflow Diagnostic Interface (uniFLOW => 5.0)

This page provides access to the workflow engine logging page for workflow diagnostics:

http://localhost/pwserver/workflowSupport.asp

uniFLOW Web RegEx Editor

This WebSite displays the RegularExpression test website:

http://localhost/pwserver/dispRegExEditor.asp

Change Language Switch

This page will allow you to change the language set used by replacing the language=EN extension to your required language. Full listing of the supported languages can be seen in the MOMLang.xml file.

http://<uniflowserver>/pwserver/openlang.asp?language=EN

uniFLOW SQL Connector (uniFLOW => 5.0)

This page allows the configuration of custom database imports and exports to multiple sources:

http://localhost/pwserver/SqlConnector/default.asp

MEAP Access to uniFLOW Server

Check if you can access the *IcarusRequest.dll*

http://localhost/pwclient/isapi/IcarusRequest.dll?script=LMCARDTYPELOGIN/CardLogin.icarus

4.7 Tech Support Page for uniFLOW SmartClient Diagnostics

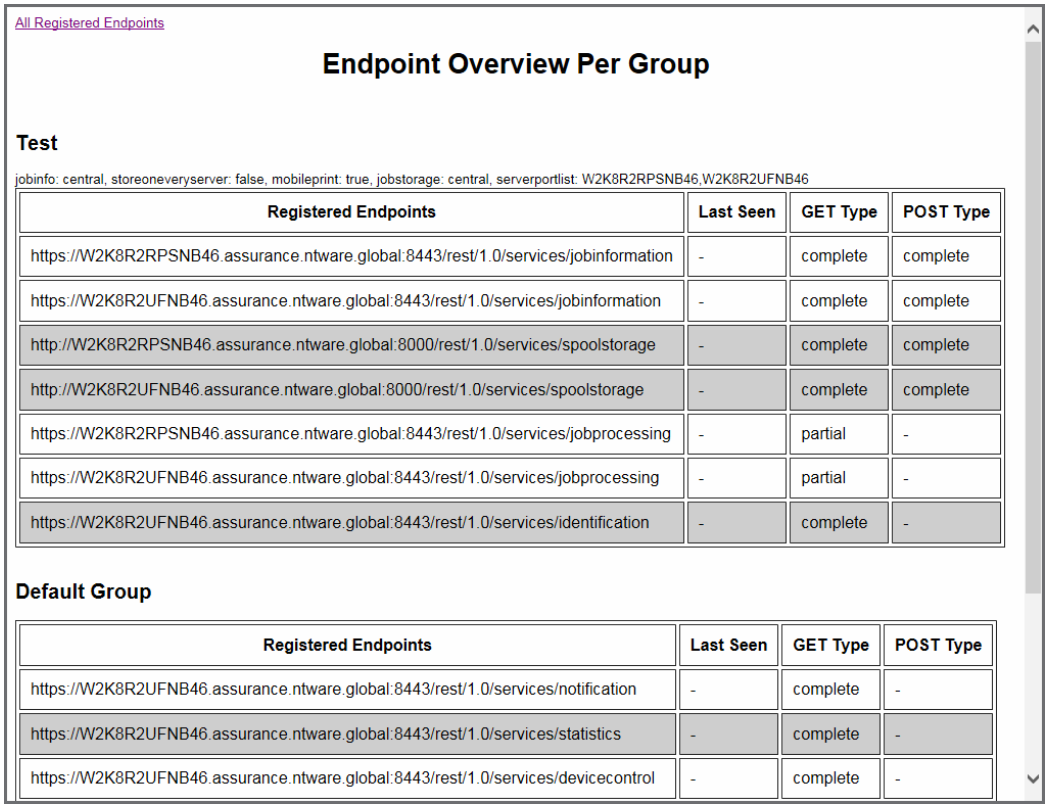
In uniFLOW SmartClient environments you can display an ***Endpoint Overview*** for diagnostic purposes. This overview will show the currently registered peers that is to say the registered MEAP devices and uniFLOW SmartClients.

- For HTTPS environments enter:
  https://<uF server or RPS>:8443/techdisppeers.asp

- For HTTP environments enter:
  http:// <uF server or RPS>:8000/techdisppeers.asp

See also uniFLOW SmartClient Issues (on page 14)

Example Screenshot



All Registered Endpoints

Endpoint Overview Per Group

Test

jobinfo: central, storeoneveryserver: false, mobileprint: true, jobstorage: central, serverportlist: W2K8R2RPSNB46,W2K8R2UFNB46

Registered Endpoints	Last Seen	GET Type	POST Type
https://W2K8R2RPSNB46.assurance.ntware.global:8443/rest/1.0/services/jobinformation	-	complete	complete
https://W2K8R2UFNB46.assurance.ntware.global:8443/rest/1.0/services/jobinformation	-	complete	complete
http://W2K8R2RPSNB46.assurance.ntware.global:8000/rest/1.0/services/spoolstorage	-	complete	complete
http://W2K8R2UFNB46.assurance.ntware.global:8000/rest/1.0/services/spoolstorage	-	complete	complete
https://W2K8R2RPSNB46.assurance.ntware.global:8443/rest/1.0/services/jobprocessing	-	partial	-
https://W2K8R2UFNB46.assurance.ntware.global:8443/rest/1.0/services/jobprocessing	-	partial	-
https://W2K8R2UFNB46.assurance.ntware.global:8443/rest/1.0/services/identification	-	complete	-

Default Group

Registered Endpoints	Last Seen	GET Type	POST Type
https://W2K8R2UFNB46.assurance.ntware.global:8443/rest/1.0/services/notification	-	complete	-
https://W2K8R2UFNB46.assurance.ntware.global:8443/rest/1.0/services/statistics	-	complete	-
https://W2K8R2UFNB46.assurance.ntware.global:8443/rest/1.0/services/devicecontrol	-	complete	-