

Universal Login Manager

Installation and Configuration Guide

ULM V4.12



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.

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the prior written permission of NT-ware Systemprogrammierungs-GmbH (hereinafter also referred to as NT-ware).

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 HP Inc.; 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®, Hyper-V® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries of Microsoft Corporation; Mopria Print Service of Mopria Alliance Inc.; 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-Technologies B.V. Océ is a Canon company, 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®, mdsFLOW®, uniFLOW Serverless Secure Printing®, Helix Production Workflow®, MIND®, microMIND®, MiCard® and uniFLOW Service for AirPrint® 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; VMware vSphere® and VMware vSphere® Motion® are registered trademarks of VMware; 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 the 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 operating 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.

Wednesday, December 2, 2020, 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.

uniFLOW and corresponding components like Web Submission and Internet Gateway rely heavily on their SQL databases. We strongly suggest that you refrain from modifying these SQL databases manually without prior consultation from the NT-ware support team. NT-ware does not assume responsibility or liability for possible impact on your uniFLOW environment after modifying any of the SQL databases.

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

©1998-2020 NT-ware Systemprogrammierungs-GmbH.

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.

Technical Support

Your dealer will provide first technical support services. Before you contact the dealer for technical support, ensure you have read this document.

Open Source License Information

The following copyright statement and license apply to the opencsv software components that are used by the Universal Login Manager.

Apache License - Version 2.0, January 2004 - <http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Contents

1	General Introduction	1
2	Introduction	1
2.1	General Architecture	1
2.2	Authentication Mode	2
2.2.1	Local Authentication Mode.....	2
2.2.2	Domain Authentication Mode	3
2.2.3	uniFLOW Server Mode.....	3
2.3	Login Types	3
2.3.1	Image Login or Image Login + PIN.....	4
2.3.2	Proximity Card Login or Proximity Card Login + PIN.....	4
2.3.3	User Name and Password Login	5
3	Components	6
3.1	Application	6
3.2	Usage Tracker (Rich Internet Application).....	7
4	System Requirements.....	7
4.1	Hardware and Optional Items	7
4.2	Software Requirements	7
4.2.1	Web Browsers.....	7
4.2.2	Printer Driver and AMS Printer Driver Add-in Module.....	8
4.2.3	Active Directory Server Requirements	8
5	Installation	9
5.1	Installation via Content Delivery System (Device UI).....	9
5.2	Installation via Content Delivery System (Remote UI)	14
5.3	Manual Installation via Remote UI	16
6	Update	18
7	Uninstallation.....	19
8	Configuration	23
8.1	Administration Tool Login	23
8.1.1	Activation	25
8.1.2	Main Page	25
8.2	Users	26
8.2.1	Home Folder	28
8.2.2	Home Folder Settings.....	30

8.3	Profile	31
8.4	Setup	32
8.4.1	Login Type	33
8.4.1.1	Image Login and Image Login + PIN.....	33
8.4.1.2	Proximity Card and Proximity Card + PIN	35
8.4.1.3	User Name / Password	36
8.4.2	Authentication Mode.....	36
8.4.2.1	Active Directory	38
8.4.3	Import/Export	41
8.4.4	System Manager Settings	43
8.5	Roles	43
8.5.1	Access Control.....	44
8.5.2	Import and Map Groups from Active Directory.....	45
8.6	Customize	47
8.6.1	Customized Language Strings	49
8.7	Usage Tracker	53
8.7.1	Adding a Device	56
8.7.1.1	Creating a Certificate.....	57
8.7.2	Cost Table.....	59
8.7.3	Creating a Report	59
8.7.4	Security Aspects.....	62
9	Secure Print	64
10	Upgrade to uniFLOW Server	64
11	How to obtain Log Files	64
12	Appendix	65
12.1	Hardware	65
12.2	Optional Items	67
12.2.1	Supported Card Readers	67
12.2.2	USB Device Port	68
12.2.3	AMS - Access Management System.....	68
13	Glossary	70
14	Index	73

1 General Introduction

This document describes the technical requirements and setup procedures for the Universal Login Manager. It is aimed at product managers, service managers, service technicians, account managers, support, showroom personnel and external Canon partners, who need to be able to set up and configure the Universal Login Manager.

Definitions and Abbreviations used in this document

- ULM:** Universal Login Manager
- AD:** Active Directory
- CDS:** Content Delivery System
- RIA:** Rich Internet Application
- AMS:** Access Management System

2 Introduction

Universal Login Manager is a MEAP application developed by NT-ware for imageRUNNER ADVANCE devices to provide a convenient server-less solution for simple user authentication, including image login and proximity card login support. This application helps to fully utilize the native capabilities of the imageRUNNER ADVANCE for personalization, and also delivers basic usage and cost reporting functionality. Universal Login Manager also utilizes the Access Management System (AMS) to allow granular control of access per user.

In addition, Universal Login Manager can be used as a login application for uniFLOW. Users can easily migrate to a uniFLOW solution without sacrificing their initial investments such as MiCard card readers.

2.1 General Architecture

Universal Login Manager combines two concepts:

- **Authentication Provider:**
The server the user authenticates against. This server can be configured in the setting *Authentication Mode*.
- **Authentication Presentation:**
The way the user logs in to a device. This can be configured in the setting *Login Type*.

Universal Login Manager is very flexible, supporting any size of customer by using a combination of authentication mode and login type.

Login Type	Authentication Mode		
	Local Authentication	Domain Authentication (Active Directory)	uniFLOW Authentication
Image Login	✓		
Proximity Card Login	✓	✓	✓
User Name and Password Login	✓	✓	✓

2.2 Authentication Mode

You can select three different kinds of *Authentication Providers*.

- Local Authentication Mode:**
 An administrator can establish a user database on the device locally and utilize it as an authentication provider.
- Domain Authentication Mode:**
 Utilizes an existing Active Directory on a Windows server as authentication provider.
- uniFLOW Server:**
 A uniFLOW server can be selected as an authentication provider. Universal Login Manager can also act as a login application for uniFLOW. This enables an easy upgrade from a server-less solution to the uniFLOW solution. In this case, the chargeable Device Access License is required on the uniFLOW server.



Local Authentication Mode and *Domain Authentication Mode* can **only** be activated if the device is **not** configured as printer in uniFLOW. Otherwise, the *Authentication Mode* automatically switches to *uniFLOW Server* as soon as the uniFLOW server connects to the device.

2.2.1 Local Authentication Mode

Local Authentication Mode allows users to authenticate against a local database on the device containing authentication information. This database can be exported and imported via a web interface and can be manually distributed to other devices.

Universal Login Manager Configuration can register up to 1,000 users. Only users that are associated with the administrator role can manage users.

Local Authentication mode supports the following login methods:

- Image Login (up to 48 users)
- Image Login + PIN (up to 48 users)
- Proximity Card Login (up to 1,000 users)
- Proximity Card Login + PIN (up to 1,000 users)
- Username and Password (up to 1,000 users)

You can select the login type in the *Setup* menu of the Universal Login Manager Administration Configuration.

2.2.2 Domain Authentication Mode

The Domain Authentication Mode allows users to authenticate against an Active Directory on a Windows server at the customer's site. You can also assign role information to each group in an Active Directory.

The following login methods are available here:

- Proximity Card Login
- Proximity Card Login + PIN
- Username and Password

When users enter their user name and password for network access, or swipe their proximity card which is linked to the network credentials, user authentication is performed.

2.2.3 uniFLOW Server Mode

Universal Login Manager can be used as login application for the uniFLOW solution. This minimizes additional investment when upgrading to uniFLOW.

2.3 Login Types

Universal Login Manager supports different login types that are described in the following chapters.



The PIN code used in some of the login types is **not** the same PIN code as used in the department ID management of the printer. The PIN codes for device department IDs should be set to 0 in order to avoid problems.

2.3.1 Image Login or Image Login + PIN

Image Login allows users to login by pressing a button on the device's UI with an image representing the user account. Image Login works on Local Authentication Mode only.

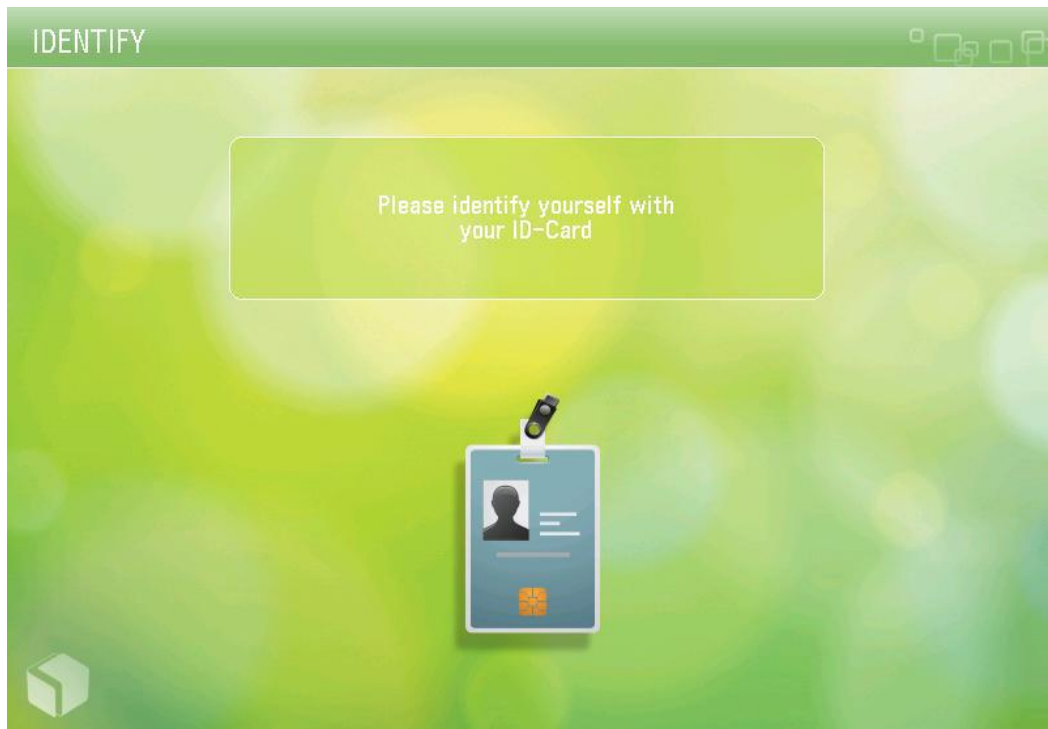
Up to 48 user icons can be registered and uploaded as account image through the ULM Configuration on the Universal Login Manager RUI. You can select *Image Login* or *Image + PIN* mode, in which case an additional PIN code input will also be required for login.



2.3.2 Proximity Card Login or Proximity Card Login + PIN

Proximity Card Login allows users to perform authentication by using a proximity card such as HID, Mifare and others.

The supported card reader must be connected to the device. The USB Device Port option is recommended for fitting the Card Reader securely inside the device. Proximity Card Login works with all authentication modes (Local, AD, uniFLOW). You also can set a PIN code for additional security on login.

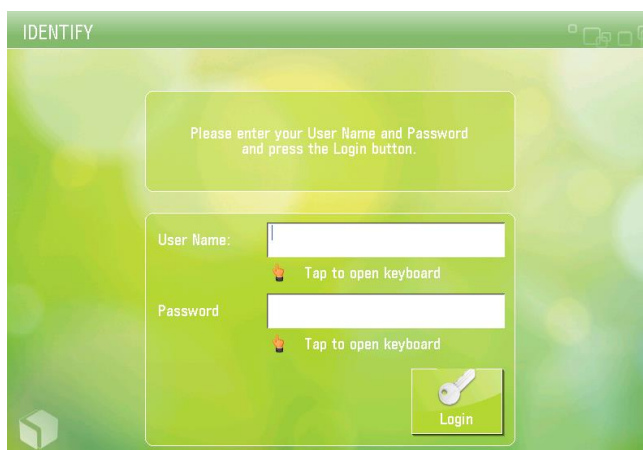


Supported Card Readers

See Supported Card Readers (on page [67](#)) for a list of all supported card readers.

2.3.3 User Name and Password Login

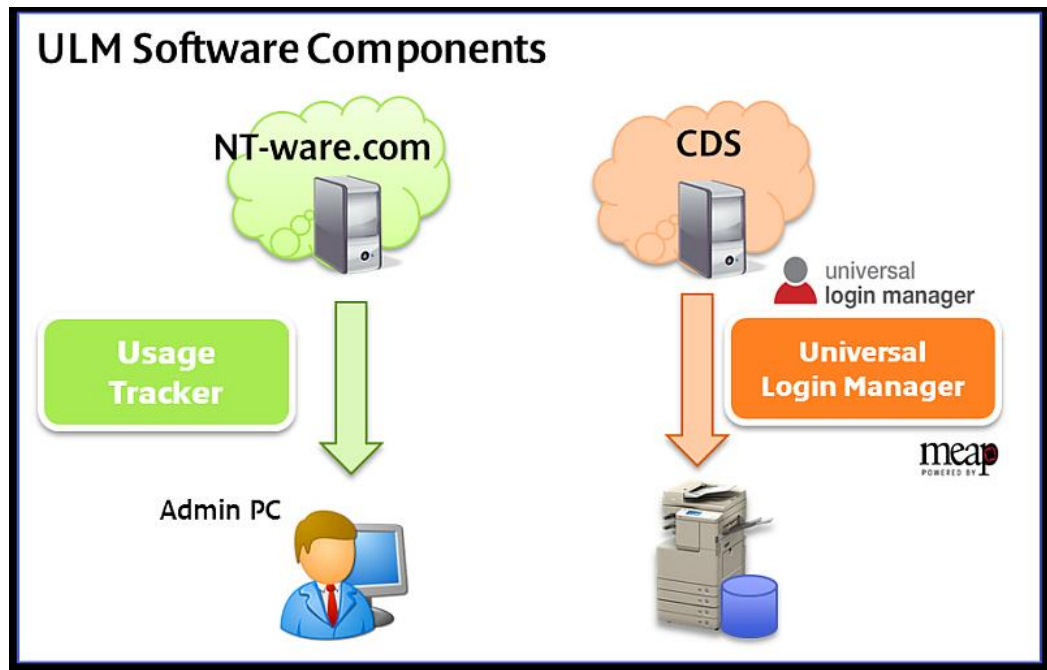
Similar to SSO-H which is standard on MEAP enabled devices (iR and imageRUNNER ADVANCE), you can login with the user name and password registered in the user database. All authentication modes (Local, AD or uniFLOW) are possible.



3 Components

Universal Login Manager consists of two software modules. These are individually described in the following sections.

- Universal Login Manager: The main package installed locally on the device.
- ULM Usage Tracker: Web browser plug-in application (RIA).



3.1 Application

Universal Login Manager for MEAP

Universal Login Manager is developed by NT-ware, based on uniFLOW Login Manager. Unlike uniFLOW Login Manager, it can perform without a uniFLOW server and enhances the existing native functionalities on the imageRUNNER ADVANCE such as Send to Myself, personal buttons/workflows and AMS functionality, all of which are dependent on user authentication on the device.

	Size
Maximum file space	20000 KB
Maximum memory usage	6000 KB
Maximum file descriptor usage	30 KB
Maximum socket usage	8 KB
Maximum thread usage	20 KB

3.2 Usage Tracker (Rich Internet Application)

ULM Usage Tracker is a web application that can be downloaded as a web browser plug-in via a link in the ULM RUI menu. Once it is downloaded to a PC, it works in the web browser until the cache is cleared.

ULM Usage Tracker can collect job log data from all registered devices (up to 10 devices) and shows print/copy/scan activities per user or per device including transaction costs, which are maintained in a separate table.

The chapter Security Aspects (on page [62](#)) describes in detail, how the ULM Usage Tracker works and why it is safe to use it.

4 System Requirements

4.1 Hardware and Optional Items

A list of supported devices and firmware versions as well as optional items can be found in the appendix (on page [65](#)).

4.2 Software Requirements

4.2.1 Web Browsers

A web browser is required in order to access and operate the ULM Configuration and the ULM Usage Tracker.

	ULM Config.	ULM Usage Tracker
	V3.1	V4.0
Internet Explorer 11.0	✓	✓
Microsoft Edge (EdgeHTML-based)	✗	✗
Microsoft Edge V83 (Chromium-based)	✓	✓
Mozilla Firefox 73	✓	✓
Safari 5.1 (Windows)	✓	✗
Opera for Mac 12	✓	✗
Opera 67	✓	✓
Google Chrome 80	✓	✓



NT-ware does not test Internet Explorer versions older than Internet Explorer 11 because versions before 11 are not supported by Microsoft anymore.



The export/import functionalities for cost tables in the ULM Usage Tracker use Flash and will only work on systems with an installed version of Adobe's Flash Player 10 or higher..

4.2.2 Printer Driver and AMS Printer Driver Add-in Module

One of the following printer drivers must be installed on the computer in advance.

- UFR II Printer Driver V20.60 or later
- PCL 6 Printer Driver V20.60 or later
- PCL 5e/5c Printer Driver V20.60 or later
- PS 3 Printer Driver V20.60 or later

If users require AMS functionality, the AMS Printer Driver Add-in Module must also be installed on all PCs in the network.

4.2.3 Active Directory Server Requirements

Supported Windows Server: Windows Server 2003/2008 or later.



Trust relationships between domains are currently not supported by the Universal Login Manager.

5 Installation

This section describes the procedure for installing Universal Login Manager on a MEAP device.



The installation is described based on an imageRUNNER ADVANCE third generation model. Therefore, if you use a different device, the installation procedure may vary slightly.

There are several ways of installing the Universal Login Manager application:

- Content Delivery System (CDS) - License Access Number (LAN) required
 - Installation via Content Delivery System (Device UI) (on page [9](#))
 - Installation via Content Delivery System (Remote UI) (on page [14](#))
- Manual Installation - .jar file and .lic file are required
 - Manual Installation via Remote UI (on page [16](#))



uniFLOW Online Connection

The Universal Login Manager can also be installed when you connect your device to uniFLOW Online or uniFLOW Online Express. Since this is not meant as a stand-alone installation, this is not described here.

Details can be found in the uniFLOW Online First Steps Guide (https://www.nt-ware.com/uFO_FS/).

Required Items	Default Admin Password	License Access Number	Application Files [.jar/.lic]	Networked PC with Web Browser	Internet Connection
Installation Methods					
CDS via Local UI	see Canon documentation	Required			Required
CDS via Remote UI	see Canon documentation	Required		Required	Required
Manual Installation via SMS	see Canon documentation		Required	Required	

The recommended installation mechanism is CDS. However, in some circumstances CDS may not be suitable. In these cases, please obtain the MEAP application .jar file and the .lic file from the Canon Software Download Center and install using SMS.

5.1 Installation via Content Delivery System (Device UI)

In order to install the Universal Login Manager through the CDS, a sixteen-digit License Access Number (LAN) is required:

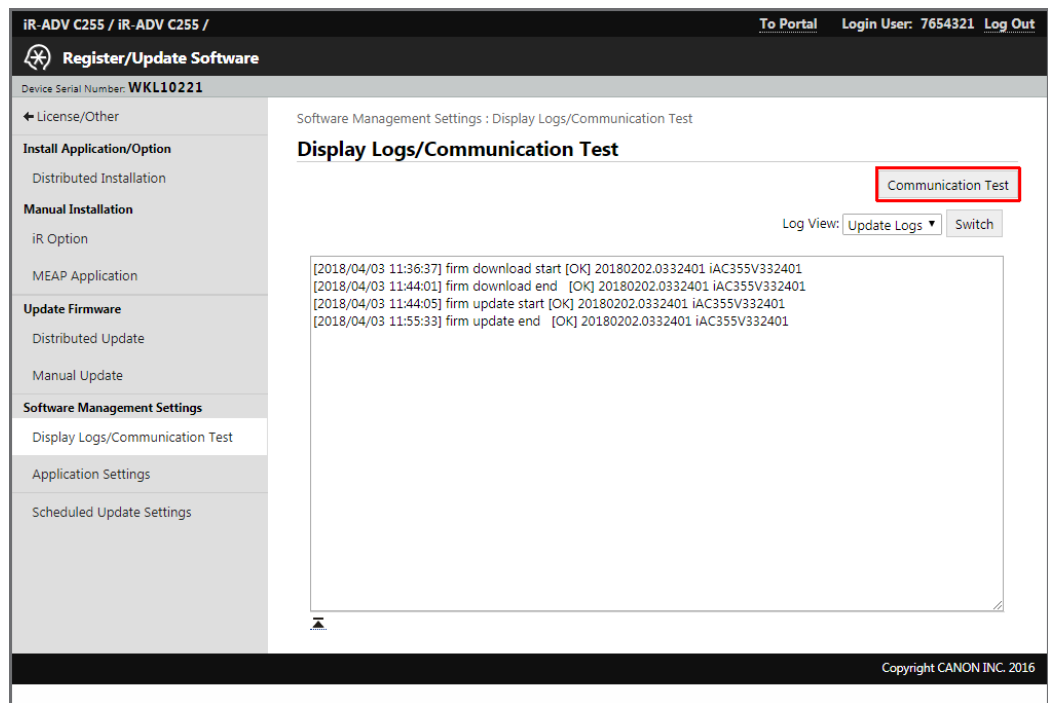
Please find the LAN for your version of ULM here (<https://link.nt-ware.net/id250>).

In order to access the CDS, you can operate from either the device's local UI or the device's remote UI from a networked PC.

Before you install the Universal Login Manager via CDS, please make sure your network can communicate with the CDS. The "Communication Test" function is available to test the network conditions.

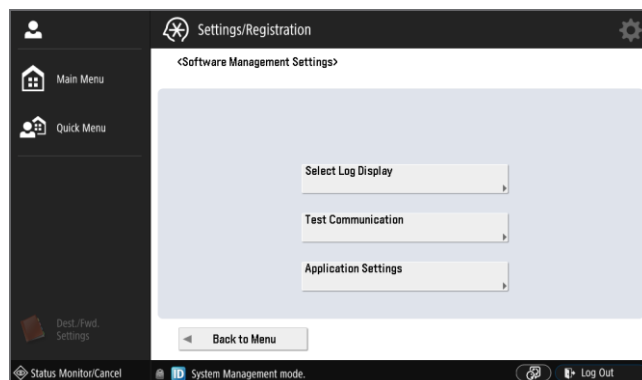
Remote UI

Settings & Registration > Liscense/Other > Register/Update Software > Display Logs/Communication Test



Local UI

Settings and Registration > Management Settings > License/Other > Register/Update Software > Software Management Settings > Test Communication



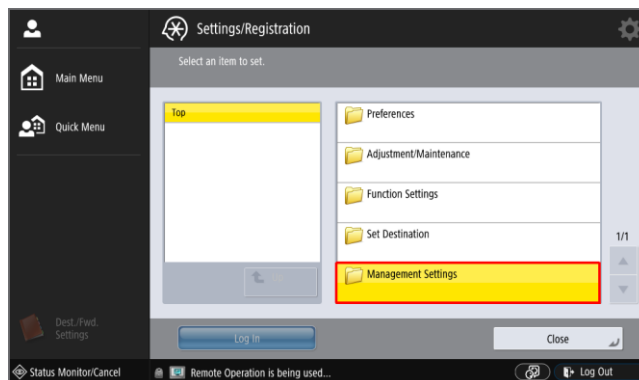
CDS Install From Local UI

Please follow the steps described below:

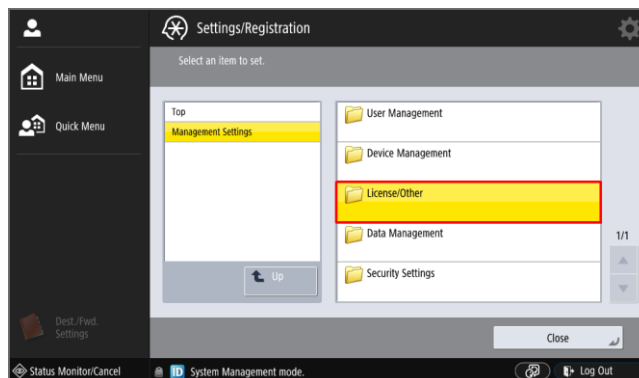
1. From the MFP's touch panel, press **Setting and Registration** and login as system manager (if required).



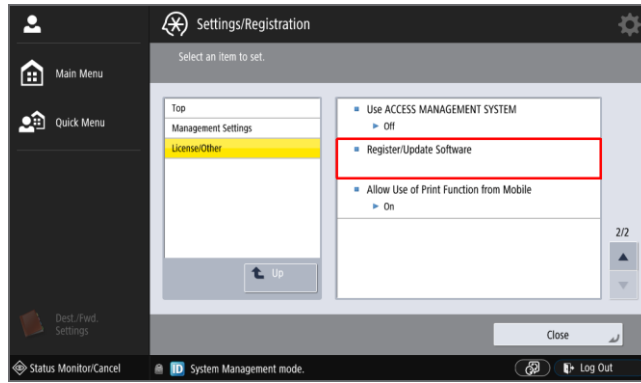
2. From the **Settings/Registration** menu select **Management Settings**.



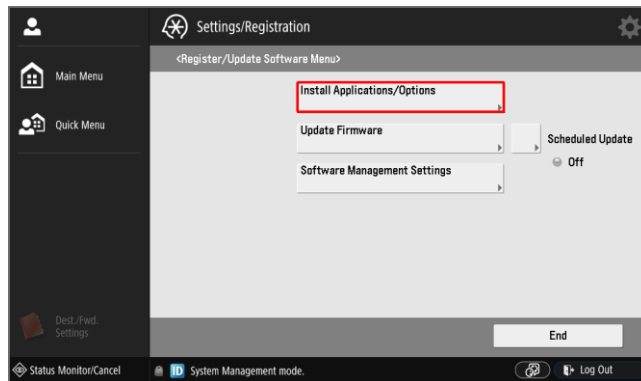
3. Select **License/Other**.



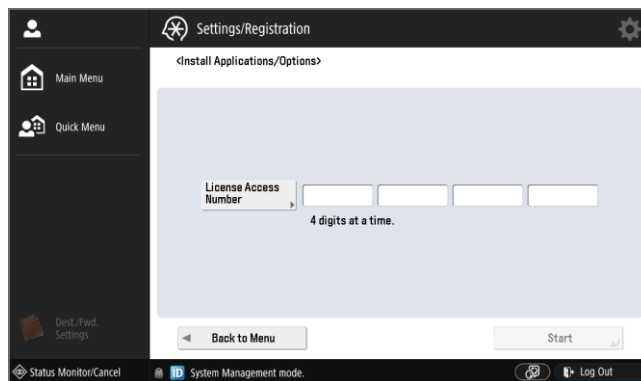
4. Select **Register/Update Software**.



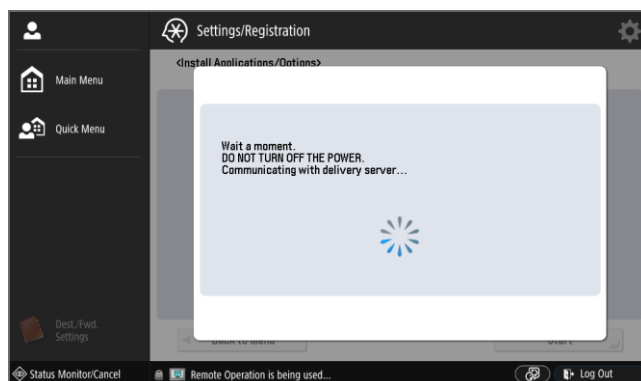
5. Click **Install Applications/Options**.



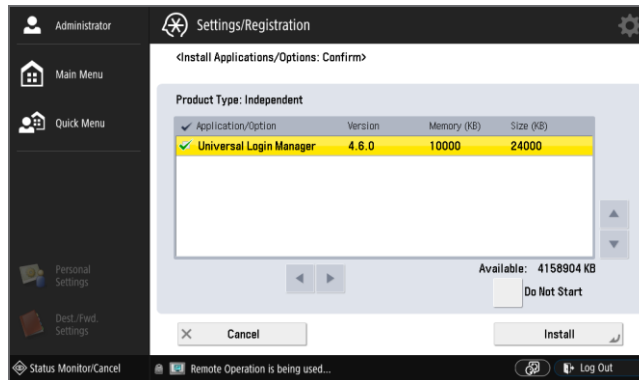
6. Enter the sixteen-digit LAN. Each set of four digits must be entered separately:
Please find the LAN for your version of ULM here (<https://link.nt-ware.net/id250>).



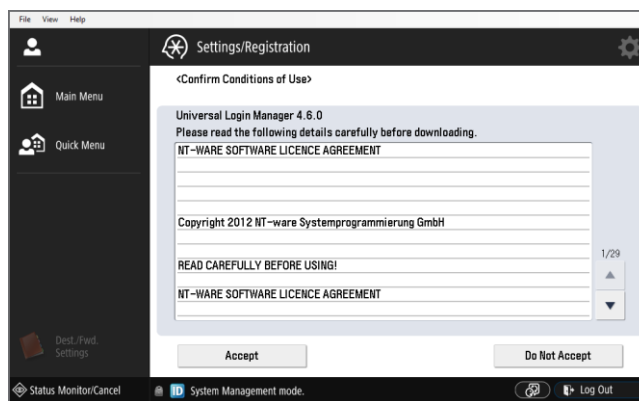
7. Click on **Start** to start the installation process.



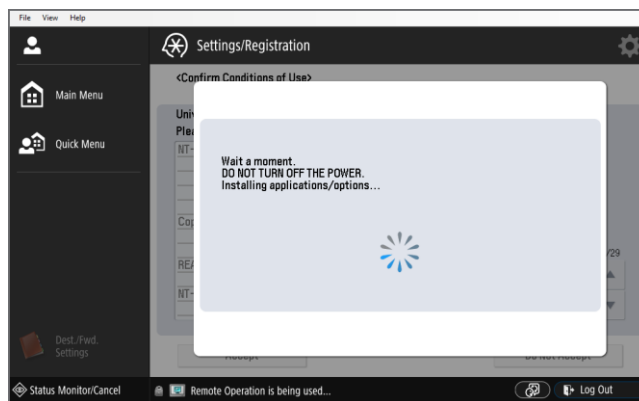
8. Select Universal Login Manager by checking the box in the first column. Also ensure that the **Do Not Start** button is NOT selected.



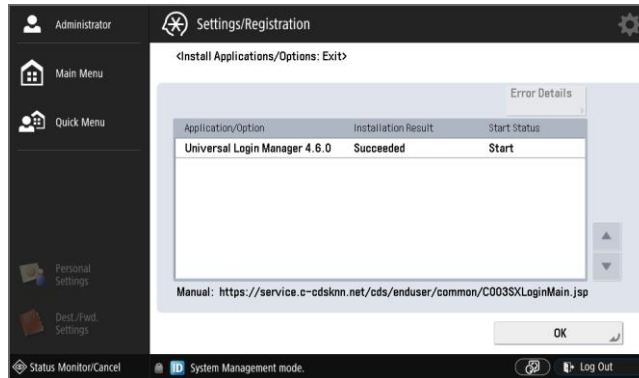
9. Read and accept the license agreement. If you cannot comply with the terms of the license agreement you must not continue with the installation.



10. The application will download and install.



11. When the application has finished installing, a new screen will appear prompting the user to complete the installation. Click the **OK** button on this screen to complete the installation.



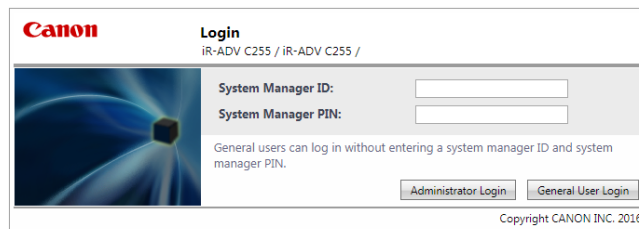
12. Restart the device.



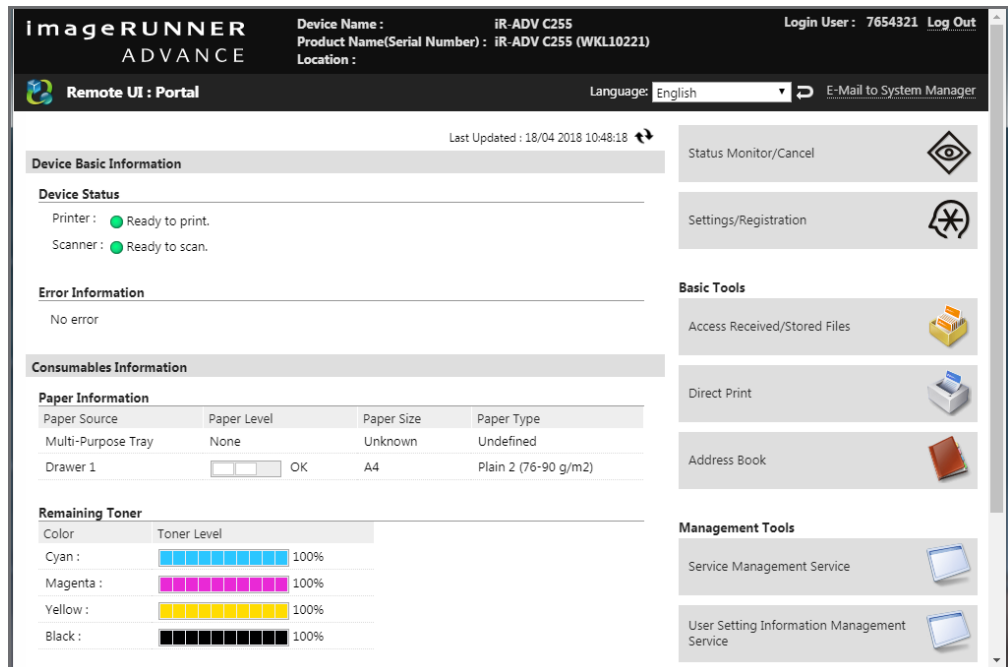
Note that restarting the device automatically starts ULM. You will be locked out from the device until ULM is activated.

5.2 Installation via Content Delivery System (Remote UI)

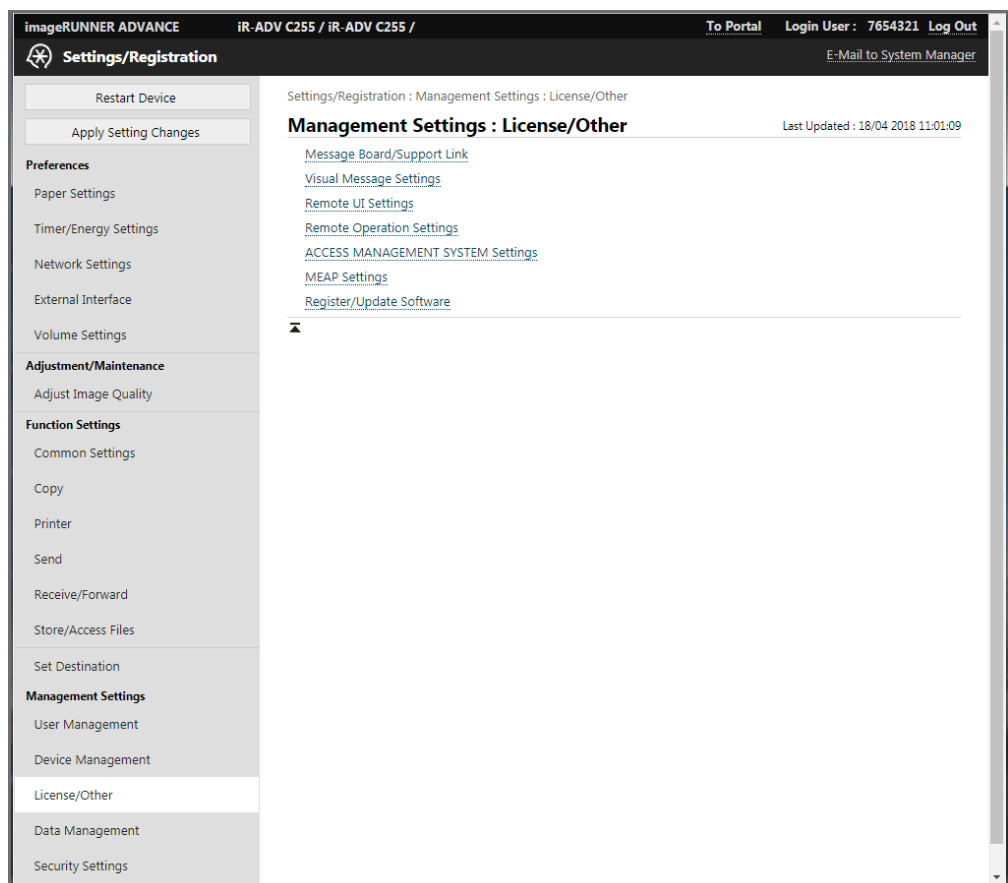
1. Please follow the steps below:
2. Open your web browser and login to the remote UI by entering the URL:
http://<ipaddress>:8000
where <ipaddress> is the IP address of the device on which you wish the Universal Login Manager to be installed.
 - o Enter the administrator login and password and click on **Administrator Login**.



- Once logged in as administrator, you are presented with following screen.

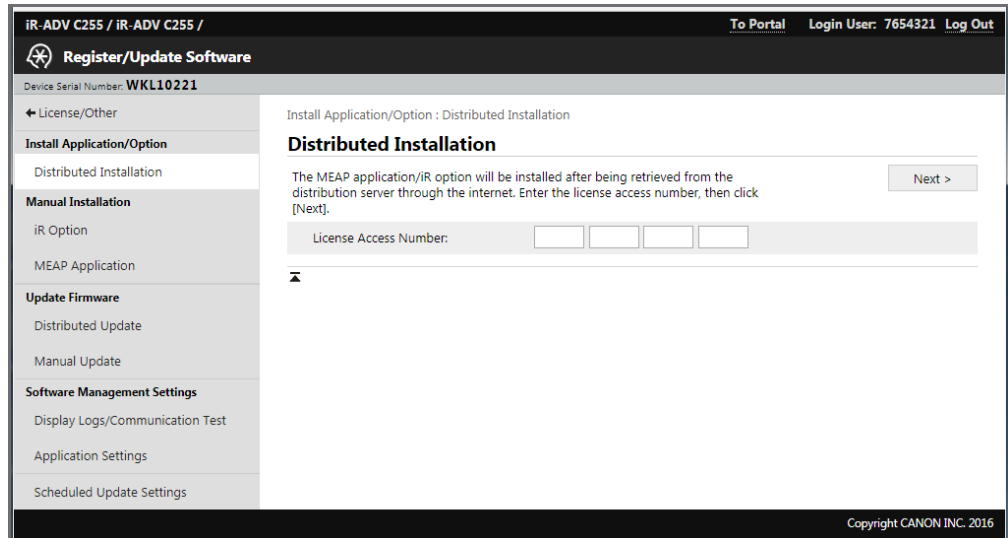


- Open the **Settings/Registration** menu and select **Management Settings > License/Other > Register/Update Software**.

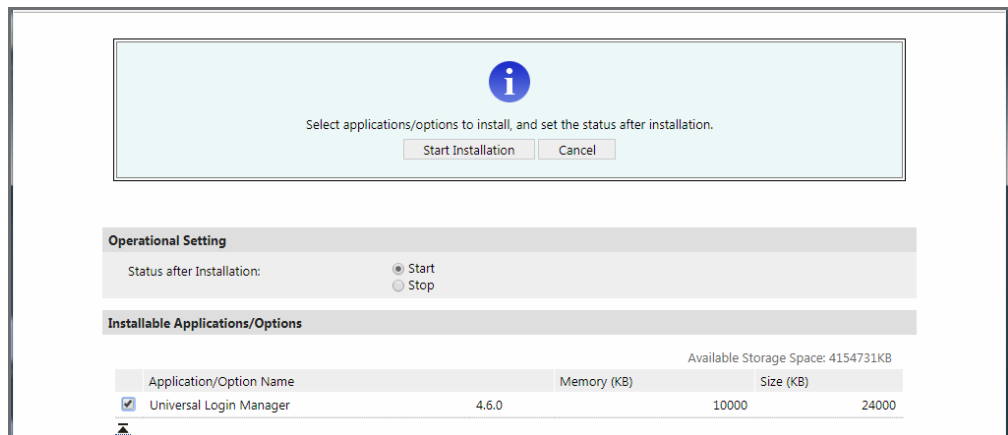


- Enter the sixteen-digit License Access Number (LAN) and click **Next**.

Please find the LAN for your version of ULM here (<https://link.nt-ware.net/id250>).



6. Select the **Universal Login Manager** by checking the box in the first column. Also ensure that the **Start** radio button is selected, if you do not want to start the Universal Login Manager immediately (needs restart of the device). Click **Start Installation** to begin with the installation process.



7. Read and accept the license agreement.
8. The application will be downloaded and installed.
9. Afterwards, click **To Distributed Installation**.
10. Restart the device.



Note that restarting the device automatically starts ULM. You will be locked out from the device until ULM is activated.

5.3 Manual Installation via Remote UI

Manual installation does not require an internet connection for the imageRUNNER ADVANCE. You can use your networked PC to install the Universal Login Manager with a web browser.

SMS - Service Management Service

SMS (Service Management Service) is a servlet that enables you to access imageRUNNER ADVANCE devices via a network from a web browser and install or manage MEAP applications. In order to install the Universal Login Manager via SMS, you must have the Universal Login Manager application file (.jar) and the license file (.lic) on a file system accessible from your PC.

You can download the Universal Login Manager .jar file and the .lic file from the uniFLOW Embedded Applet for MEAP (<https://link.nt-ware.net/id250>) download page.

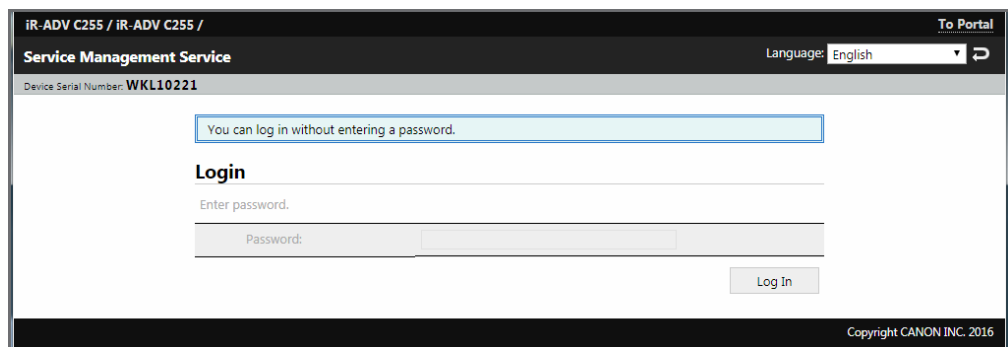
For installation via SMS follow the steps below:

1. Log in to the Service Management System (SMS).

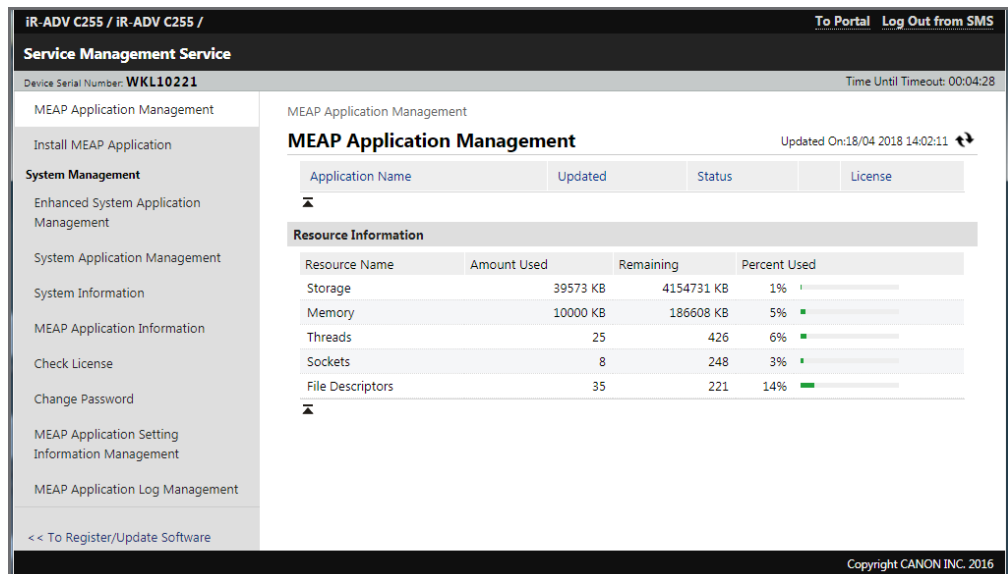
Open your web browser and login to SMS by entering the following URL:

http://<IP-address>:8000/sms

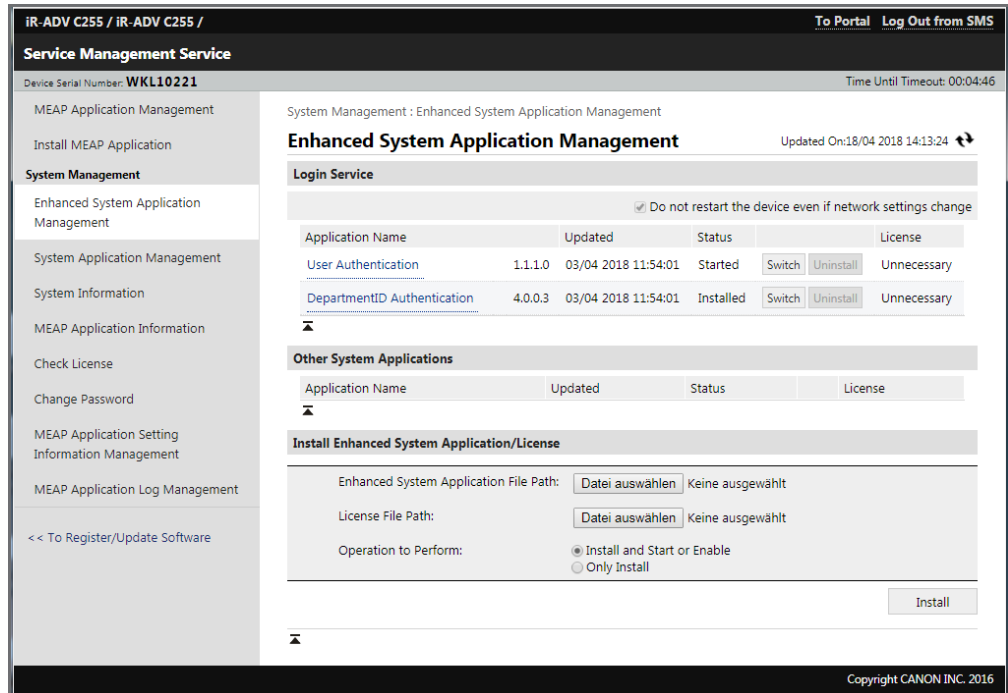
where <IP-address> is the IP address of the device on which you wish Universal Login Manager to be installed.



2. Enter the appropriate password (if required) in the *Password* field.
3. Click the *Log In* button to login to SMS.



4. Select **Enhanced System Application Management**.



On the **Enhanced System Application Management** list page, the status and other details of the enhanced system applications installed on the machine are displayed. You can also add new applications or stop applications from this screen.

5. Under Install **Enhanced System Application File Path**, select the Universal Login Manager .jar file (application).
6. Under Install **License File Path**, select the Universal Login Manager .lic file (license).
7. Under **Operation to Perform**, select **Install and Start or Enable**.
8. Click **Install**.
9. After a check, a confirmation window is displayed. Confirm this windows with **Yes**.
10. Restart the machine.



Note that restarting the device automatically starts ULM. You will be locked out from the device until ULM is activated.

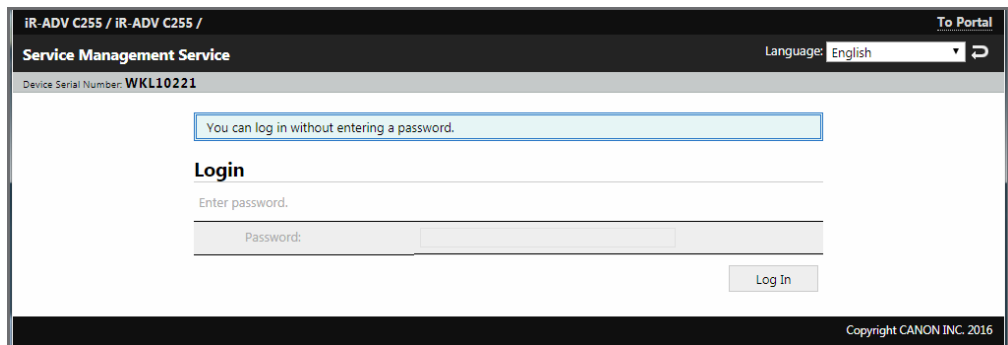
6 Update

To update an existing uniFLOW Universal Login Manager start a new installation process with the new version. Follow the instructions in the chapter Installation (on page 9).

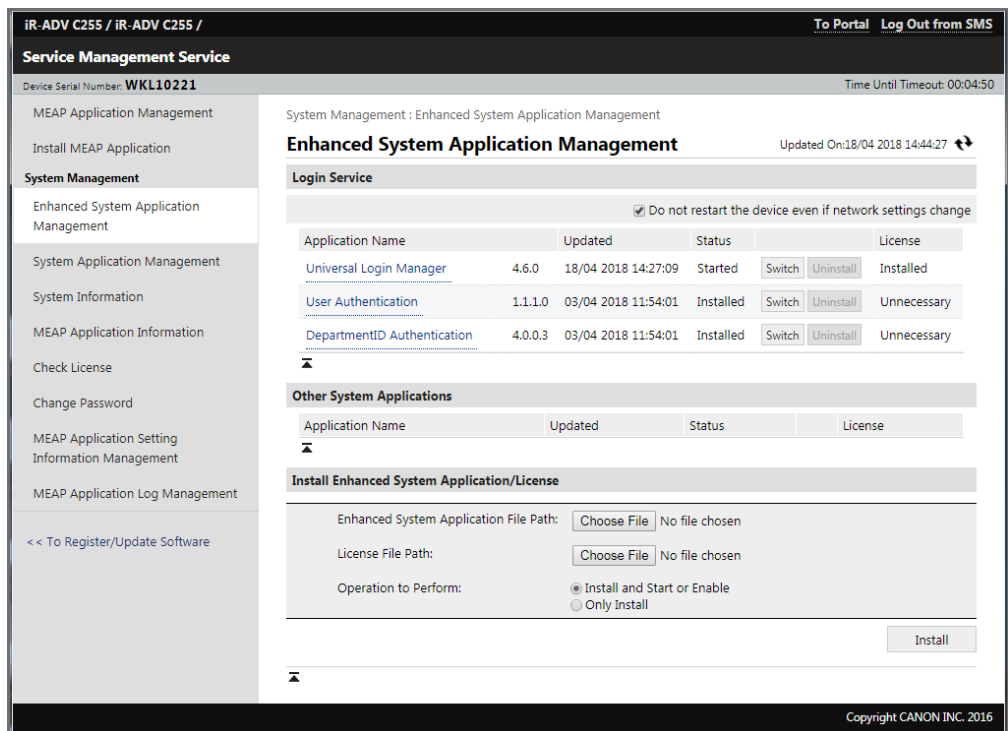
7 Uninstallation

Please follow these steps to uninstall the Universal Login Manager via the Service Management System (SMS):

1. Log in to the Service Management System (SMS).
 Open your web browser and login to SMS by entering the following URL:
http://<IP-address>:8000/sms
 where <IP-address> is the IP address of the device on which you wish Universal Login Manager to be installed.

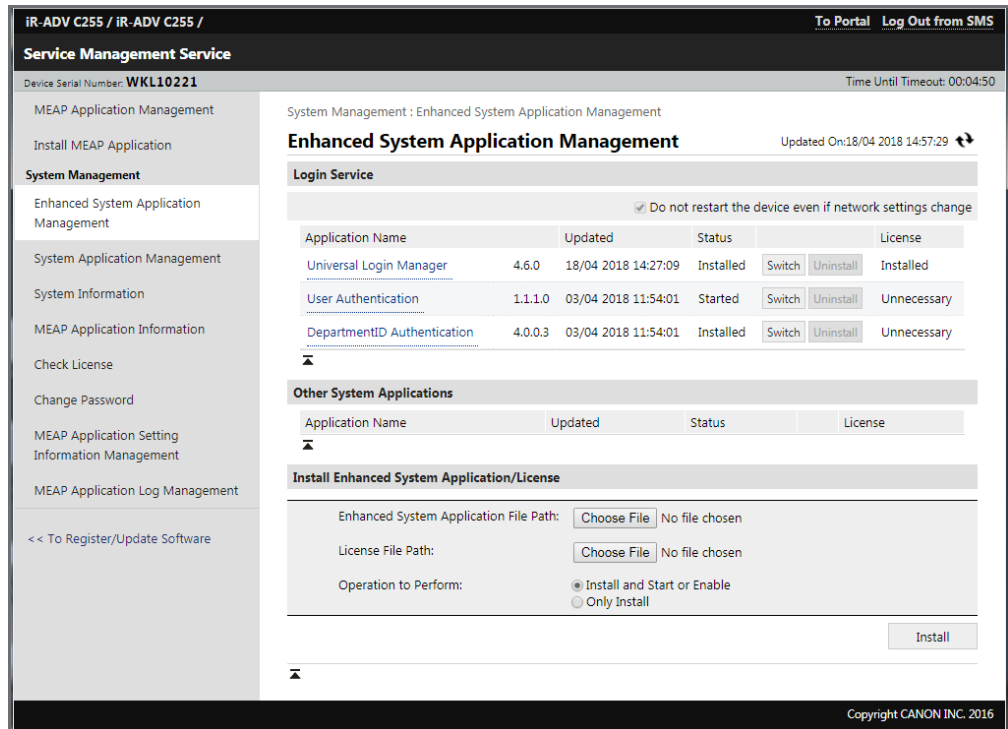


2. Enter the appropriate password (if required) in the *Password* field.
3. Click the *Log In* button to login to SMS.
4. Select *Enhanced System Application Management*.
 On the *Enhanced System Application Management* list page, the status and other details of the enhanced system applications installed on the machine are displayed. You can also add new applications or stop applications from this screen.



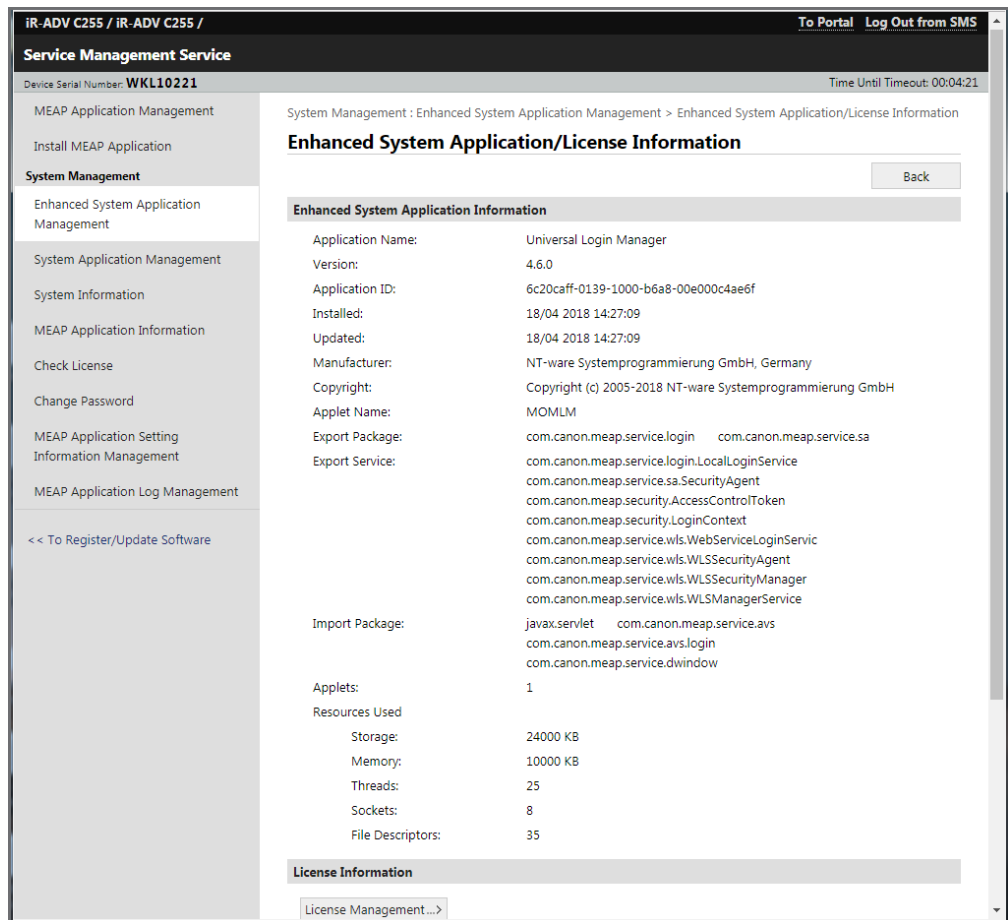
5. Activate a different application, for instance *User Authentication*, by clicking on *Switch*.

6. Restart the machine.
This stops the *Universal Login Manager* application and starts the selected application.
7. After a restart of the machine, login again by performing steps 1-3 and go to *Enhanced System Application Management*.

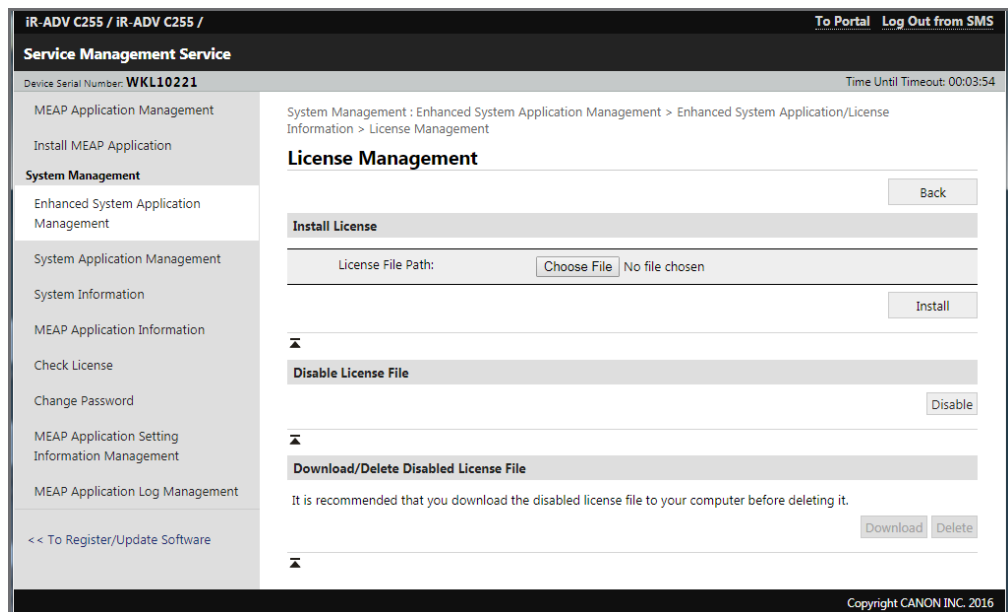


8. Click on the application name *Universal Login Manager*.

- In the *Enhanced System Application/License Information* screen, click *License Management...*

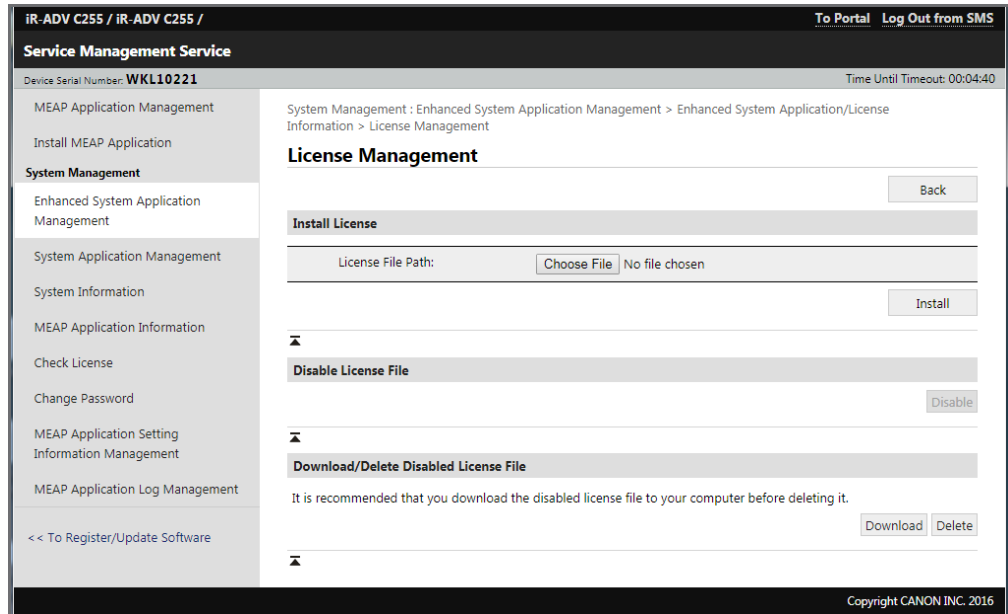


- In the *Disable License File* section, click *Disable*.

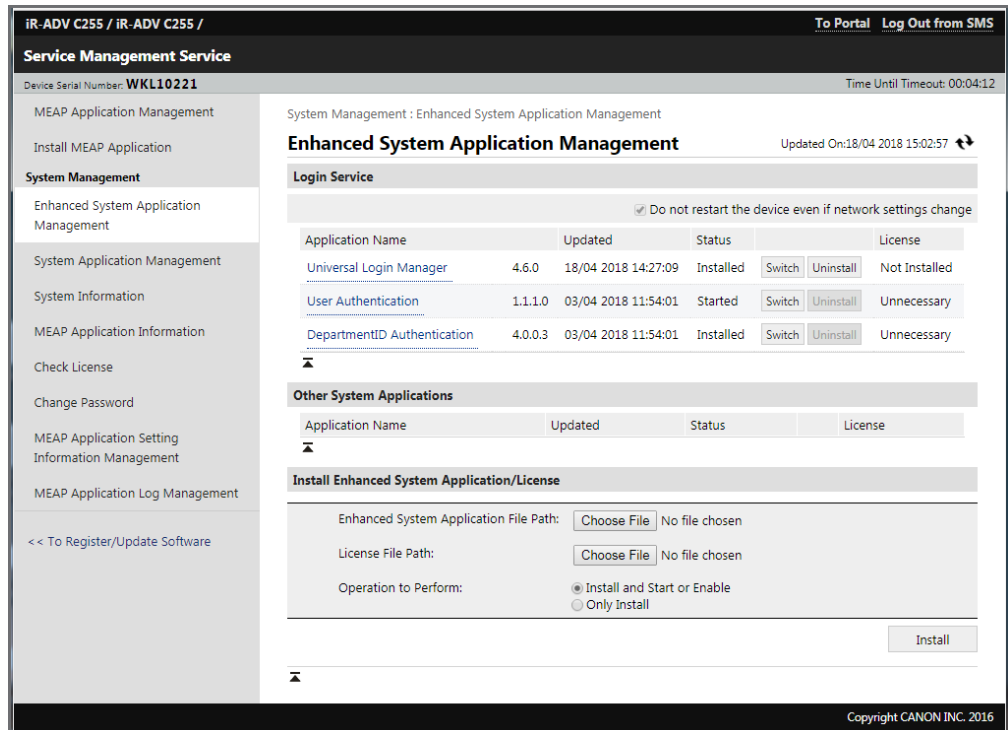


- Confirm disabling the license file in the next window.

- In the **Download/Delete Disabled License File** section, click **Delete**.



- Confirm deleting the license file in the next window.
- Go to **Enhanced System Application Management**.
- Click **Uninstall** for the **Universal Login Manager** application.



- Confirm uninstalling the Universal Login Manager in the next window.

The Universal Login Manager is now uninstalled and application is deleted from the list.

8 Configuration

Various parameters and settings can be configured by the administrator using the Universal Login Manager RUI.

- Users and their profiles including passwords, images or home folders.
- Authentication Providers such as **Active Directory**, **Local** or **uniFLOW**.
- Authentication Presentation methods such as **Image Login** or **User Name/Password**.
- **Export/Import** of the local database.
- **Roles** and their access rights.
- Customization of the user interface.



Language Settings

The Universal Login Manager RUI is always shown in the same language as the Universal Login Manager UI on the device.

The Universal Login Manager UI language on the device can be changed by changing the display language of the device.

8.1 Administration Tool Login

Universal Login Manager hosts its own website. You can directly login to the Universal Login Manager Administration Tool via the following address:

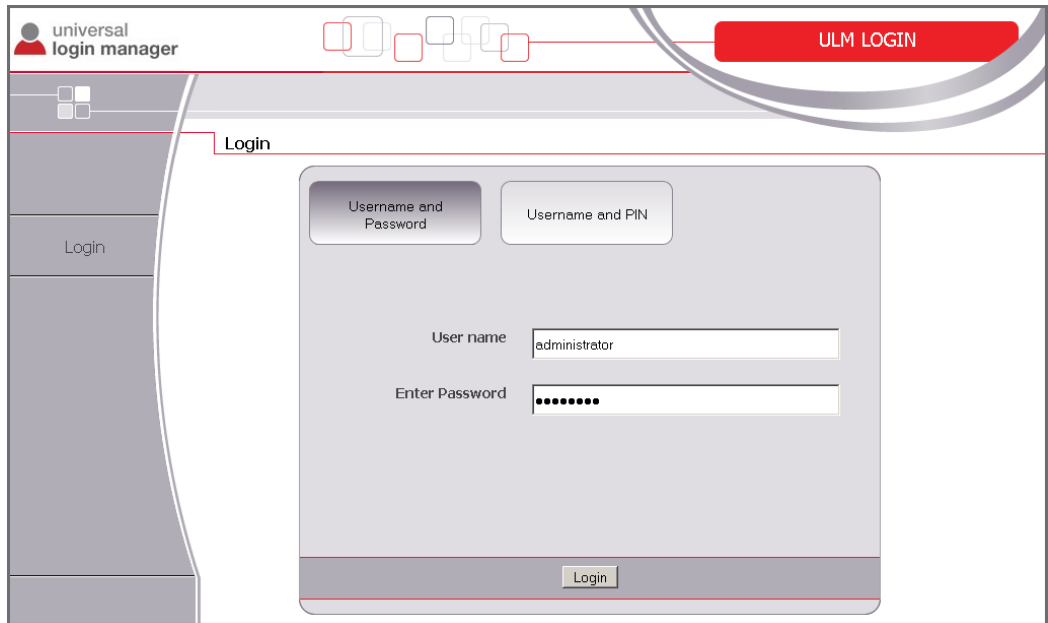
ULM for MEAP devices: `http://<IPaddress>:8000/ulm`

Here you can log in as administrator with the appropriate password. The default password for the user "administrator" is "password". The password can be changed on the **Profile** page of the Universal Login Manager.



If you connect ULM to uniFLOW 2020 LTS / uniFLOW Online 2020.1 or newer versions, the default RUI password automatically changes upon connection of the device. The new RUI password can then be viewed and changed under the security settings of uniFLOW / uniFLOW Online.

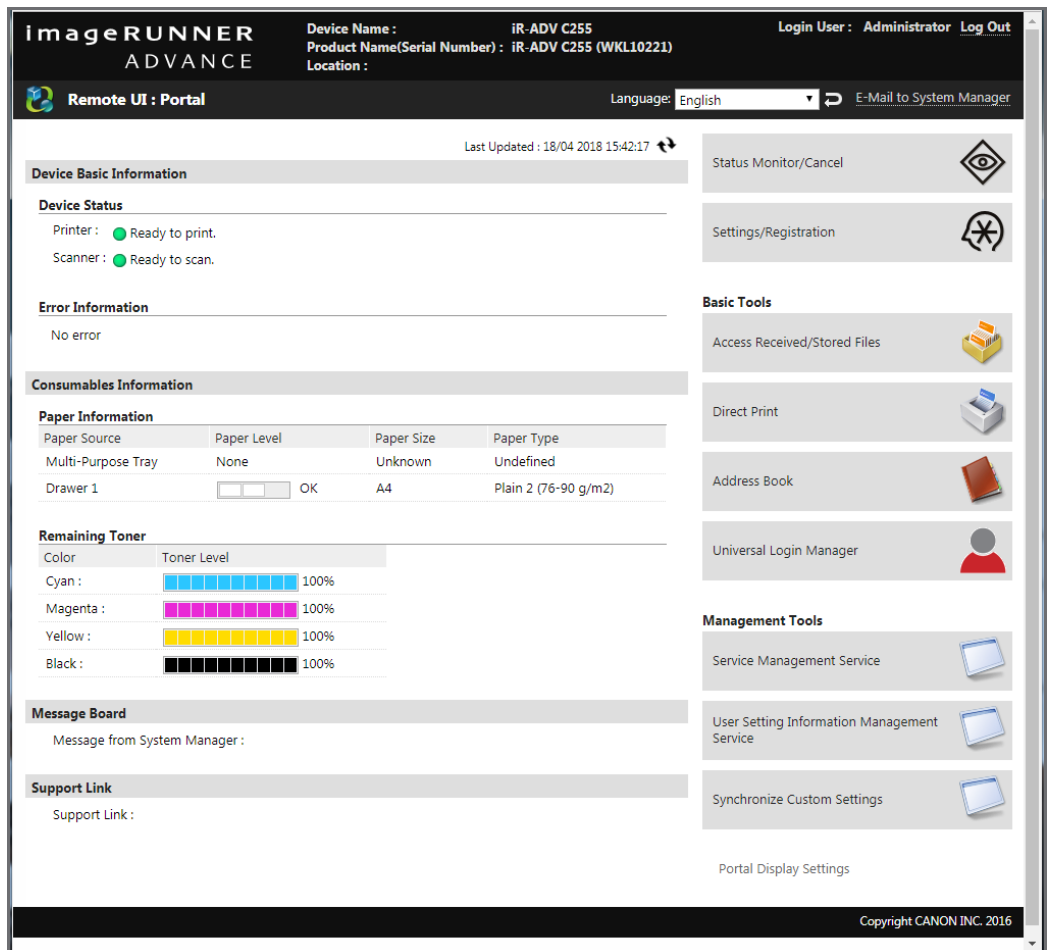
Refer to the corresponding user manual for more information.



Alternatively, the website is available through the remote UI of the imageRUNNER ADVANCE devices. The RUI can be opened in your web browser by entering the following URL:

http://<IP-address>:8000

After logging in, you can find Universal Login Manager under **Basic Tools** on the right hand side of the screen.

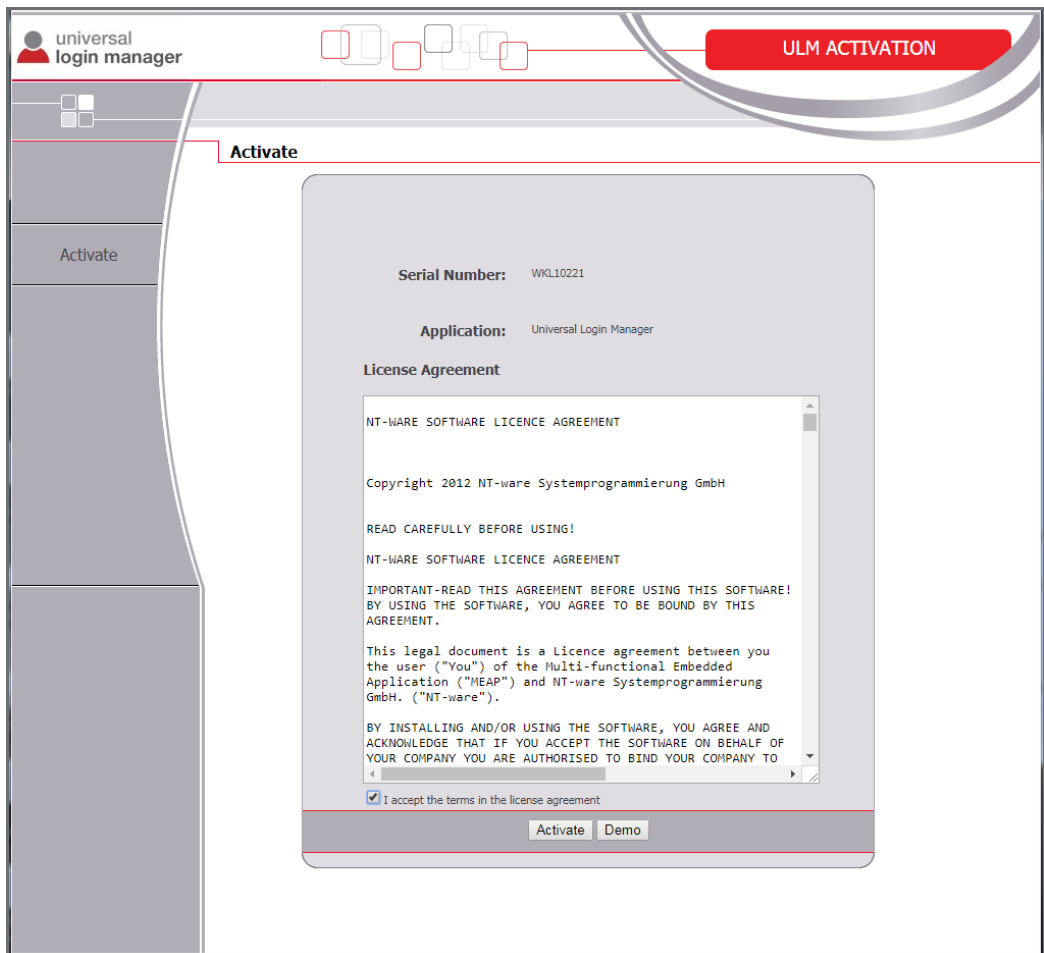


8.1.1 Activation

If this is the first time Universal Login Manager is started, it has to be activated. In order to do so, the computer from which you access your device needs to be connected to the internet.

1. Check *I accept the terms in the license agreement*.
2. Press the **Activate** button.

The **Demo** button only activates the Universal Login Manager until the device is restarted. This is for testing purposes only.

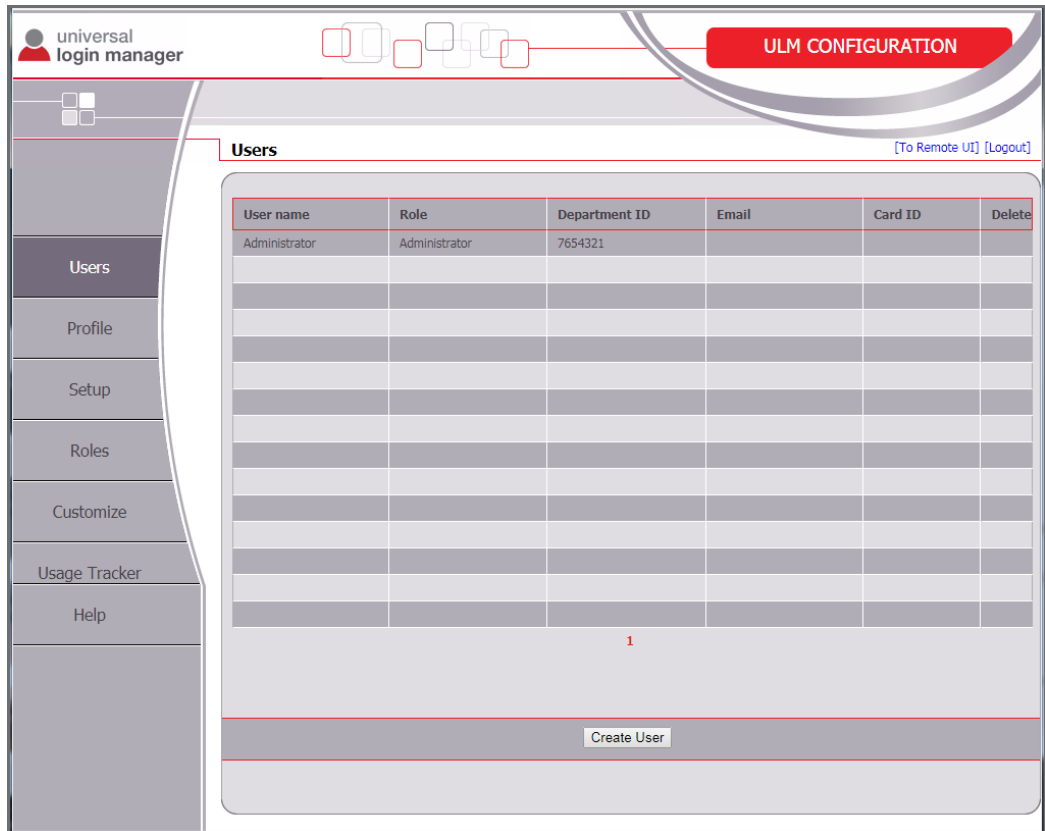


8.1.2 Main Page

When entering Universal Login Manager you will see the main menu, comprising the following items:

• Users	For Local Authentication mode only.
• Profile	User details of the currently logged in user.

• Setup	Authentication mode, Login Type, Import/Export.
• Roles	For AMS function settings.
• Customize	UI Screen Customization.
• Usage Tracker	Link to the ULM Usage Tracker.
• Help	Link to the Online Help.



The submenus will be described in the following chapters.

8.2 Users

On the *Users* screen, a list of the users currently registered on the device can be found. Here a user can be created, deleted or modified.

Clicking on either the *Create User* button or on an existing user opens the user properties.

Login name	Role	Department ID	Email	Card ID	Delete
Administrator	Administrator	0			
NorbertB	PowerUser				✕
PaulS	PowerUser				✕



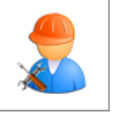

Create User
✕

Role

PowerUser
 Reporter
 FunctionLevelLogin
 Administrator
 Guest

List of ID images
 Here you can choose your ID image or you can upload new images. The recommended width and height is: 75x75 pixels. The allowed image formats are: JPEG, PNG and GIF.

Available images

The table below specifies the fields that can be changed here:

Field	Description	Setting Conditions
User name	Login name of the account	Unique name consisting of up to 32 characters excluding the following characters: SPACE (\ / : * ? < > [] ; , = + @ ") . The user name is not case sensitive.
Enter PIN / Confirm PIN	The PIN code used with Simple ID (with or w/o images) or Prox Card ID. Has to be confirmed in the second field.	Can be left blank or a number of up to seven digits. Leading zeros are automatically added, if less than seven digits are entered.
Home Folder	The home folder of the user. Not supported by imageRUNNER ADVANCE Generation 1 devices.	Full path in UNC notation.
Password / Confirm Password	The password used for the authentication presentation of type "username/password". Has to be confirmed in the second field.	

Field	Description	Setting Conditions
Card ID	The card number registered for the user's card.	The format depends on the type of card.
Department ID	The user's department ID.	Depending on the device.
Email	The user's email address.	Any existing email address.
User Display Index	Used to sort the ID images on the login screen. The images are sorted in descending order, so the user with the highest index is listed first.	Any integer number.
Role	The roles that are assigned to the user.	Multiple selection possible.
List of ID images	Graphic representation of the user.	Images can be uploaded and should have a size of 75x75 pixels. Accepted formats are JPG, GIF and PNG. Larger images will be scaled down.



- When configuring Department IDs, please note that although you are able to configure a Department ID in Universal Login Manager, the configuration of a Department ID password is not possible here. For that reason it is unnecessary in this case, to set the password of the Departments IDs on the devices to 0.
- If you select the following roles: Administrator, Reporter, NetworkAdmin, DeviceAdmin the "Department ID" field will be greyed out and "System Manager" will be displayed in it. For these roles, the user will be assigned the system manager department ID.
- ID images should not exceed 500 kb. Larger images can slow down the user interface considerably.
- Users with names that consist only of numbers cannot have custom images as ID image. You can upload an image but only the standard ID image will be shown.

8.2.1 Home Folder

The Home Folder functionality is only available on generation 2 imageRUNNER ADVANCE devices. If a valid folder is entered as **Home Folder** in the user profile, the respective settings for **Scan and Send** on the device are automatically populated.

Depending on the authentication provider and authentication mode, the settings on the device vary slightly.

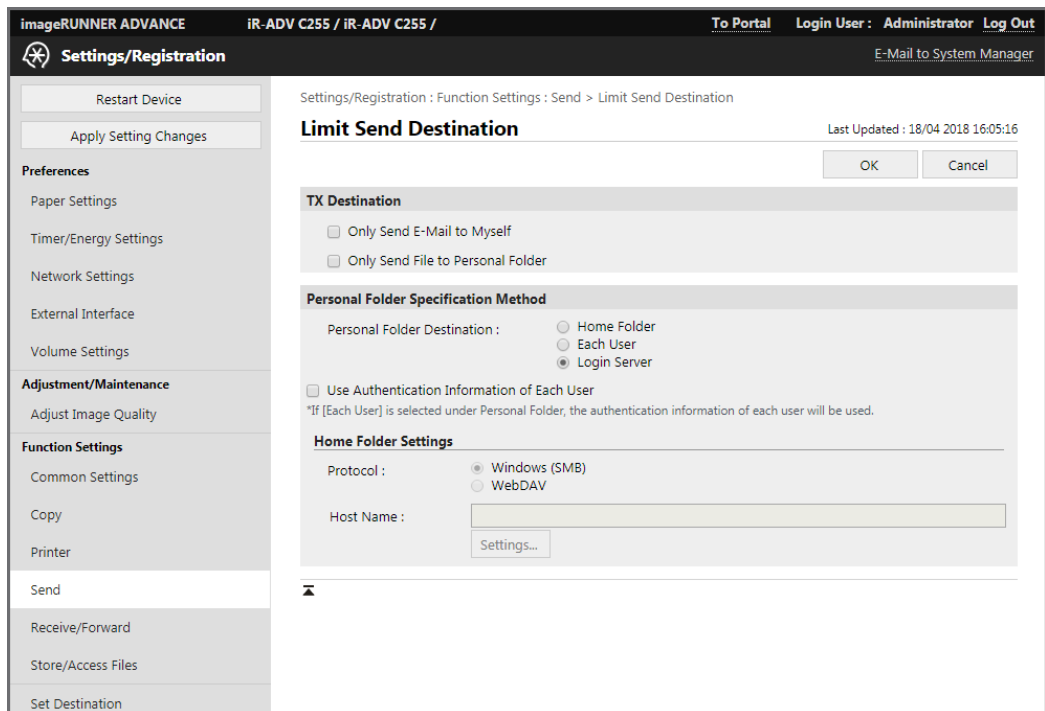
If **Active Directory** is used as the authentication provider **with user name/password login type**, the user credentials are automatically filled in every time the function is used.

- Log in to the device as system manager and go to **Settings/Registration : Function Settings : Send > Limit Send Destination**
In the section **Personal Folder Specification Method** select **Login Server**.
- The setting **Use Authentication Information of each User** influences how the credentials are handled:
 - If **active**, the credentials have to be entered manually for the first time of use, after that they are permanently stored on the device. The next time the credentials will be filled in automatically.
 - If **inactive**, the credentials are automatically filled in by the Universal Login Manager.

If **Active Directory without user name/password login type** or **Local Database** is used as the authentication provider, the user credentials have to be entered at the first use, but can be stored permanently on the device. See section *Home Folder settings on the device* below.

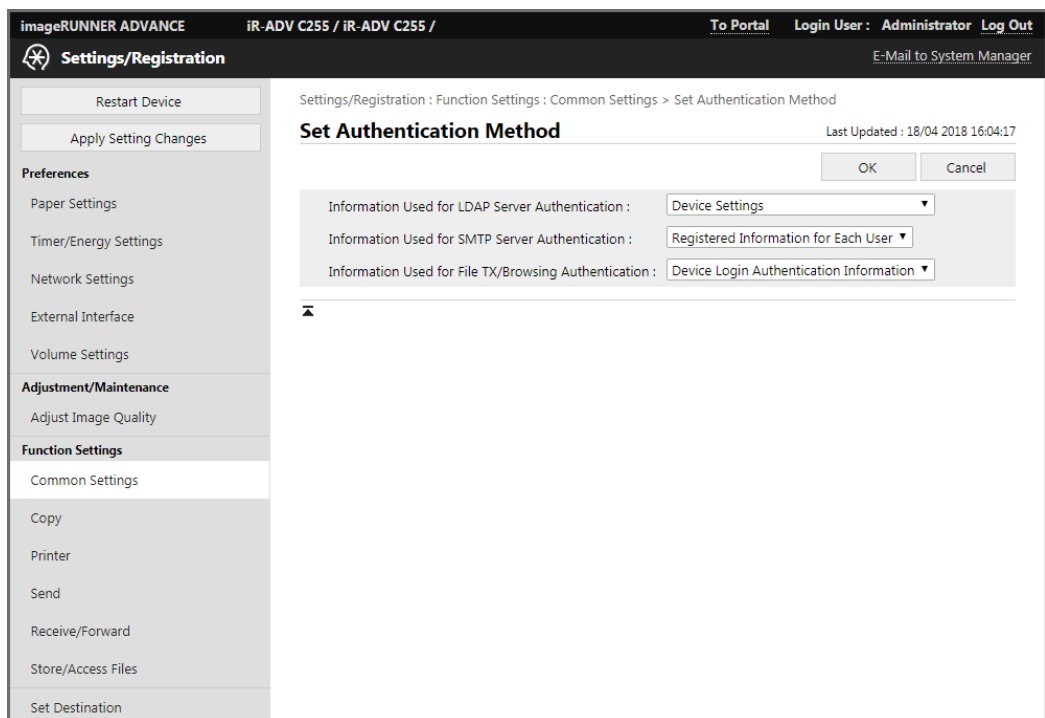
- Log in to the device as system manager and go to **Settings/Registration : Function Settings : Send > Limit Send Destination**
In the section **Personal Folder Specification Method** select **Login Server**.
- The setting **Use Authentication Information of each User** influences how the credentials are handled:
 - If **active**, the credentials have to be entered manually only for the first time of use, after that they are permanently stored on the device. The next time the credentials will be filled in automatically.
 - If **inactive**, the credentials are never filled in by the Universal Login Manager. The user credentials have to be entered manually for each use.

Press **OK**. Now the home folder function is ready to use.



Following this, open the following page: **Settings/Registration : Function Settings : Common Settings > Set Authentication Method**

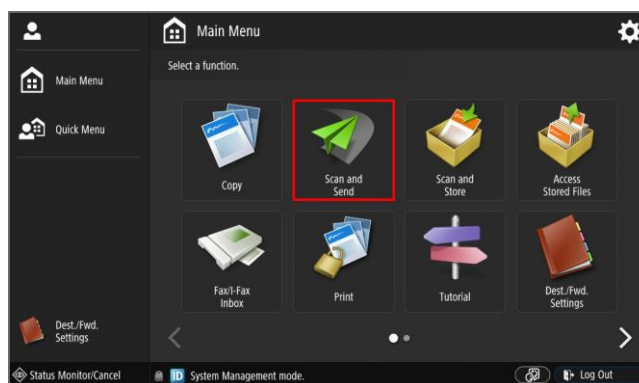
From the drop-down menu *Information Used for File TX/Browsing Authentication* select *Device Login Authentication Information*.



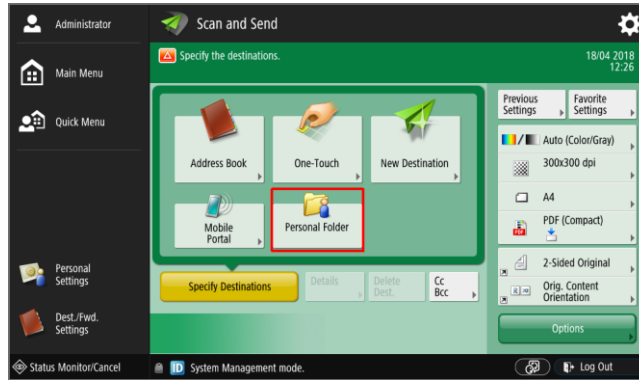
8.2.2 Home Folder Settings

If the Authentication Provider is *Local Database*, users have to do the following once on every device they want to use with their accounts.

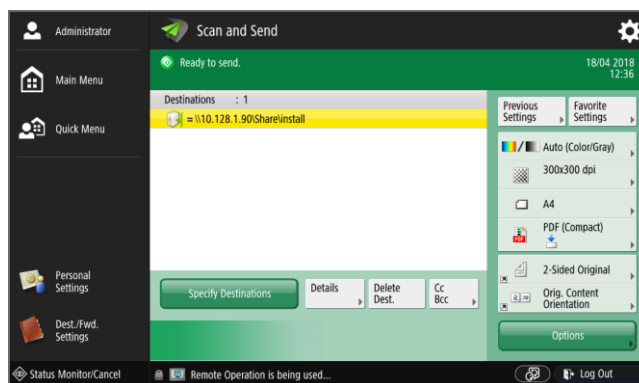
1. After logging in the user opens *Scan and Send*.



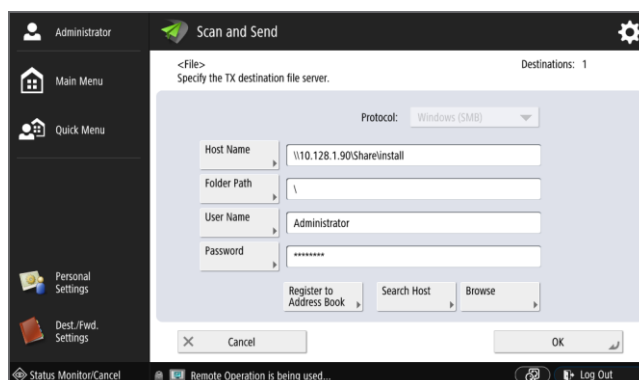
- Here the user opens the **Personal Folder** settings.



- The home folder from the ULM settings should be displayed as shown in the following screenshot.



- After tapping on **Details**, the detailed settings are displayed. **Host Name** and **Folder Path** should be preset. The user has to fill in **User Name** and **Password** and tap on **Store Password**, then on **OK**. From now on the settings are saved on the device and are ready for future use.



8.3 Profile

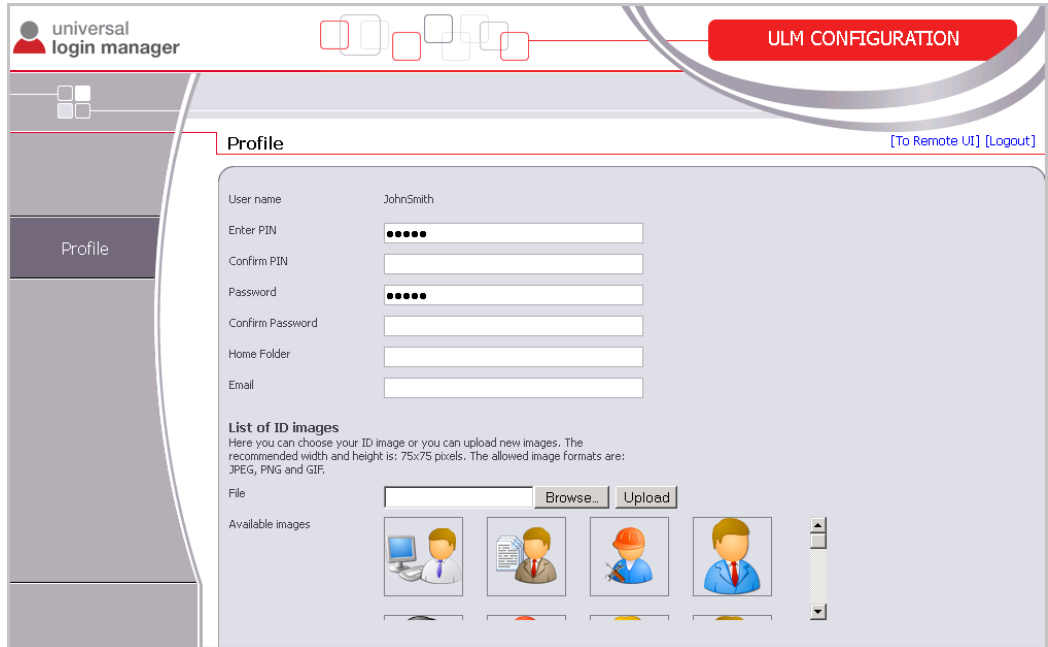
On the **Profile** screen end users can change a subset of their user properties:

- PIN
- Password
- Home Folder
- Email
- ID image



This feature is not available if Active Directory authentication is activated.

The user has to login on the device RUI and has to open the *Profile* page. For further details see chapter Users (on page 26).



8.4 Setup

The *Setup* page provides the Administrator with an easy way to configure the following features:

- *Login Type* (on page 33)
- *Authentication Mode* (on page 36)
- *Import/Export* (on page 41) of the user database

- **System Manager Settings** (on page [43](#))

8.4.1 Login Type

In this section the Authentication Presentation can be selected. The following types are available:

- Image Login
- Image Login + PIN
- Proximity Card
- Proximity Card + PIN
- User Name / Password

8.4.1.1 Image Login and Image Login + PIN

Image Login

Image Login provides the user with an easy method of logging in. Login is done by tapping on the associated icon on the device screen. There is no means of authentication here other than the user name assigned to the ID image. No security check is done and anybody with physical access to the printer can log in with any identity.



This login method should only be considered for small offices that are not concerned with security issues or usage tracking.

Image Login + PIN

The **Image Login** type can also be used in conjunction with a PIN code. This PIN code is defined in the User/Profile setup and can contain up to seven digits. Since security is provided here, this login type makes sense for small offices requiring usage tracking and/or access control functionality.

For both login types, up to 48 accounts can be configured. This login method only works with the setting **Authenticate against Local Database**.

Show Admin Image

It is possible to exclude the administrator from the Image Login. That way no user can login with administrative rights via Image Login. Just set the setting **Show Admin Image** to **No**.

Show Login Names

If this is set to **Yes** the user names are shown below the ID image on the ULM login screen. Otherwise, only the ID images are shown.

Login Type <input type="radio"/> Image Login <input checked="" type="radio"/> Image Login + PIN <input type="radio"/> Proximity Card <input type="radio"/> Proximity Card + PIN <input type="radio"/> User Name/Password Show Admin Image: Yes Show Login Names: No	Authentication Mode Authenticate Against: Local Database Configure
Import / Export Export Configuration Database: Export Import Configuration Database: Browse... Import Import user data from CSV file: Browse... Import	System Manager Settings System Manager ID: 7654321 System Manager Password: [masked]

Save

8.4.1.2 Proximity Card and Proximity Card + PIN

The login types *Proximity Card* and *Proximity Card + PIN* provide easy login with a high level of security. Users only have to swipe their cards and - if configured, enter a PIN code for additional security.



The use of a proximity card reader is required for this login type, see Supported Card Readers (on page [67](#)) for a list of all supported card readers.

These login types can be configured for Active Directory as well. With a self-registration process it is very simple to register the card with the authentication provider, such as an Active Directory server. The card number will be registered during the first login with the new card and the administrator does not have to enter any data manually other than user name and password. The following configuration is required for this login type:

- **Card training method**
 - **None:**
Means that the card has to be registered manually by the administrator.
 - **User Name/Password:**
The card is registered by the user authenticating with user name and password.
- **Register PIN Code** (only visible for *Proximity Card + PIN*):
This parameter determines, whether the users can also enter a new PIN code while registering the card. When set to **No**, the administrator has to enter the PIN codes for the users manually; when set to **Yes**, the users can enter the PIN codes themselves.
- **Alternative Login Method:**
For both *Proximity Card Login* types this offers an alternative method of authentication. This can either be **None** or **User Name/Password**. In the latter case, a user can alternatively login without a card.

How to register a new card

1. The user swipes the new card.
2. The user enters user name and password for authentication.
3. If so configured the user enters the new PIN code.
4. The card number is now associated with the user and is stored in the database.

Local Authentication Mode as well as Domain Authentication Mode are supported. The number of users for *Proximity Card Login* is unlimited. Since uniFLOW also supports MiCard readers, a migration to uniFLOW is easy to accomplish.



To automatically store the new card number in Active Directory, users need write access to their Active Directory profile. If this is not available, automatic registration will not be possible and the card number has to be stored manually by the administrator.

The screenshot shows the configuration interface for the Universal Login Manager. It is organized into four quadrants:

- Login Type:** Contains radio buttons for 'Image Login', 'Image Login + PIN', 'Proximity Card', 'Proximity Card + PIN' (selected), and 'User Name/Password'. It also includes dropdown menus for 'Card Training Method' (None), 'Register PIN Code' (No), and 'Alternative Login Method' (None).
- Authentication Mode:** Features a dropdown menu for 'Authenticate Against' set to 'Local Database' and a 'Configure' button.
- Import / Export:** Includes an 'Export' button for the configuration database and two 'Import' buttons, each with a 'Browse...' button, for importing the configuration database and user data from a CSV file.
- System Manager Settings:** Contains text input fields for 'System Manager ID' (7654321) and 'System Manager Password' (masked with dots).

8.4.1.3 User Name / Password

With this method the user has to provide user name and password when logging in to the device. This method is secure and easy to set up but not as convenient as the methods described above.

This method works with all authentication providers.

8.4.2 Authentication Mode

In the **Authentication Mode** section, the administrator can configure how the user data is managed and whether the device is connected to a local uniFLOW server or to the uniFLOW Online cloud service.

If the device is connected to a local uniFLOW server, the user interface and the behaviors are loaded from that uniFLOW server.

If the device is connected to uniFLOW Online, the user interface and the behaviors are loaded from the uniFLOW Online cloud service. In that case, the setting in **Authenticate Against** is irrelevant.

- **Authenticate Against:**

The changes under **Authenticate Against** will be saved automatically after selecting an authentication provider. Clicking on **Save** is not necessary.

This parameter is irrelevant for uniFLOW Online.

- **Active Directory:**

Connect to an Active Directory server. See chapter Active Directory (on page [38](#)) for further details.



Please note that LDAP servers other than Microsoft Active Directory are not supported. In case a different LDAP system is required (e.g. OpenLDAP), please utilize uniFLOW.

- **Local Database:**
Use a local user database on the device.
- **uniFLOW:**
This setting is only relevant, if the device is configured by a uniFLOW server. It is set automatically after a device restart when the uniFLOW configuration is completed.

Connection with uniFLOW Online



The following settings are only visible if the Universal Login Manager is accessed via an SSL connection (HTTPS). This has to be configured in the device settings, see below.

The following settings are only relevant if the device is to be connected to uniFLOW Online.

- **uniFLOW Online URL:**
In this field enter the uniFLOW Online URL. Please note that an *https://* prefix is obligatory in order to connect to uniFLOW Online.
- **Proxy Settings:**
In this section a network proxy can be configured if necessary to connect to the internet. Enter IP or FQDN address and the port. Please note that the connection to uniFLOW Online is not possible without internet access.



Proxy Settings - Username and Password

Please note that username and password settings for proxies with authentication are taken from the device settings on the device itself. Therefore these settings have to be correct.



For further details on connecting devices to uniFLOW Online please refer to the uniFLOW Online Help, section Device Registration.



Enable SSL for MEAP

If SSL is not enabled for MEAP applications on your imageRUNNER ADVANCE printer, please follow these steps:

1. Open the **Remote UI: Portal:**
http://<Device_IP_Address>
2. Open **Settings/Registration.**
3. Under **Management Settings** open **License/Other.**
4. Open **MEAP Settings.**
5. Check **Use SSL.**
6. Click **OK.**
7. Restart the printer.

The next time you log in to the Universal Login Manager, you can use the following URL:

https://<Device_IP_Address>:8443/ulm

8.4.2.1 Active Directory

If **Authenticate Against** is set to **Active Directory**, the **Configure** button can be used to set all necessary parameters for the connection.

The following screenshots show the steps to establish the connection:

1. Enter the server data.

2. Enter authentication data for a user who has reading rights in the Active Directory in order to browse the directory tree. Write access is not necessary here. For **Authentication Method**, the following methods can be selected: **NTLM**, **Kerberos** and **Active Directory**. The steps described below are identical for each of them.

User Name Entry

The domain setting in the LDAP configuration has to match the domain provided by the AMS printer driver add-in. In case the AMS driver add-in always has an uppercase domain, the LDAP config should be done with uppercase domain as well.



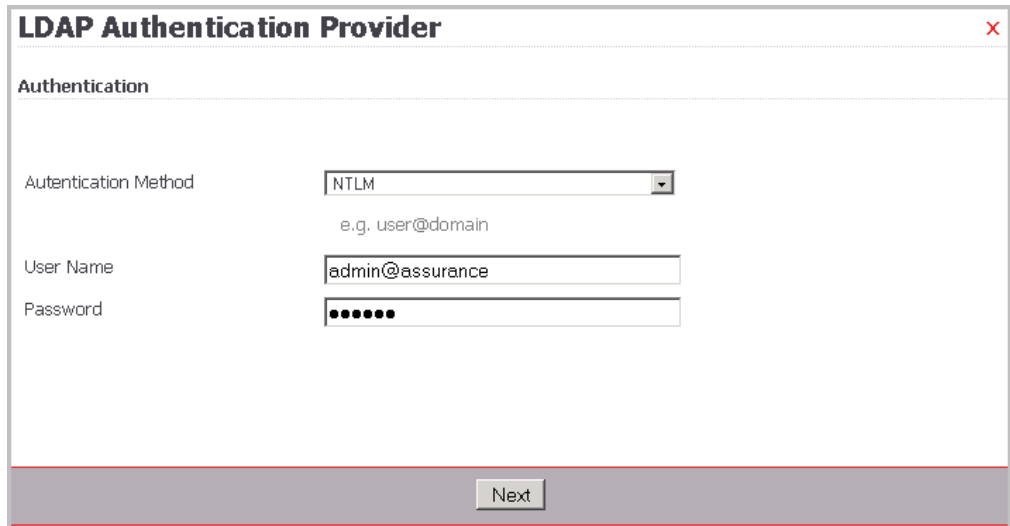
Example:

Active Directory domain name: *example.co.jp*

NetBIOS domain name: *EXAMPLEDOM*

User name: *user01*

The user name *user01@EXAMPLEDOM* must be entered in the **Authentication** window.



LDAP Authentication Provider [Close]

Authentication

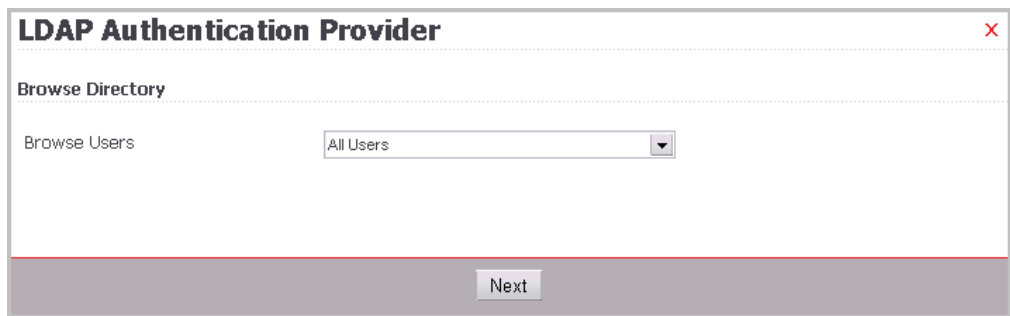
Authentication Method: [v]
e.g. user@domain

User Name:

Password:

[Next]

- 3. Select how the directory tree is browsed. Select *All Users*.



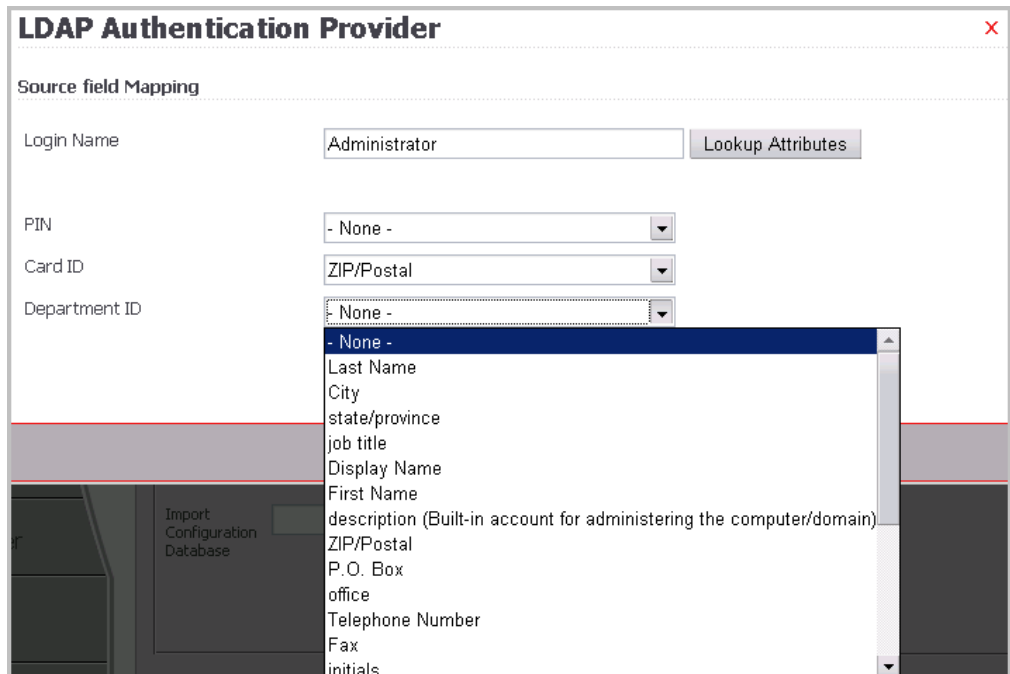
LDAP Authentication Provider [Close]

Browse Directory

Browse Users: [v]

[Next]

- 4. Now you can simply map existing attributes to the user's profile. Press *Save + Close* to finish the process.



LDAP Authentication Provider [Close]

Source field Mapping

Login Name: [Lookup Attributes]

PIN: [v]

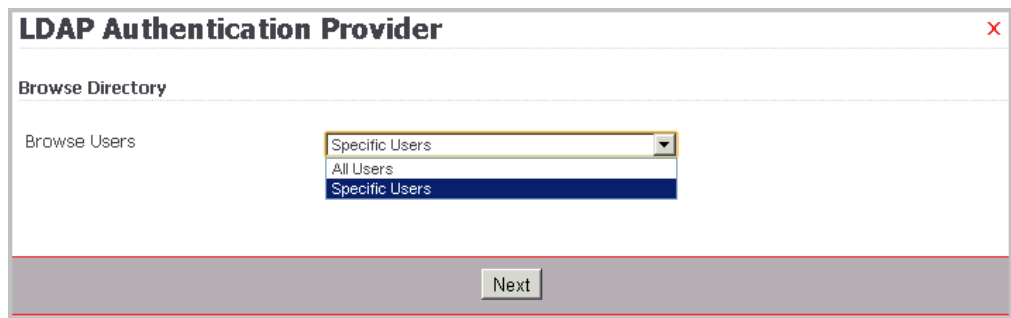
Card ID: [v]

Department ID: [v]

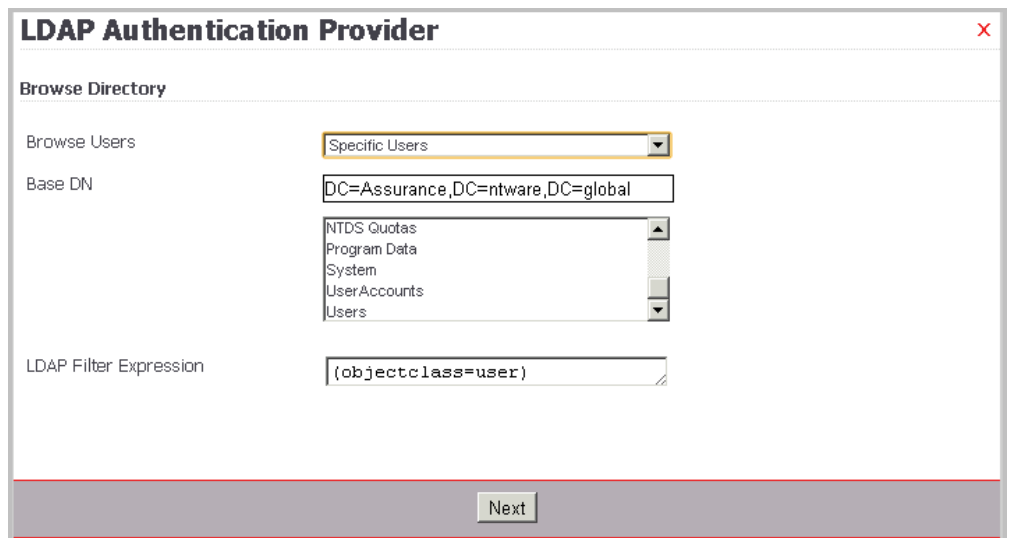
[v] - None -
Last Name
City
state/province
job title
Display Name
First Name
description (Built-in account for administering the computer/domain)
ZIP/Postal
P.O. Box
office
Telephone Number
Fax
initials

Import Configuration Database

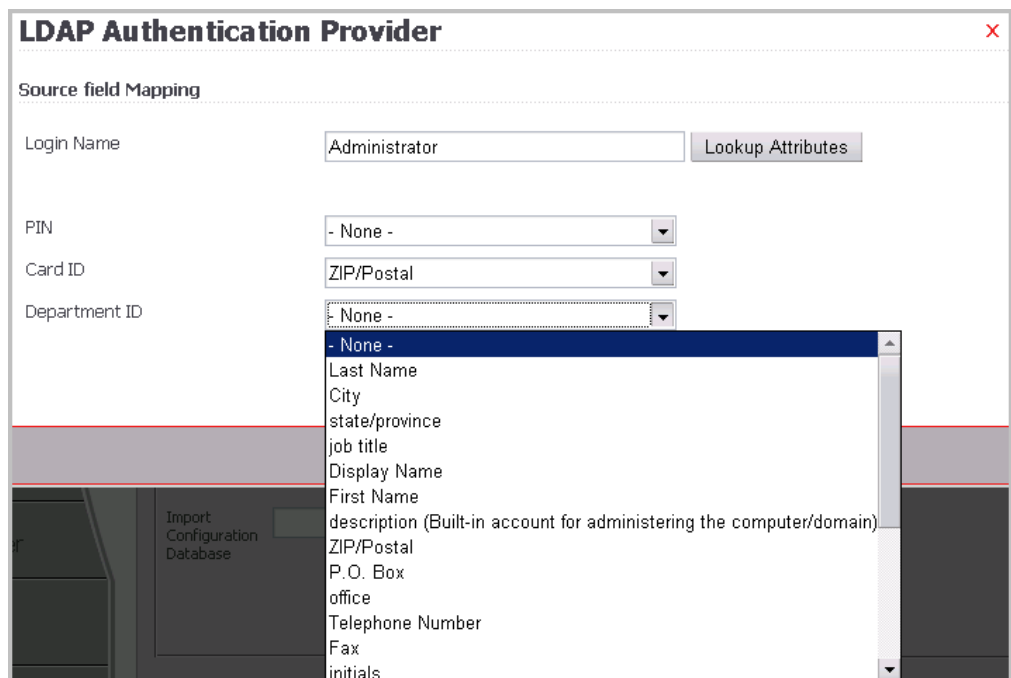
- Alternatively select *Specific Users* in one of the previous steps to enable detailed browsing of the directory tree.



- Browse and select the directory.



- Select the field mapping.



After stepping through all configuration screens your connection is ready to use.



- For the Active Directory, only read rights are required, except for changes that are made by users in their own profiles. Therefore the users need write access on their own Active Directory profiles.
- This is also important for card training purposes, where the users can change their saved card numbers by associating their cards to their profiles by entering their credentials.

8.4.3 Import/Export

The administrator can export and import the Universal Login Manager configuration along with the user configuration. This can be done on the *Setup (on page 32)* screen. All system data including background images, icons, user data etc. will be saved. This works with all database types.

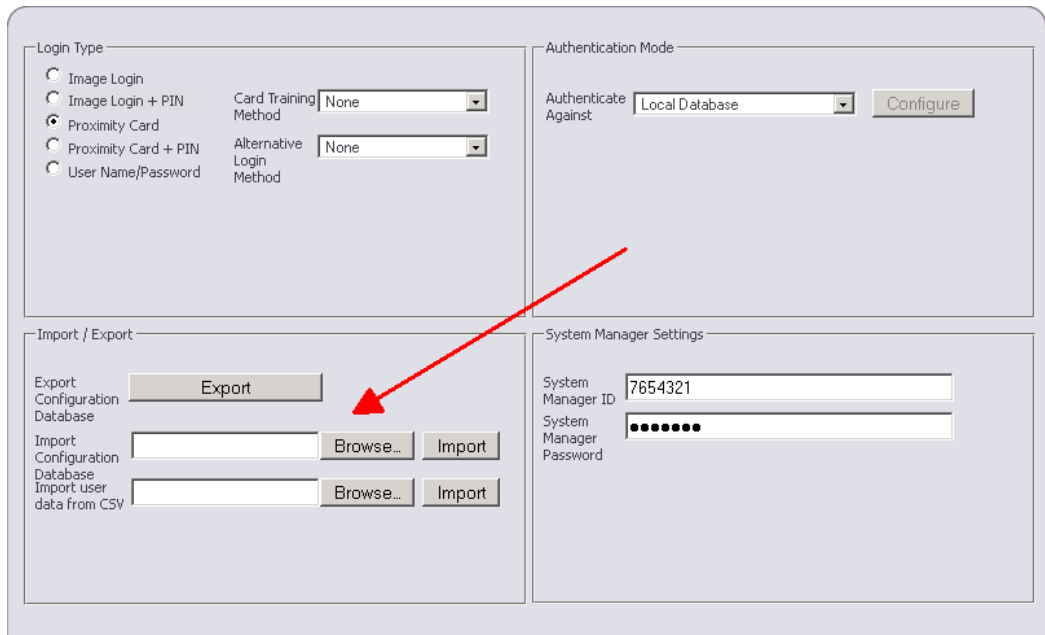
The exported data can easily be imported into another imageRUNNER ADVANCE device.

Several options exist for the import and export respectively.

- **Export Configuration Database:**
Using this option you can export the complete Universal Login Manager database, including user data and Universal Login Manager configuration data, to an *ulmConfig.ucf* file. This .ucf file can then be imported to other devices in order to provide the relevant devices with the same ULM configuration settings and user data.

- **Import Configuration Database:**

With this option you can import a *ulmConfig.ucf* file in order to transfer configuration settings and user data from a different device without the need to manually configure the device. Only *ulmConfig.ucf* files exported from other Universal Login Manager devices using the **Export Configuration Database** option are supported.



- **Import User Data from CSV File:**

This option allows you to import user data from a comma-separated text file (CSV). The .csv file must consist of a column header including all or some of the following keywords:

loginname, mail, cardid, homefolder, pincode, password, deptid, roles, displayindex



The following requirements have to be fulfilled:

- The keyword `loginname` is mandatory.
- The delimiter should be either `,` or `;` (without quotes).
- If delimiters like `,` or `;` are part of a field value, the complete value has to be set in quotes.
Example: `10,4` must be converted to `"10,4"`
- If a quote is part of a value, the quote has to be doubled and the complete value has to be set in quotes.
Example: The value `String ("A")` must be converted to `String ("\"A\"")`.
- Backslashes in a value must be doubled and the complete value has to be set in quotes.
Example: `\\server\homefolder` must be converted to `"\\\\server\\homefolder"`



Note that the data will be merged. Existing data will be overwritten with the imported data.

Example

User A and User B exist in the database. A CSV file with data of User B and User C is imported. In the end User A remains untouched and User C is imported from the CSV while the existing data of User B will be overwritten with the data from the CSV file.

See example below. Note the usage of the quotes in the last column of the first user, where there is a comma within the field.

```
loginname;mail;displayindex;homeFolder;password;pincode;cardid;deptid;roles
USR000001;USR000001@my.domain;1;\\\\10.190.57.158\\HomeFolder\\USR000001";PWD000001;999991;999991; ;"PowerUser, Guest "
USR000002;USR000002@my.domain;2;\\\\10.190.57.158\\HomeFolder\\USR000002";PWD000002;999992;999992; ;PowerUser
USR000003;USR000003@my.domain;3;\\\\10.190.57.158\\HomeFolder\\USR000003";PWD000003;999993;999993; ;PowerUser
USR000004;USR000004@my.domain;4;\\\\10.190.57.158\\HomeFolder\\USR000004";PWD000004;999994;999994; ;PowerUser
USR000005;USR000005@my.domain;5;\\\\10.190.57.158\\HomeFolder\\USR000005";PWD000005;999995;999995; ;PowerUser
```

8.4.4 System Manager Settings

Here the system manager's ID and password can be changed.

8.5 Roles

A role is a set of access rights to device features (e.g. permission to print duplex or to print in color). The access rights are controlled by the AMS kit, which is therefore required on the device. The **Roles** screen allows administrators to define different roles with different access rights. Each user has at least one role that is assigned by the administrator. The assignment of roles takes place in the **User** (see "[Users](#)" on page 26) menu.

There are different role types: preconfigured roles and custom roles.

Preconfigured Roles

Most of the preconfigured role names also already in use on the device and have been implemented in the Universal Login Manager for consistency reasons. The **Administrator**, **NetworkAdmin** and **DeviceAdmin** roles all use the System Manager ID as Department ID and as such, have access to the ULM Usage Tracker. The **Reporter** role also has access to the ULM Usage Tracker. This role has been especially created to enable a non-admin user to enter the ULM Usage Tracker if required. The **PowerUser**, **GeneralUser**, **LimitedUser** and **Guest** are preconfigured roles with various limited permissions. For more details, see the specific permission configuration of each role that is displayed on the right hand side of the **Roles** menu.



Preconfigured roles cannot be edited.

Custom Roles

A custom role can be created by clicking on the **Create** button and entering a name for the new role. Existing custom roles can be modified by clicking on the role name in the

role list. Then, you can configure each feature supported by AMS for the selected role, e.g. the permission for printing color or printing duplex.

8.5.1 Access Control

In the section **Access Control** on the left lower side you can choose whether access control takes place on device level or on function level.

- **Device level login** - If this radio button is checked, the device is locked if no user is logged in. As soon as users unlock the device by authenticating, they have access to all functions that have been assigned to their individual role.
- **Function level login** - If this radio button is checked, some particular functions on the device can be used without user authentication. Which functionality can be used without user authentication is configured via the *permit/deny* settings of the **FunctionLevelLogin** role. For this role, only the main functions can be permitted or denied, e.g. printing but not explicitly color or B/W printing. When a user chooses a function that is not available via the **FunctionLevelLogin** role, a user authentication is required. In this case it depends on the settings of the role that has been applied to this user whether the functionality is available for this particular user or not.
 - Under **Restricted Applets** each MEAP-Applet installed can be restricted.

Feature	Setting
Print Category	Permit
Copy Category	Permit
Color Copy	Color
Scan Category	Permit
Mailbox Category	Permit
Send Category	Permit
Browser Category	Permit
Utility Category	Permit
Default (MEAP) Category	Permit
Restricted Applets	-None- Copy ConvenienceCo



If **Department ID Management** is activated on the device, function level login only works if the department ID 9 was created manually without password beforehand.

In the section **Access Control** also general functions can be permitted or denied. This applies to **Remote scan**, **Remote copy** and **Remote print**. If allowed, these functions can be used remotely, otherwise they are forbidden.

The field **AMS Printer Driver Plug-In** controls, whether the use of this plug-in is mandatory in order to use the AMS controlled functions or not.

After having finished the configuration press the **Save** button to save the settings.

The screenshot shows the configuration interface for the Universal Login Manager. It is divided into three main sections:

- Roles:** A list of roles including PowerUser (selected), Reporter, FunctionLevelLogin, Administrator, Guest, NetworkAdmin, DeviceAdmin, GeneralUser, and LimitedUser. There are 'Create' and 'Delete' buttons next to the list.
- Access Control:** A section with radio buttons for 'Device level login' (selected) and 'Function level login'. Below are dropdown menus for 'Remote scan' (Permit), 'Remote copy' (Permit), 'Remote print' (Permit), and 'AMS Printer Driver Plugin' (Optional).
- PowerUser:** A table showing settings for the selected role. The table has two columns: 'Feature' and 'Setting'.

Feature	Setting
Print Category	Permit
Color print	Color
Simplex Print	Permit
Mailbox Print	Permit
Copy Category	Permit
Color Copy	Color
Simplex Copy	Permit
1 Page Per Sheet (no NUP)	1
Scan Category	Permit
Color Scan	Color
Mailbox Category	Permit
Color Print	Color
Simplex Print	Permit
1 Page Per Sheet (no NUP)	1

8.5.2 Import and Map Groups from Active Directory

If a connection to an Active Directory (AD) is configured, it is possible to import groups from the AD and map these to roles within the Universal Login Manager.

To import an AD group, just press the button **Import AD Groups**. A list with the AD groups appears from which you can select one or more groups. After pressing the **Save** button, the group(s) will be imported as roles with the same name and appear in the section **Roles** together with the already existing roles.

Roles

- PowerUser
- Reporter
- FunctionLevelLogin
- Administrator
- Guest
- NetworkAdmin
- DeviceAdmin
- GeneralUser
- LimitedUser

PowerUser

Feature	Setting
Print Category	Permit
Color print	Color
Simplex Print	Permit
Mailbox Print	Permit
Copy Category	Permit
Color Copy	Color
Simplex Copy	Permit
1 Page Per Sheet (no NUP)	1
Scan Category	Permit
Color Scan	Color
Mailbox Category	Permit
Color Print	Color
Simplex Print	Permit
1 Page Per Sheet (no NUP)	1

Access Control

Device level login
 Function level login

Remote scan:

Remote copy:

Remote print:

AMS Printer Driver Plugin:

X

Group Import

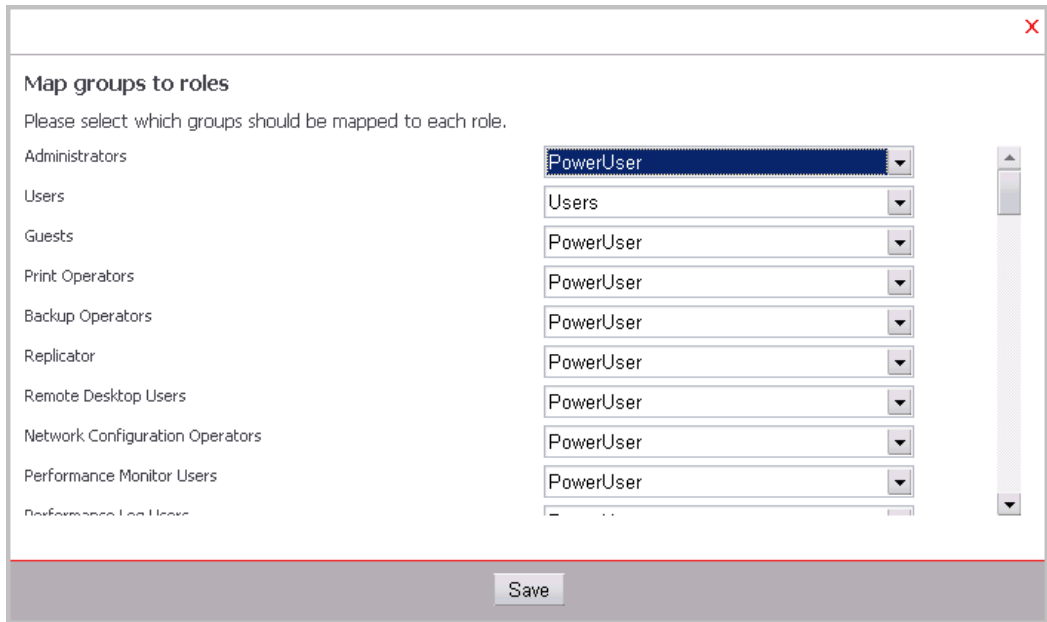
Please select which groups you would like to be imported.

- Administrators
- Users
- Guests
- Print Operators
- Backup Operators
- Replicator
- Remote Desktop Users
- Network Configuration Operators
- Performance Monitor Users
- Performance Log Users
- Distributed COM Users
- IIS_IUSRS

Make an implicit mapping of groups to roles. If you uncheck this box, you will have to make the mapping manually, by clicking on the "Map groups to roles" button.

If **Make an implicit mapping of groups to roles...** is checked, the imported groups are automatically mapped to the newly created roles of the same name. Otherwise, the mapping has to be done manually.

To manually map groups, press the button **Map Groups to Roles**. A new window appears with the groups on the left and the roles selectable from a drop-down list on the right. If **Make an implicit mapping of groups to roles...** is checked in the first step, the group and role with the same name are mapped automatically (as for "users" in the screenshot). Otherwise, no mapping is done and the administrator has to select a mapping by hand. Pressing **Save** concludes the mapping.



8.6 Customize

On this screen, the user interface can be customized. This can be done by selecting an existing theme or creating a new one from the **Themes** section. On the right side, a name can be entered for a new theme (existing themes cannot be renamed) and several settings like **Font Size** or various color settings can be defined. Additionally a background image can be uploaded and the positions of the login mask and info text can be set. Allowed image formats are JPG, PNG and GIF.

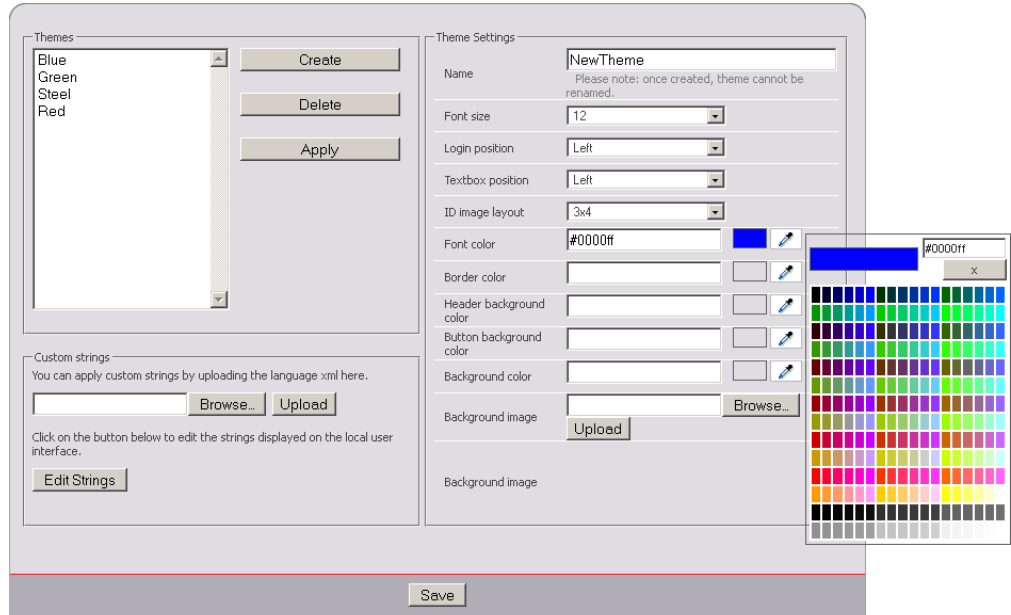
The following **Theme Settings** are available:

- **Name** - The name of the theme. Cannot be changed after a theme has been created.
- **Font size** - Font size of the texts shown.
- **Login position** - The position of the Login box. Can be **Left**, **Center**, **Right** or **Hidden**. If **Hidden** is selected, no card symbol will be shown for the Proximity Card and Proximity Card with PIN login types.
- **Textbox position** - The position of the Text box. Can be **Left**, **Center** or **Right**.
- **ID image layout** - Determines what matrix is used for the alignment of ID images on the device UI. Either 2x4 or 3x4 images can be displayed on one screen.
- **Font color** - Color of the fonts.
- **Border color** - Color of the border around the boxes.
- **Header background color** - Background color of the header line.
- **Button background color** - Background color of the login button.

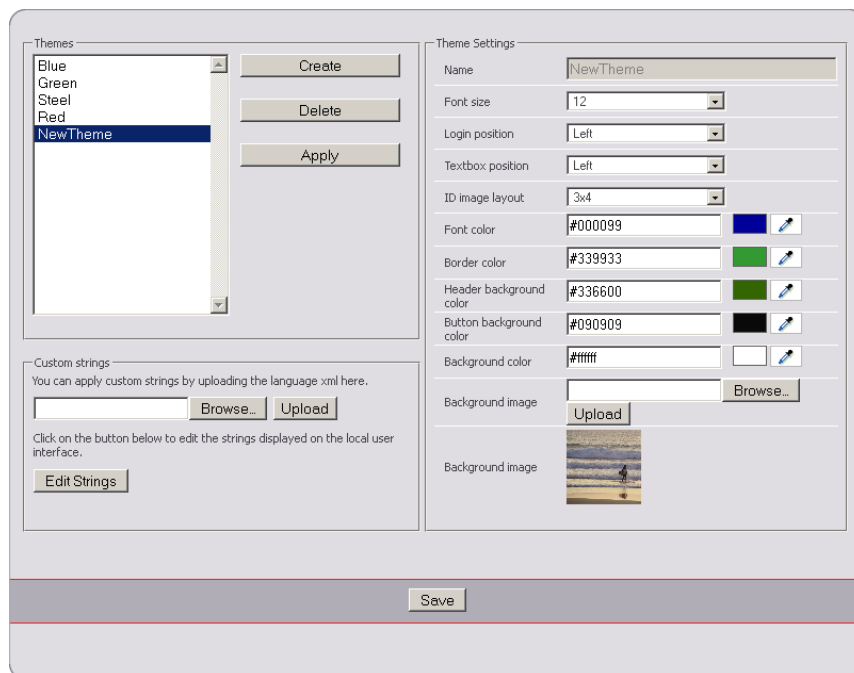
- **Background color** - Color of the main window background.
- **Background image** - Miniature of the uploaded image.

Example

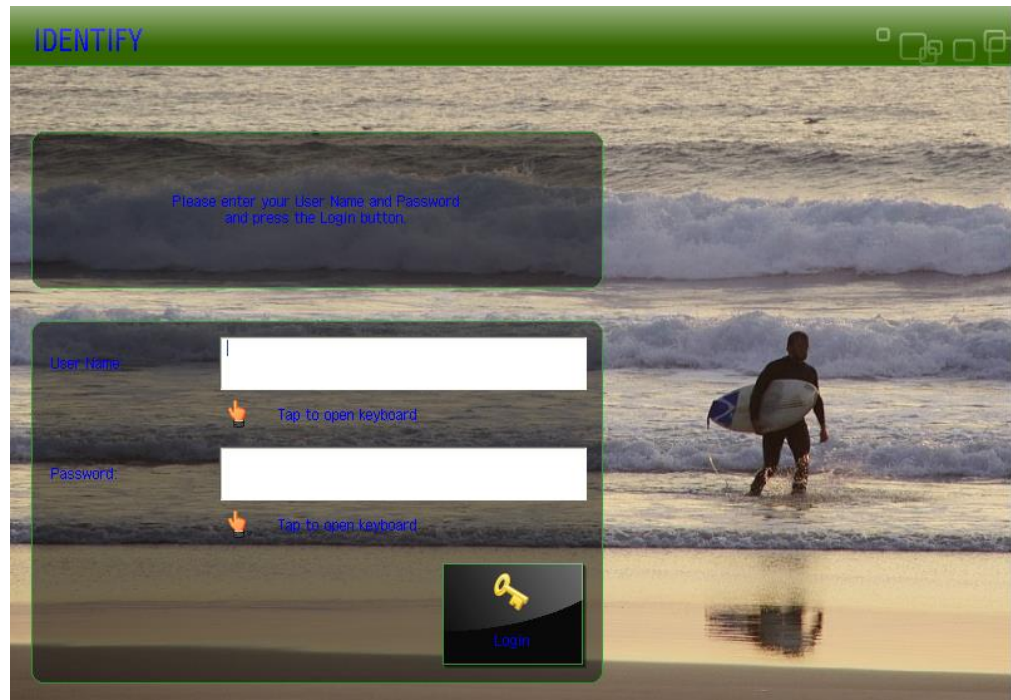
- Press the **Create** button and enter a name. Choose the font size you want and decide on the position of the login box and the information text box. Then, use the color picker for each of the color fields.



- Choose a font color and if necessary a color for the border, header, button and general background.



- You can also browse for a background image for the device screen and upload it. Click **Save** to apply your settings. Now the new settings are active and your login manager UI has a completely customized design.



8.6.1 Customized Language Strings



- The displayed language of the Universal Login Manager is dependent on the display-language of the device.
- If you want to change the UI language of the Universal Login Manager, change the display language of the device. E.g. if you change the display language of the device to Spanish, then the UI of the Universal Login Manager is also displayed in Spanish.
- Note that only languages that are installed on the device can be set. Therefore, before changing the language, you should ensure that the language pack of the language you would like to set is available on the device.

The installer of the Universal Login Manager includes the language strings of all languages that were available in the NT-ware String Portal at the time when creating the installer. These strings are included in a file called *MomLang.xml*. Once you have installed the Universal Login Manager, you can switch the UI language of the Universal Login Manager to one of these languages. NT-ware only ensures the translation of strings into EFIGS (English, French, Italian, German and Spanish). That's why it can happen, that (part) of the strings are not available in your local language, although the language is available in the *MomLang.xml*. To overcome this, you can download the *MomLang.xml* with the Universal Login Manager strings, add the missing translations and then upload the translated file to the device in question (see below). If your local language does not yet exist in the *MomLang.xml*, you first have to add it to the

MomLang.xml and only then translate the corresponding strings. Please note that knowledge about XML editing is required.

Available Languages

At present the following languages are available:



Language codes are case sensitive. Please use upper-case characters only.

Language	Language code
Arabic	AR
Bahasa Melayu	MS
Brazilian-Portuguese	BRA
British English	GB
Catalan	CA
Chinese	CN
Croatian	HR
Czech	CZ
Danish	DK
Dutch	NL
English	EN
Estonian	EE
Finnish	FI
French	FR
German	DE
Hebrew	HE
Hungarian	HU
Icelandic	IS
Italian	IT
Japanese	JP
Korean	KO
Latvian	LVA
Lithuanian	LT
Norwegian	NO
Polish	PL

Language	Language code
Portuguese	PT
Russian	RU
Slovenian	SL
Spanish	ES
Swedish	SE
Thai	TH
Traditional Chinese	TW
Turkish	TR

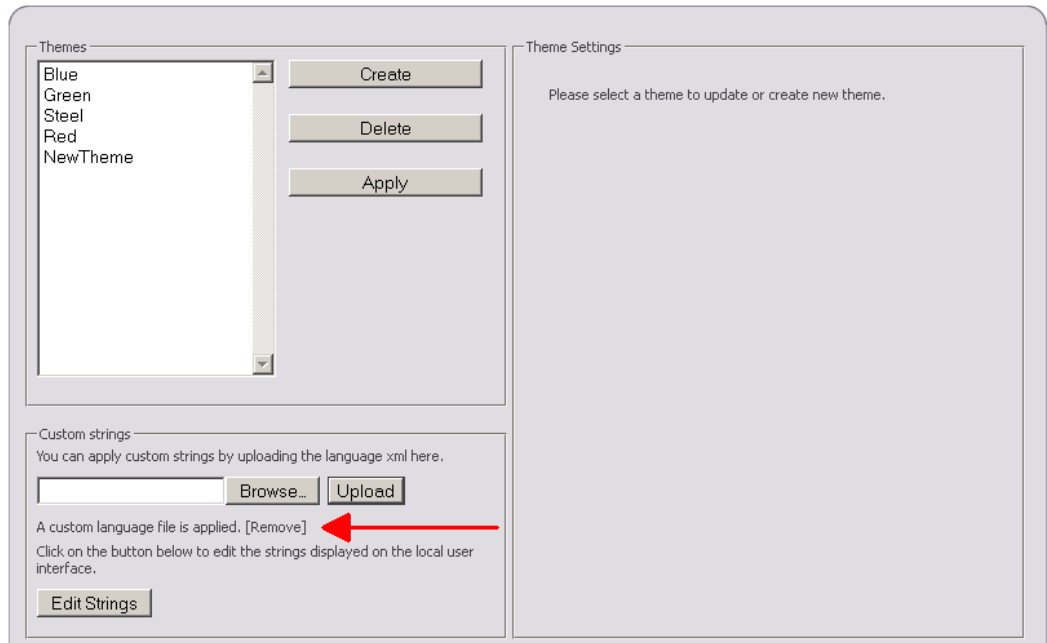
Customized Language File (MomLang.xml)

If you want to make use of a customized language file, proceed as follows.

1. Extract the required strings from the NT-ware String Portal by clicking on the following link: Universal Login Manager String Export (<https://ntwlabib.dnsalias.com/Stringtable/MomLang.xml?from=40000&to=40999>).
2. Save the downloaded file of type MomLang.xml locally. You should give the file a meaningful name. E.g. you could add the language code to the name of the file so that it is easy to identify that it is not the default MomLang.xml provided by the installer.
3. Open the file in an XML editor, locate the desired language or create language strings in your own language in case your language does not exist yet. If you need to add your language strings to the file, make sure to use the ISO-639-1 code of the language you want to add.
4. When done, upload the modified file in the **Customize menu** under **Custom Strings**. Browse for the file by clicking on the **Browse** button and upload the file using the **Upload** button. You can remove the file by clicking on **Remove**. This removal reactivates the default MomLang.xml provided with the installer.



In addition to your local language, the English language strings must always be present in the customized XML file. Otherwise, the import of customized strings will not be successful.



The language files are stored locally on the device. If you have multiple devices, you need to repeat the import for all devices.

Edit Strings for MEAP UI

You can also edit the strings displayed on the MEAP display. Press **Edit Strings** on the **Customize** page. Now you can select the string to edit by ticking the checkbox next to it. Finish with **Save**.

Customize Strings✕

Tick the checkbox for each string that you would like to customize.

Please identify yourself with your ID-Card	<input type="checkbox"/>
Please enter your User Name and Password and press the Login button.	<input type="checkbox"/>
Please identify yourself with your personal PIN Code and press the login button.	<input type="checkbox"/>
Login in Progress. Please wait a moment.	<input type="checkbox"/>
Your ID Card is unknown. Please log in with your user name and password to register your ID Card.	<input type="checkbox"/>
Please try again by entering your full credentials.	<input type="checkbox"/>
User authentication failed. Please try again.	<input type="checkbox"/>



You can reset each field simply by unchecking the checkbox. The string will revert to the default string.

8.7 Usage Tracker

The Universal Login Manager / embedded Universal Login Manager provides the possibility of downloading a Rich Internet Application for tracking the usage of the devices, the Universal Login Manager Usage Tracker. This application is run in a local browser on the user's computer. With the usage tracker, the user can manage a list of up to 10 registered devices and retrieve reporting data from the devices.



Reporting Data Limitation

Please note that the amount of retrievable reporting data is dependent on the CPCA log storage capacity on the device. The storage capacity is typically limited to 5,000 entries but can vary on different devices. Please refer to the user manual of the relevant device for details.

The link to the ULM Usage Tracker can be found on the **Usage Tracker** tab of the Universal Login Manager / embedded Universal Login Manager administration tool.

The ULM Usage Tracker has three sub menus:

ULM Usage Tracker

On this page up to 10 printers can be added and reports for a given period of time can be created.

Select	Device Model	Device IP Address	Serial Number	Earliest Date	Neighbors	Delete	Availability
There are no configured devices.							

Report Name	Report Description	Generate Report
User Details	Will show a report of all the jobs which were performed between the given dates, grouped per user.	
Device Details	Will show a report of all the jobs which were performed between the given dates, grouped per device.	
User Summary	Will show a summary report for each user which has executed a job on one of the selected devices between the given dates.	
Device Summary	Will show a summary report for the selected devices, for the jobs executed on them between the given dates.	

Cost Table

On this page prices for each product can be entered, sorted by media and service, e.g. for **Print A4 Color**. The value is entered without currency unit.



Prices can be specified with two decimal places.

	Print	Copy	Scan	Fax
A3 B/W	8.00	7.00	1.00	0.00
Small B/W	2.00	5.00	0.00	0.00
A4 B/W	3.00	6.00	0.00	0.00
A5 B/W	2.00	4.00	0.00	0.00
SRA3 B/W	0.00	0.00	0.00	0.00
Letter B/W	0.00	0.00	0.00	0.00
Legal B/W	0.00	0.00	0.00	0.00
Tabloid B/W	0.00	0.00	0.00	0.00
Half Letter B/W	0.00	0.00	0.00	0.00
A3 Color	0.00	0.00	0.00	
Small Color	0.00	0.00	0.00	
A4 Color	5.00	8.00	1.00	
A5 Color	3.00	5.00	1.00	
SRA3 Color	0.00	0.00	0.00	
Letter Color	0.00	0.00	0.00	
Legal Color	0.00	0.00	0.00	
Tabloid Color	0.00	0.00	0.00	
Half Letter Color	0.00	0.00	0.00	
Staple	0.00			
Hole Punch	0.00			



All data like prices or added printers are only stored in the local browser's cache and controlled with cookies. All configured data is lost, if cache and cookies are deleted. To save data, use the export/import functions where available.

Settings

Here two parameters for CSV export of reports and *Cost Tables* can be changed.

- Decimals delimiter:**
 Decimal delimiter can either be a dot (.) or a comma (,).
- CSV columns delimiter:**
 You can either select semicolon (;), comma (,) or a tabulator (TAB.).

8.7.1 Adding a Device

In order to add a device for which you want to create a report, open the ULM Usage Tracker page and press the button **Add Device**. A new row opens where you can add a new device. Enter the IP address and press the button **Add**. If you have checked **Find neighbors**, the ULM Usage Tracker tries to find more devices in the same subnet. The new device(s) appear(s) in the device list. The names are automatically filled in. When the registration of new devices is finished, press the button **Done**. The "Add Device row" closes.

The device list consists of the following columns:

- **The select column (first column):**
Here you can select the device for reporting by checking the corresponding select box. By checking the select box in the column header, you select all available devices. By unchecking this box, you unselect all devices.
- **Device Model:**
This name will be automatically retrieved when the IP address of the device has been entered.
- **Device IP Address:**
The IP of the device.
- **Serial Number:**
The serial number of the device.
- **Earliest Date:**
If you click on **Check**, the ULM Usage Tracker tries to determine the date of the oldest entry in the device's job list. This only works if a valid user name and password have been entered.
- **Neighbors:**
If you click on **Find**, the ULM Usage Tracker tries to find more devices in the same subnet.
- **Delete:**
Press the delete icon in order to delete the device from the list.

- **Availability:**
If the device is available the icon shown here is green, otherwise it is red.

Usage Tracker

User name: administrator
 Password: ●●●●●●
 Start Date: 01-05-2012
 End Date: 30-04-2013

Here you can add or edit the devices for which you would like to create a report. You can add a maximum of 10 devices. After you have finished editing the list, please indicate which device you would like to be included in your report, by selecting the checkboxes.

<input type="checkbox"/>	Device Model	Device IP Address	Serial Number	Earliest Date	Neighbors	Delete	Availability
<input type="checkbox"/>	IR-ADV C5030/5035	10.129.51.86	XXXXXXXXXX	27-01-2010	[Find]	✖	✔
<input type="checkbox"/>	IR-ADV C2020/2030i		XXXXXXXXXX	[Check]	[Find]	✖	✖
<input type="checkbox"/>	IR-ADV C2220/2230	10.128.51.235	XXXXXXXXXX	13-09-2012	[Find]	✖	✔
<input type="checkbox"/>	Miskin	192.168.38.100	XXXXXXXXXX	[Check]	[Find]	✖	✖
<input type="checkbox"/>	IR-ADV C2020/2030i	10.129.50.98	XXXXXXXXXX	[Check]	[Find]	✖	✖
<input type="checkbox"/>	IR-ADV C7055/7065	10.129.50.21	XXXXXXXXXX	[Check]	[Find]	✖	✖
<input type="checkbox"/>	IR-ADV 400/500	10.129.51.92	XXXXXXXXXX	[Check]	[Find]	✖	✖

Please choose the type of statistic data that should be generated.

Report Name	Report Description	Generate Report
User Details	Will show a report of all the jobs which were performed between the given dates, grouped per user.	
Device Details	Will show a report of all the jobs which were performed between the given dates, grouped per device.	
User Summary	Will show a summary report for each user which has executed a job on one of the selected devices between the given dates.	
Device Summary	Will show a summary report for the selected devices, for the jobs executed on them between the given dates.	

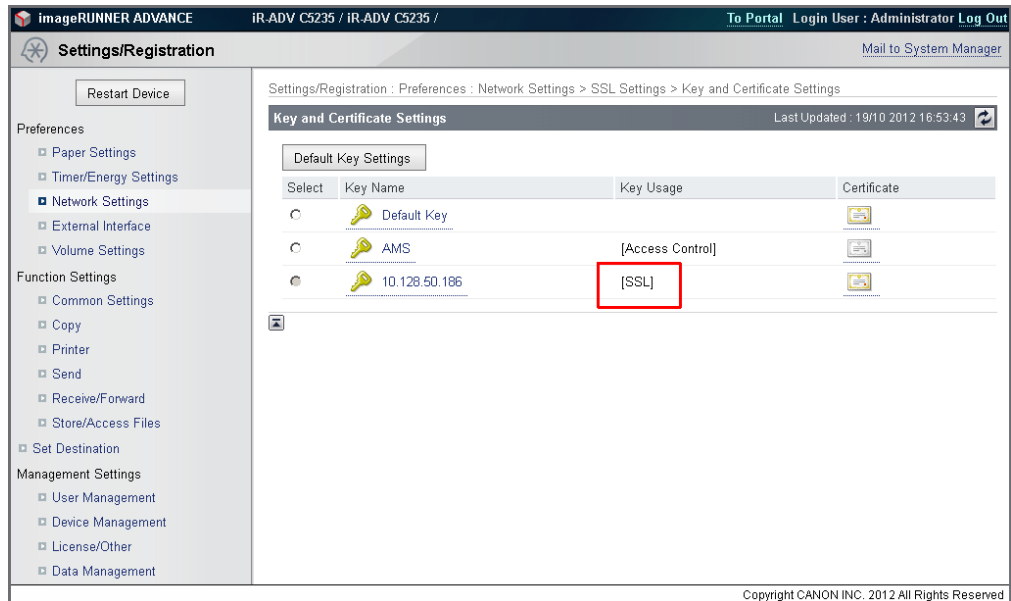
8.7.1.1 Creating a Certificate

It is possible that your browser cannot retrieve information from the device due to certificate problems when using an SSL connection. In this case the printer appears as unavailable in the device list.

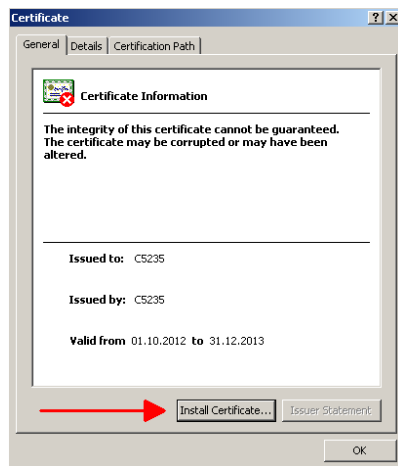
To solve this problem you need to create a new certificate on the device including its IP address. In order to do this, follow these steps:

- Open the device's RUI in a browser and log in with system manager credentials.
- Open **Settings/Registration : Management Settings : License/Other > MEAP Settings** and uncheck **Use SSL**.
- Click on **OK** and restart the device.
- Login again and open **Settings/Registration : Preferences : Network Settings > SSL Settings > Key and Certificate Settings**
- If a key other than the **Default Key** was used before, check the radio button in front of **Default Key** and click on **Default Key Settings** to set it as the standard SSL key. Restart the device.
- Login again. In **Settings/Registration : Management Settings : Device Management > Key and Certificate Settings** click on **Generate Key**, then open **Network Communication**.
- Enter the device IP address in the field **Common Name**, fill out the **Certificate Settings** and click on **OK**.

- Open **Settings/Registration : Preferences : Network Settings > SSL Settings > Key and Certificate Settings**.
- Select the new key and click on **Default Key Settings**. Now **[SSL]** marks this key as the active SSL key.



- Open **Settings/Registration : Management Settings : License/Other > MEAP Settings** and check **Use SSL**.
- Click on **OK** and restart the device.
- Now open the device's RUI from your browser again and save the SSL certificate to your file system. The way how to do that depends on your browser.
- Open the Windows file explorer and double-click on the saved certificate.



- Start the Certificate Import Wizard by clicking on **Install Certificate** and follow the steps.
- After finishing the wizard start the ULM Usage Tracker. The printer is now marked as available in the device list



Note that the certificate has to be installed on each PC running the ULM Usage Tracker.

8.7.2 Cost Table

On this page you can enter prices for media and services. For instance, you can enter different prices for Fax or Print in A4.

The screenshot shows the 'Cost Table' interface in the ULM Usage Tracker. The table lists various media and services with their respective costs for Print, Copy, Scan, and Fax. The 'Print' column has values ranging from 0.00 to 8.00, 'Copy' from 0.00 to 8.00, 'Scan' from 0.00 to 1.00, and 'Fax' from 0.00 to 0.00. A 'Save' button is located at the bottom of the table.

	Print	Copy	Scan	Fax
A3 B/W	8.00	7.00	1.00	0.00
Small B/W	2.00	5.00	0.00	0.00
A4 B/W	3.00	6.00	0.00	0.00
A5 B/W	2.00	4.00	0.00	0.00
SRA3 B/W	0.00	0.00	0.00	0.00
Letter B/W	0.00	0.00	0.00	0.00
Legal B/W	0.00	0.00	0.00	0.00
Tabloid B/W	0.00	0.00	0.00	0.00
Half Letter B/W	0.00	0.00	0.00	0.00
A3 Color	0.00	0.00	0.00	
Small Color	0.00	0.00	0.00	
A4 Color	5.00	8.00	1.00	
A5 Color	3.00	5.00	1.00	
SRA3 Color	0.00	0.00	0.00	
Letter Color	0.00	0.00	0.00	
Legal Color	0.00	0.00	0.00	
Tabloid Color	0.00	0.00	0.00	
Half Letter Color	0.00	0.00	0.00	
Staple	0.00			
Hole Punch	0.00			

The **Cost Table** can be exported and imported by using the export and import buttons in the upper left corner of the screen.

8.7.3 Creating a Report

To create a report, proceed as follows:

- Enter a valid user name and password.
- Enter the date range using the **Start Date** and **End Date** fields.
- In the device list check the select boxes of the device(s) you want reports for or the select box in the column header for all devices. Only devices shown as available can be selected.
- Select a report by clicking on the icon in the column **Generate Report**. The report is being generated and appears after a period of time. Depending on the range of time and the number of devices this can take several minutes.



- If you select more than one device, make sure that the user who is generating the report has an Administrator or Reporter role on all selected devices and that name and password are the same on all devices.
- FAX logs can only be read from devices running Universal Login Manager V4.1 or higher.

User name:

Password:

Start Date:

End Date:

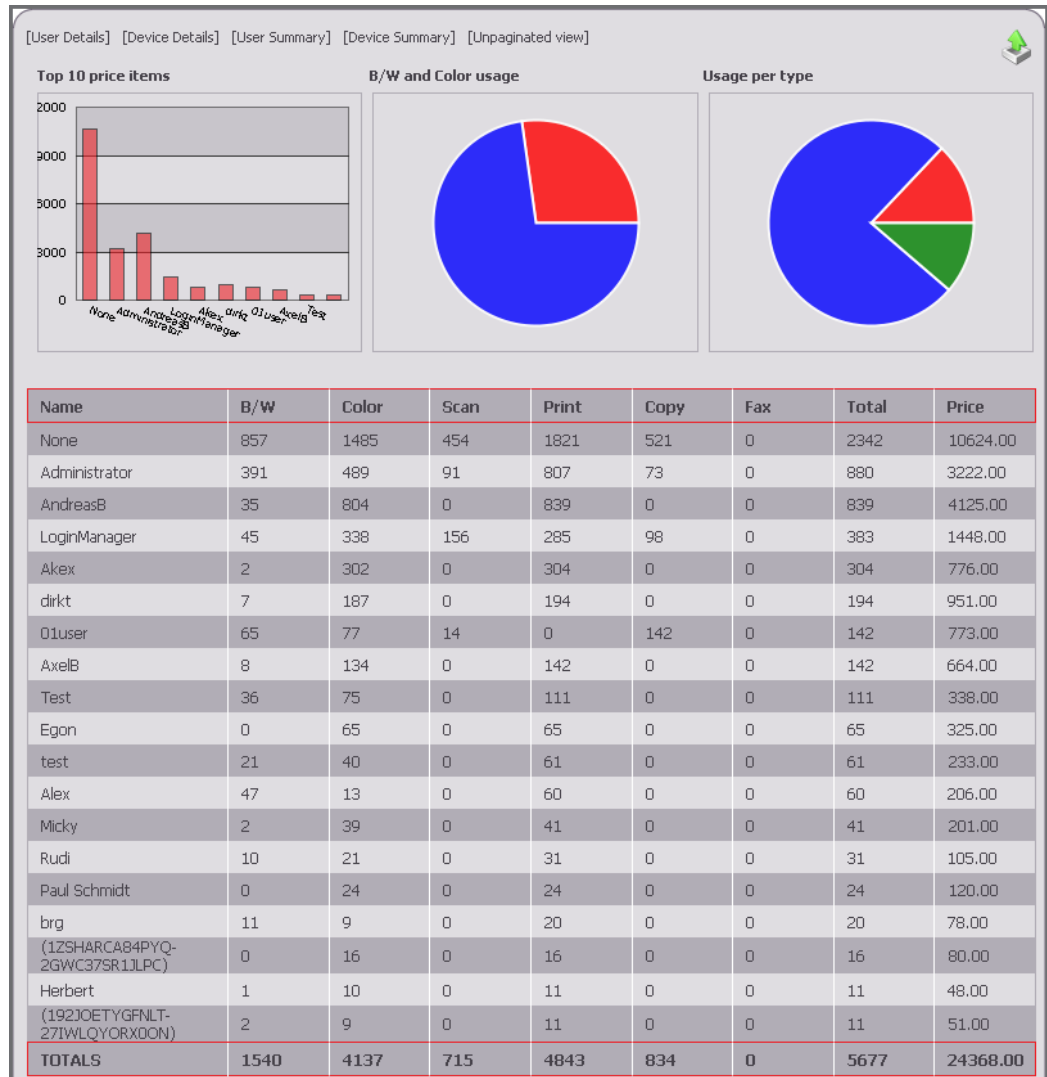
Here you can add or edit the devices for which you would like to create a report. You can add a maximum of 10 devices. After you have finished editing the list, please indicate which device you would like to be included in your report, by selecting the checkboxes.

<input checked="" type="checkbox"/>	Device Model	Device IP Address	Serial Number	Earliest Date	Neighbors	Delete	Availability
<input checked="" type="checkbox"/>	IR-ADV C5030/5035	10.129.51.86	XXXXXXXX	27-01-2010	[Find]	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	IR-ADV C2020i/2030i		XXXXXXXX	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	IR-ADV C2220/2230	10.128.51.235	XXXXXXXX	13-09-2012	[Find]	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Miskin	192.168.38.100	XXXXXXXX	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	IR-ADV C2020i/2030i	10.129.50.98	XXXXXXXX	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	IR-ADV C7055/7065	10.129.50.21	XXXXXXXX	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	IR-ADV 400/500	10.129.51.92	XXXXXXXX	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>

Please choose the type of statistic data that should be generated.

Report Name	Report Description	Generate Report
User Details	Will show a report of all the jobs which were performed between the given dates, grouped per user.	
Device Details	Will show a report of all the jobs which were performed between the given dates, grouped per device.	
User Summary	Will show a summary report for each user which has executed a job on one of the selected devices between the given dates.	
Device Summary	Will show a summary report for the selected devices, for the jobs executed on them between the given dates.	

After reading out the data from the device(s), the selected report is shown. You can switch between the report types without re-reading data by simply clicking on the report names in the upper left corner. The tab unpaginated view opens the selected report in a pop-up window to enable the user to make a print-out of the displayed html page. To close this pop-up click on the red X in the upper right corner.



In case different articles are accounted in a print job, for some report types the overall amount of articles is shown for the job, followed by the articles grouped by type.

Example

A job comprises 5 pages A4 Color, 6 pages A4 B/W and 5 x Duplex. This sums up to 16 articles in total. In the table, the total count for the print job is shown as 16 and the job types are listed separately with their respective count.

The reports can be exported as *.csv files for further processing in a spread sheet application. Click the export icon in the upper right hand corner of the screen to do so.



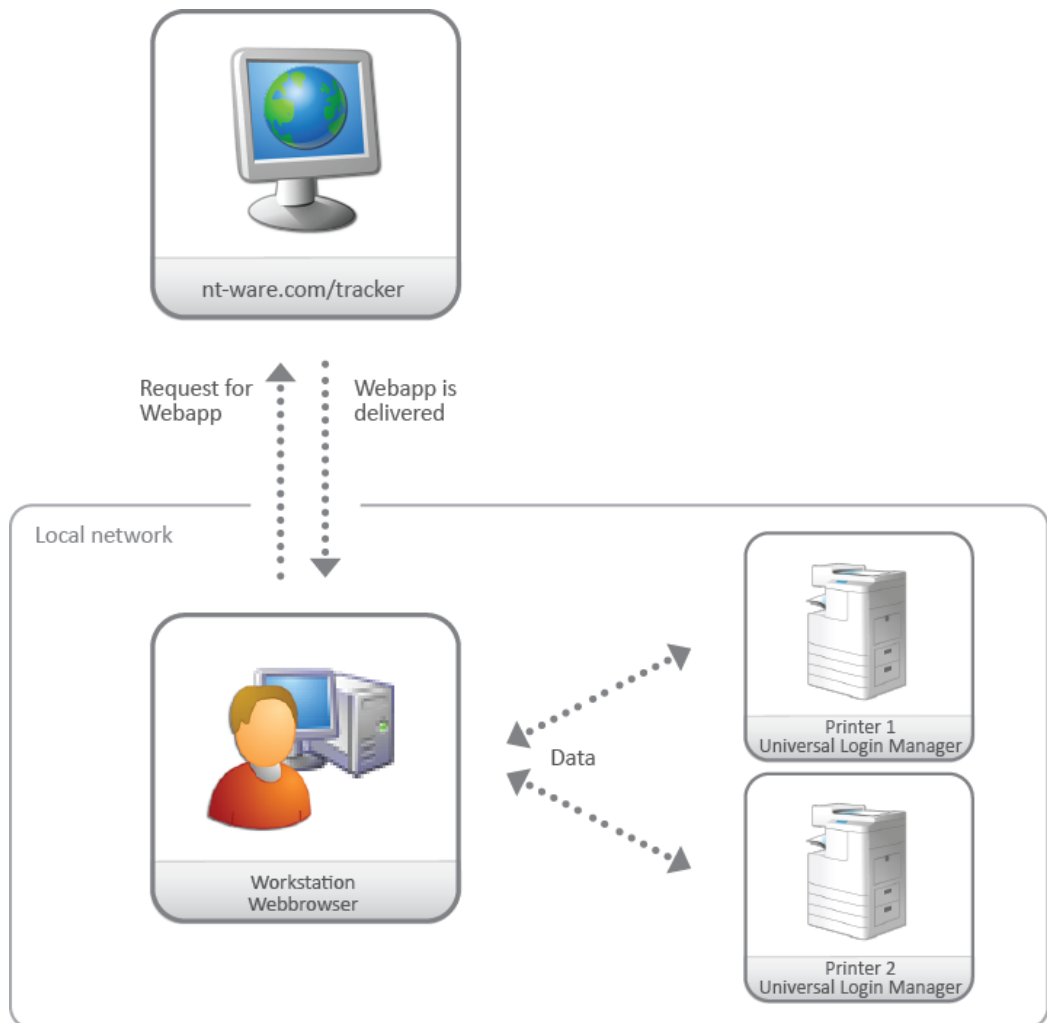
The exported *.csv file uses the delimiters configured under **Settings**.

8.7.4 Security Aspects

The ULM Usage Tracker is a web app that is executed locally within the browser. When the user opens the ULM Usage Tracker from the user interface the web browser requests the web app package from the NT-ware web site. The package comprises all scripts and files necessary to run the ULM Usage Tracker (JS, Flash, HTML, images, CSS). After receiving the package the browser starts the web app locally. The app runs in the browser alone and keeps its data within the browser cache or cookies, depending on the type of data, see below for more details.



No data is shared outside the local network. No data leaves the local network. Communication with printers takes place encrypted via HTTPS protocol.



ULM Usage Tracker Communication in Detail

- All scripts that run within the ULM Usage Tracker environment are downloaded locally and are kept in the browser's cache. That concerns the following technologies:
 - **JavaScript + HTML:**
General application.
Import of prices, except for IE8/9.
 - **Adobe Flash:**
All browsers: for export of reports and prices.
IE8/9 only: import of prices
- The browser makes requests to the devices through the HTTP(S) protocol, using JavaScript AJAX calls. The answer is returned in JSON format and is locally parsed by the JavaScript code running in the browser.
- Data transfer between workstation and printer is done via HTTPS. Only if HTTPS is not available for any reason (network configuration, certificates etc.), the system falls back to HTTP.
- User name and password, printer IP and settings as well as the price tables are stored within cookies.
- Data coming from the printers are kept in the workstation's memory.
- Due to different technologies used in the Internet Explorer (only for version 8/9) the communication is done in JSON-P. When using HTTPS, you will get a warning that the certificate is unknown. This can be resolved by installing the certificate locally. See chapter Creating a Certificate on the Device (see "[Creating a Certificate](#)" on page 57).

9 Secure Print

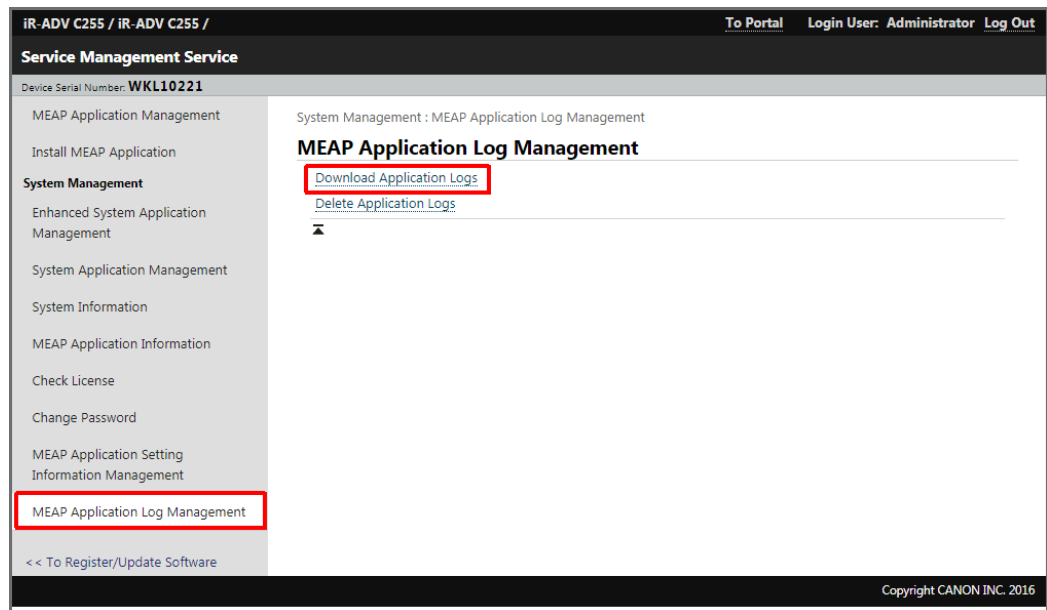
For configuring the Secure Print feature of your printer, please refer to the portal *Canon Office Imaging Products User Manuals* (https://ug.oipsrv.net/portal-eu-af-me-ru/frame_htmls/home.html) and search for your specific printer model.

10 Upgrade to uniFLOW Server

The Universal Login Manager can be connected to a uniFLOW server or RPS. Then, it automatically will switch into a "uniFLOW Client" mode. In that mode the Universal Login Manager is controlled by the uniFLOW server like a standard uniFLOW Login Manager.

11 How to obtain Log Files

The Universal Login Manager logs its activities and writes the log data into the device logs, which can be accessed via the Service Management Service page.



12 Appendix

12.1 Hardware

A list of supported devices and firmware versions can be found below.

Device Name	Minimum Firmware Version	AMS	Note
imageRUNNER ADVANCE C9280 PRO	v10.23	Standard	*1
imageRUNNER ADVANCE C7280i/C7270i/C7260i	v10.23	Standard	
imageRUNNER ADVANCE C5255/C5255i/C5250/C5250i/C5240i/C5235i	v06.01	Standard	
imageRUNNER ADVANCE C2230i/C2225i/C2220i	v06.01	Standard	
imageRUNNER ADVANCE C2220L	v10.23	Standard	
imageRUNNER ADVANCE 8205 PRO/8295 PRO/8285 PRO	v02.01	Standard	
imageRUNNER ADVANCE 6275i/6265i/6255i	v02.01	Standard	
imageRUNNER ADVANCE 4251i/4245i/4235i/4225i	v10.20	Standard	
imageRUNNER ADVANCE C9070 PRO/C9060 PRO	v69.03	Optional	*1
imageRUNNER ADVANCE C7065i/C7055i	v69.03	Optional	
imageRUNNER ADVANCE C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i	v69.03	Optional	
imageRUNNER ADVANCE C2030L/C2020L	v32.01	Optional	*2
imageRUNNER ADVANCE C2030i/C2025i/C2020i	v32.01	Optional	
imageRUNNER ADVANCE 8105 PRO/8095 PRO/8085 PRO	v44.03	Optional	
imageRUNNER ADVANCE 6075/6075i/6065/6065i/6055/6055i	v44.03	Optional	
imageRUNNER ADVANCE 4051i/4045i/4035i/4025i	v17.02	Optional	

Device Name	Minimum Firmware Version	AMS	Note
imageRUNNER ADVANCE 500i/400i	v1.02	Standard	
imageRUNNER ADVANCE C351iF/C350i/C250i/C350P	v17.01	Standard	
imagePRESS C700/800	v05.02	Standard	
imageRUNNER ADVANCE C33xx	v3.15	Standard	
imageRUNNER ADVANCE 8405/8495/8485			
imageRUNNER ADVANCE 8505/8505P/8595/8585	v1301.0.501	Standard	
imageRUNNER ADVANCE 6575i/6565i/6555i	v2002.0.1004	Standard	
imageRUNNER ADVANCE C5560i/5550i/5540i/5535i/5535	v1023.0.1101	Standard	
imagePRESS C850/C750/C650/C65	v36.01	Standard	
imageRUNNER ADVANCE C255/C355	v134.0.102	Standard	
imageRUNNER ADVANCE C3530/C3525/C3520	v260.0.101	Standard	
imageRUNNER ADVANCE 4551/4545/4535/4525	v254.0.223	Standard	
imageRUNNER ADVANCE C256/356	v2538.0.101	Standard	
imageRUNNER ADVANCE C525/615/715	all versions	Standard	
imageRUNNER ADVANCE 525i, 615i, 715i	all versions	Standard	
imageRUNNER ADVANCE C7565i III, C7570i III, C7580 III	all versions	Standard	
imageRUNNER ADVANCE 8505 III, 8585 III, 8595 III	all versions	Standard	
imageRUNNER ADVANCE 6555 III, 6560 III, 6565 III, 6575 III	all versions	Standard	
imageRUNNER ADVANCE C5535 III, C5540 III, C5560 III	all versions	Standard	
imageRUNNER ADVANCE 4525 III, 4535 III, 4545 III, 4551 III	all versions	Standard	
imageRUNNER ADVANCE C3520 III, C3525 III, C3530 III	all versions	Standard	
imageRUNNER ADVANCE C256 III, C356i III	all versions	Standard	

Device Name	Minimum Firmware Version	AMS	Note
imageRUNNER ADVANCE C475i III	all versions	Standard	
imageRUNNER ADVANCE 525i, 615i,715i	all versions	Standard	
imageRUNNER ADVANCE DX	all versions	Standard	
imageRUNNER ADVANCE: <ul style="list-style-type: none"> Gen3: 1st Edition, 2nd Edition, 3rd Edition 	all versions	Standard	
imageRUNNER (AddOn Platform)	all versions	Standard	

*1 AMS for Print function not supported on Local/AD mode

*2 Secure Print function (My job status) not supported

12.2 Optional Items

12.2.1 Supported Card Readers

The Universal Login Manager supports the following NT-ware card readers:

- MiCard Magnetic Card Reader
- MiCard MultiTech4-P
- MiCard MultiTech4-P LEGIC
- MiCard MultiTech4-PI
- MiCard PLUS
- MiCard PLUS-2
- MiCard PLUS-2 V2
- MiCard V2
- MiCard V3 Multi



Card Reader User Manuals

Download links for all card readers can be found on the NT-ware resources page (<https://link.nt-ware.net/id160>).

12.2.2 USB Device Port

The USB Device Port option is recommended in order to keep the card reader secure and safe. It provides two additional USB ports and you can easily install and store a card reader in it. A4 ADVANCE devices don't have a device port option. Instead, use the IC Card Reader option to store a card reader secure and safe.

See Supported Card Readers (on page [67](#)) for a list of all supported card readers.



Item Code	Products	Supported devices
5594B004AA	USB Device Port-E4	imageRUNNER ADVANCE C50xx/C52xx/C22xx/42xx/33xx
5594B003AA	USB Device Port-E3	imageRUNNER ADVANCE 4251i/4245i/4235i/4225i C50xx/C52xx/C22xx
5594B002AA	USB Device Port-E2	imageRUNNER ADVANCE C5255/C5255i/C5250/C5250i/C5240i/C5235i/ C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i/ C2230i/C2225i/C2220i/ C2220L
3720B001AA	USB Device Port-B1	imageRUNNER ADVANCE C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i
4790B001AA	USB Device Port-C1	imageRUNNER ADVANCE C2030i/C2030L/C2025i/C2020i/C2020L
5010B001AA	USB Device Port-D1	imageRUNNER ADVANCE 4051i/4045i/4035i/4025i
6866B001AA	IC Card Reader Box-A1	imageRUNNER ADVANCE 500i/400i C351iF/C350i/C250i

The USB Device Port is standard on imageRUNNER ADVANCE 6xxx/8xxx PRO, C7xxx/C9xxxPRO.

12.2.3 AMS - Access Management System

AMS Kit

In order to set up access control per user/group, an AMS kit is required. The Access Management System is standard on the imageRUNNER ADVANCE

C92xx/C72xx/C52xx/C22xx/C351iF/C350i/C350P/C33xx/C250i/82xx/62xx/42xx/500i/400i series. For other imageRUNNER ADVANCE models, please refer to the table below for the required optional item to be ordered.

1642B011AA	AMS Kit-B1	imageRUNNER ADVANCE C9070 PRO/C9060 PRO/C7065/C7055/C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i/C2030L/C2020L/C2030i/C2025i/C2020i/8105 PRO/8095 PRO/8085 PRO/6075/6075i/6065/6065i/6055/6055i/4051i/4045i/4035i/4025i
------------	------------	--

AMS Printer Driver Add-In Module

In order to set access control for print jobs from a Windows PC, you need to install the AMS printer driver add-in module into the Canon printer driver (UFR II/PCL/PS). The AMS printer driver add-in module is provided through the Software Download Centre (<https://software.canon-europe.com/>).

Supported Version: AMS printer driver add-in module Ver 3.1.0 or later.

Glossary

AD (Active Directory)

Active directory is a Windows directory service included in most Windows server systems. It stores information of objects on the network within a database. Most commonly, data about users, printer queues or network configuration is stored. This data is made available to administrators and users.

AD Credentials (Active Directory Credentials)

Microsoft® Active Directory Service stores information of objects on a network and makes this information available to users and network administrators. AD credentials refer to the user name and password of the user.

AMS (Access Management System)

A system developed by Canon that provides access management possibilities on a per feature basis for imageRUNNER devices.



Canon Access Management System Website
(https://www.usa.canon.com/cusa/office/products/software/network_device_management/access_management_system)

CDS (Content Delivery System)

A CDS is a configurable software system that has the purpose of downloading (delivering) streaming content from a network storage to the end-user's device.

There are CDS's for Web (WCDS), for mobile devices (MCDS), for use throughout an enterprise (ECDS), etc.

CPCA (Common Peripheral Controlling Architecture)

CPCA is a proprietary communication protocol developed by Canon to communicate with multi-functional devices (MFP). CPCA controls all MFP functionality including printing, copying, scanning, and mailbox management. CPCA is implemented in MEAP as a Java class library. Any application built under MEAP can submit and control a printer, scanner, or copier job by invoking the class library. Herewith some of the functions available when using the CPCA CL (Class Library). The functionality of the MFP device itself, however, may exclude one or more of the functions in the following list.

- Copy, scan, print job submission
- Job management (cancel, hold, resume)
- Device management (get device status, get/change device settings)
- Log management (get job history)
- Mailbox and document management (list documents in mailbox, retrieve documents in mailbox, move/copy documents to other mailboxes and/or locations)
- Resource management (fonts, color calibration, etc.)

FQDN (Full Qualified Domain Name)

A fully qualified domain name (FQDN), sometimes referred to as an absolute domain name, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain, relative to the root domain. A fully qualified domain name is distinguished by its unambiguity; it can only be interpreted one way.

HID (Human Interface Device)

A Human Interface Device is a device specialized in sending output to and receiving input from human operators. The HIDs are defined in the USB HID class that in turn is part of the USB specification for PC peripheral devices.

iR (imageRunner)

Canon multi-functional devices that use UFR or UFR II as their standard page description language. They feature standard digital copying, network printing capabilities, and black-and-white and full-color network scanning capabilities.

iR-ADV (imageRUNNER ADVANCE)

The imageRUNNER ADVANCE is a new generation of Canon MFP that replaces the Canon imageRunner MFPs. All imageRUNNER ADVANCE machines have Send functionality as standard, being able to scan & send documents from the machine to destinations such as email, shared folders on a network or an FTP site.

LAN (License Access Number)

LAN is the abbreviation of License Access Number. A LAN is e.g. required for licensing MEAP applications via Canon's License Management System (LMS).

LDAP (Lightweight Directory Access Protocol)

LDAP is an application protocol for querying and modifying information services running over an IP network.

The current version is specified in RFC 4510 / RFC 4511.

MEAP (Multifunctional Embedded Application Platform)

MEAP is a Java-based application development platform that allows the creation of embedded applications for Canon multi-functional peripheral devices. Custom applications can be created to execute on the device itself.



For further information please refer to:

MEAP Enabled Product List

(https://www.developersupport.canon.com/meap_supported_products)

MFD / MFP (Multifunctional Device / Printer)

A Multifunctional Printer (MFP) is a networked device that is able to print, copy, scan, and/or fax. In addition, Canon MFPs have mailboxes on the device in which users can store document images for later retrieval. It is also referred to as MFD (Multifunctional Device).

RIA (Rich Internet Application)

A RIA is an *application* that makes use of the *internet* to deliver *rich* content. Usually, the RIA runs client-side, within the user's browser, communicating with an application server that is responsible for the data manipulation. The rich user experience is achieved with the help of JavaScript, Adobe Flash, Microsoft® Silverlight, and other plug-ins. An RIA does not require software installation.

RUI (Remote User Interface)

A tool that allows the remote administration of Canon MFPs via a web browser.

SMS (Service Management Service)

A service that allows MEAP applications to be managed on a MEAP device using a remote Web Browser. SMS can be used to install/uninstall and start/stop MEAP applications. It can also be used to obtain information about MEAP applications installed on a device.

The Service Management Service provides a run-time environment for System Services and custom applications (also called custom services). This includes managing services throughout their life-cycle on a MEAP device.

SSO (Single Sign-On)

Single Sign-On is a one-time logon method. It enables a user to log on and gain access to all devices and services of a domain with a single authentication.

The iR's display is locked until the user has entered valid credentials.

Index

A

Access Control	44
Access Management System	8
Activation.....	25
Active Directory	8, 38, 45
Active Directory Server Requirements	8
AD (Active Directory)	70
AD Credentials (Active Directory Credentials)....	70
Adding a Device	56
Administration Tool.....	23
Administration Tool Login	23
AMS - Access Management System	68
AMS (Access Management System)	70
Appendix.....	65
Application.....	6
Authentication	
Mode	36
Authentication Mode	2, 36

C

CDS (Content Delivery System)	9, 70
Certificate	57
Components	6
Configuration.....	23
Cost Table	59
CPCA (Common Peripheral Controlling Architecture).....	70
Creating a Certificate	57
Creating a Report.....	59
Customize	47, 49
Customized Language Strings.....	49

D

Department ID	44
Disclaimer	3
Domain Authentication Mode	3

F

FQDN (Full Qualified Domain Name).....	71
--	----

G

General Architecture	1
General Introduction	1

H

Hardware	65
Hardware and Optional Items	7
HID (Human Interface Device)	71
Home Folder	28, 30
Home Folder Settings	30
How to obtain Log Files	64

I

Image Login.....	4, 33
Image Login and Image Login + PIN.....	33
Image Login and Image Login + PIN.....	33
Image Login or Image Login + PIN	4
Import	45
Import and Map Groups from Active Directory	45
Import/Export.....	41
Installation	9, 16
Installation via Content Delivery System (Device UI)	9
Installation via Content Delivery System (Remote UI)	14

Introduction.....	1	R	
iR (imageRunner).....	71	Requirements	7
iR-ADV (imageRUNNER ADVANCE).....	71	RIA (Rich Internet Application)	72
L		Rich Internet Application	7
LAN (License Access Number)	71	Roles	43
Language Strings see Customize	49	Preconfigured	43
LDAP (Lightweight Directory Access Protocol) ...	71	RUI (Remote User Interface)	72
Local Authentication Mode	2	S	
Log Files	64	Secure Print	64
Login Type.....	33	Secured Print	64
Login Types	3, 33	Security	62
M		Security Aspects.....	62
Main Page	25	Setup.....	32
Manual Installation via Remote UI	16	SMS (Service Management Service).....	72
MEAP	6	Software Requirements.....	7
MEAP (Multifunctional Embedded Application Platform).....	71	SSO (Single Sign-On)	72
MFD / MFP (Multifunctional Device / Printer) ...	72	Supported Card Readers.....	67
O		System Manager	
Open Source License Information	7	ID And Password.....	32
Optional Items	67	Settings	43
P		System Manager Settings	43
Printer Driver and AMS Printer Driver Add-in Module	8	System Requirements.....	7
Profile	31	U	
Profile see User	31	uniFLOW	
Proximity Card		Upgrade	64
Proximity Card and Proximity Card + PIN Login	35	uniFLOW Server Mode.....	3
Proximity Card Reader and Card Types.....	67	Uninstallation	19
Proximity Card and Proximity Card + PIN	35	Update	18
Proximity Card Login or Proximity Card Login + PIN	4	Upgrade to uniFLOW Server	64
		Usage Tracker	7, 53
		Usage Tracker (Rich Internet Application).....	7
		USB Device Port	68
		User.....	26

Create	26
Profile	31
User Name and Password Login.....	5, 36
User Name / Password	36

User Name and Password Login	5
Users	26
W	
Web Browsers.....	7

