Universal Login Manager

Installation and Configuration Guide

V4.1.2

Disclaimer

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 Software of Adlib Software; Adobe®, Adobe® Reader, Acrobat®, Distiller®, PostScript® and products of the CREATIVE SUITE(S) of Adobe Systems Incorporated; Apple®, the Apple® logo, Mac®, Mac OS®, Macintosh®, iPhone®, iPad® and AirPrint® of Apple Inc.; CANON, imageRUNNER, imageRUNNER ADVANCE, MEAP, CPCA, AMS, iW AMS, iW Desktop, iSend, iW SAM of Canon Inc.; Crystal Reports of Business Objects SA, as of July 1, 2008: BusinessObjects of SAP; eCopy™, eCopy ShareScan®, and eCopy ScanStation® of Nuance Communications, Inc.; Foxit Reader of Foxit Corporation; Google Docs of Google Inc.; Google Cloud Print is a trademark of Google Inc., Helix™ Production Workflow is a trademark of NT-ware Systemprogrammierung GmbH; Hewlett Packard, HP, LaserJet, and PCL of Hewlett-Packard Company; iOS® of Cisco Technology Inc.; I.R.I.S. Group s.a.; JAWS pdf courier™ are trademarks of Global Graphics SA.; Microsoft®, Windows®, Windows Vista®, Windows 7®, Internet Explorer®, Internet Information Server, Microsoft® Word, Microsoft® Excel, SQL Server® of Microsoft Corporation; Neevia Document Converter ProTM of Neevia Technology; NetWare, Novell®, Novell eDirectory® of Novell Inc.; OpenOffice.org™ of Oracle Corporation; PAS™ of Equitrac Corporation; PosterJet of Eisfeld Datentechnik GmbH & Co. KG; Red Titan EscapeE of Red Titan Limited; NETAPHOR®, SiteAudit™ are trademarks of NETAPHOR SOFTWARE Inc.; Therefore™ of Therefore; UNIX® of The Open Group; uniFLOW®, uniFLOW®, uniFLOW Serverless Secure Printing®, MIND®, microMIND®, and MiCard® are registered trademarks of NT-ware Systemprogrammierung GmbH; pcProx®, AIR ID® are registered trademarks of RFIdeas Inc.Readers; CASI-RUSCO® is registered trademark of ID Card Group; Radio Key® is registered trademark of Secura Key; GProx™ II is unregistered trademark of Guardall; HID® ProxHID is registered trademark of HID Global Corporation; Indala® is registered trademark of Motorola; ioProx™ is unregistered trademark of Kantech.

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

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

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

PLEASE 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.

Tuesday, November 19, 2013, Bad Iburg (Germany)

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

Symbols

Text Styles

Text that appears in this style is used for screen text that appears in the uniFLOW user interface and on user interface controls.

Text that appears in this style is used for User entries on screen, text that the user actually has to type in.

Text that appears in this style is used for hyperlinks to an external web page, or internal links to other pages of this manual.

`Text that appears in this style is used for code examples: XML code, variables or regular expressions.`

Pictograms

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

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

Region Specific Feature: In case some features of uniFLOW are not universally available, this icon will indicate it.

Link to an external reference within the WWW.

Detailed explanation of configuration settings or operational procedures.

Screenshots, pictures and graphics

This manual contains screenshots of the software, graphics explaining relations and pictures of products. All visuals are up-to-date at the time of writing. However, please note, that these visuals are subject to change.

Copyright and Contact

In case of errors or improvement suggestions please contact documentation@nt-ware.com.

Contents

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 to the Universal Login Manager

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.

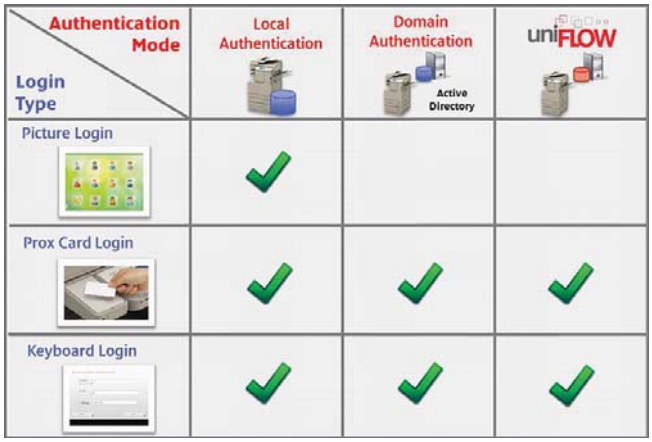
In addition, Universal Login Manager can be used as a login application for uniFLOW. Users can easily migrate to a uniFLOW solution without sacrificing their initial investments such as MiCard PLUS card readers.

2.1 General Architecture of Universal Login Manager

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.



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.

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.

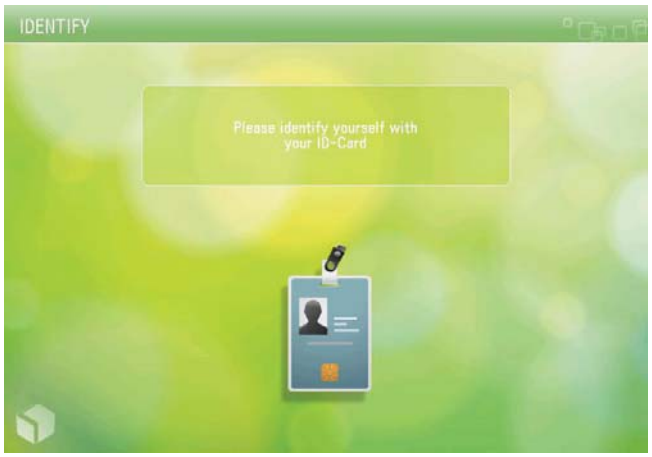
Up to 48 user icons can be registered and uploaded as account image through the ULM Configuration on the remote UI. You can select ***Image Login*** or ***Image + PIN*** mode, in which case an additional PIN code input will also be required for login.

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.

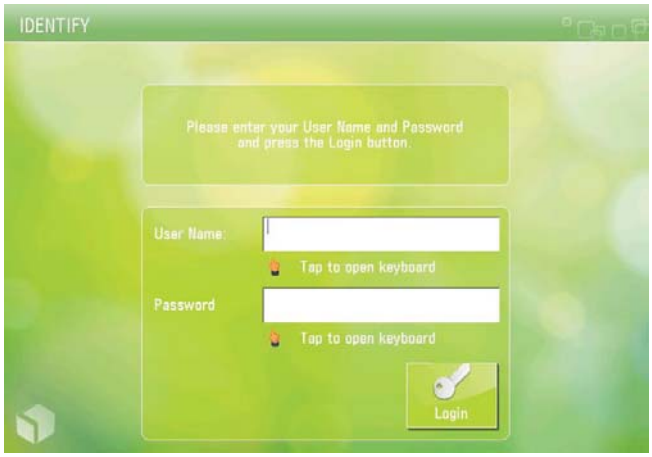
The supported card reader must be connected to the device. The USB Device Port option is recommended for fitting the Card Reader securely inside the device. Proximity Card Login works with all authentication modes (Local, AD, uniFLOW). You also can set a PIN code for additional security on login.

The supported Proximity Card Reader is the MiCard PLUS.



2.3.3 User Name and Password Login

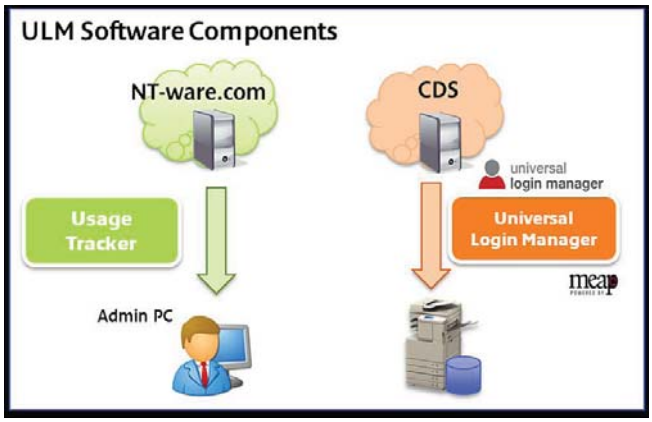
Similar to SSO-H which is standard on MEAP enabled devices (iR and imageRUNNER ADVANCE), you can login with the user name and password registered in the user database. All authentication modes (Local, AD or uniFLOW) are possible.



3 Universal Login Manager Components

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

- Universal Login Manager : MEAP application.
- ULM Usage Tracker : Web browser plug-in application (RIA).



3.1 Universal Login Manager (MEAP Application)

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 Universal Login Manager 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.

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 60).

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.

- These web browsers are supported by the Universal Login Manager:
  - Internet Explorer for Windows (version 7 or later)
  - Chrome (version 21 or later)
  - Mozilla Firefox (version 15 or later)
  - Opera for Mac (version 12 or later)
  - Safari (5.1 or later)
- These web browsers are supported by the ULM Usage Tracker:
  - Internet Explorer for Windows (version 8 or later).
  - Chrome (version 21 or later)
  - Mozilla Firefox (version 15 or later)
  - Opera for Mac (version 12 or later)
  - Safari (5.1 or later)

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 10.0 or higher.

Due to limitations of IE8/9 the import functionality for cost tables is not supported in these browsers in ULM up to version 4.0.1. From ULM V.4.0.2 onwards, these browsers are fully supported.

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 Universal Login Manager Installation

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

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

- Content Delivery System - License Access Number (LAN) required
  - From the local UI
  - From the remote UI (delivered installation)
- Manual Installation - .jar file and license file are required
  - From the Service Management System (SMS)

Required Items Installation Methods	Default Admin Password	License Access Number	Application Files [.jar/.lic]	Networked PC with Web Browser	Internet Connection
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 license file from the Canon Software Download Center and install using SMS.

If you install the application via the Service Management Service (SMS), the End User License Agreement (EULA) will be displayed and you will be prompted to accept it. If you do not accept it, the installation will abort.

5.1 Installation via Content Delivery System

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

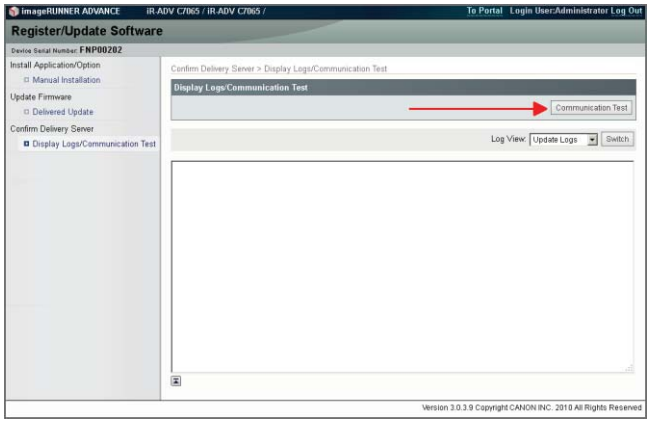
Universal Login Manager V4.1 LAN: R4ST-R5CP-77RL-JD3D

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

Before you install the MEAP application 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> Lisence/Other > Register/Update Software > Display Logs/Communication Test



Local UI

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

CDS Install From Local UI

Please follow the steps described below:

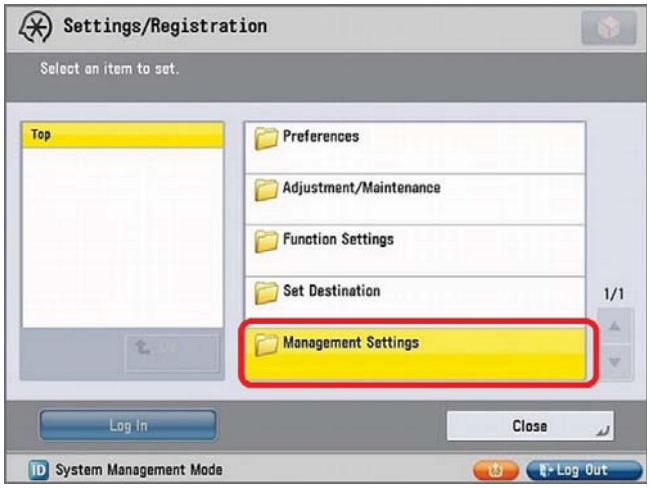
- From the MFP's touch panel, press ***Setting and Registration*** and login as system manager (if required).

The default user name/password of the imageRUNNER ADVANCE are

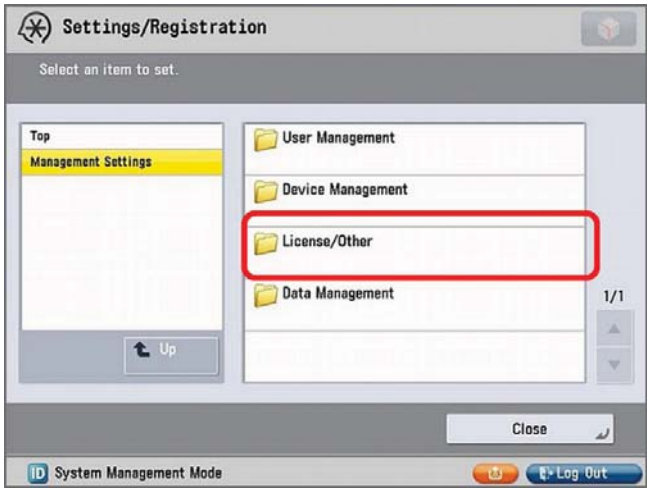
User Name : 7654321

PIN : 7654321

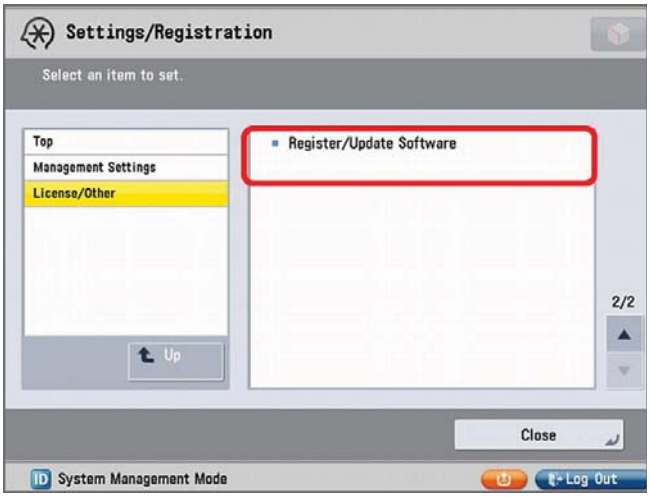
- From the ***Settings/Registration*** menu select ***Management Settings***.



- Select ***License/Other***.



- Select ***Register/Update Software***.

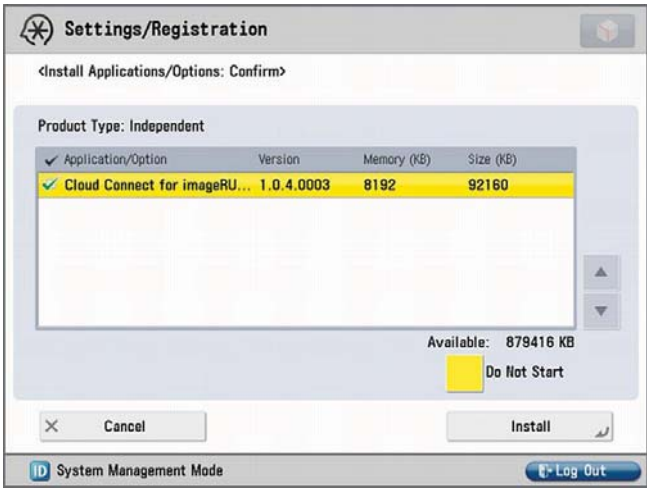


- Click ***Install Applications/Options***.

- Enter the sixteen-digit LAN. Each set of four digits must be entered separately:
  Universal Login Manager V4.1 LAN: R4ST-R5CP-77RL-JD3D

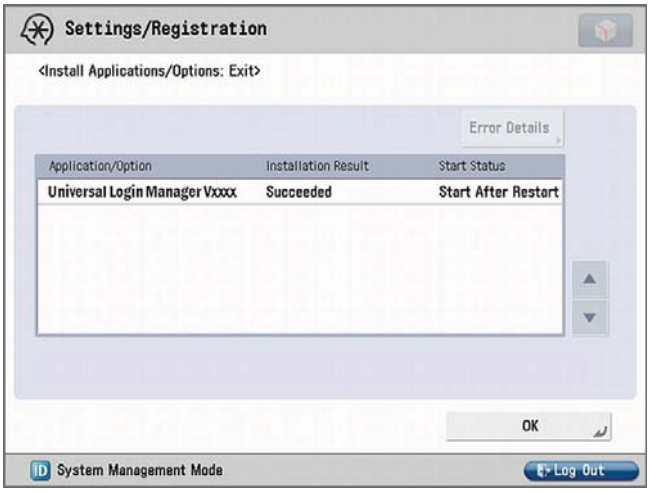
- Click on ***Start*** to start the installation process.

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



- Read and accept the license agreement. If you cannot comply with the terms of the license agreement you must not continue with the installation.
- The application will download and install.

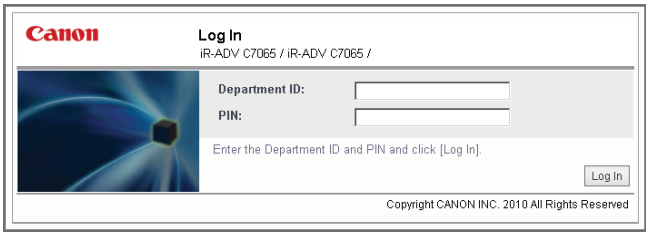
- When the application has finished installing, a new screen will appear prompting the user to complete the installation. Click the ***OK*** button on this screen to complete the installation.



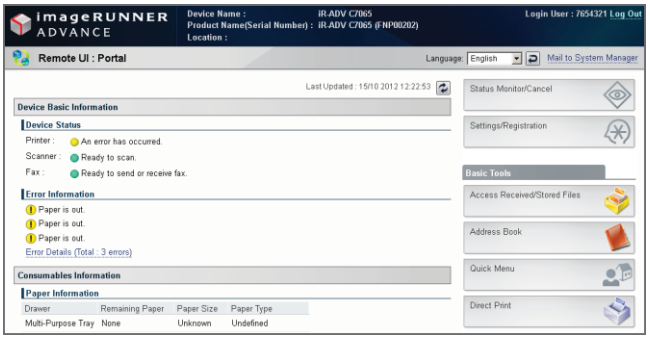
5.2 CDS Installation via Remote UI

Please follow the steps below:

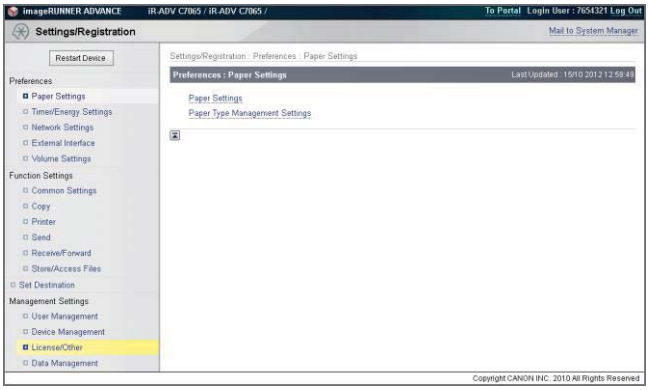
- Open your web browser and login to the remote UI by entering the URL: http://<ipaddress>:8000
  where <ipaddress> is the IP address of the device on which you wish the Universal Login Manager to be installed.
  The default user name and password of the imageRUNNER ADVANCE are:
  User Name : 7654321
  PIN : 7654321



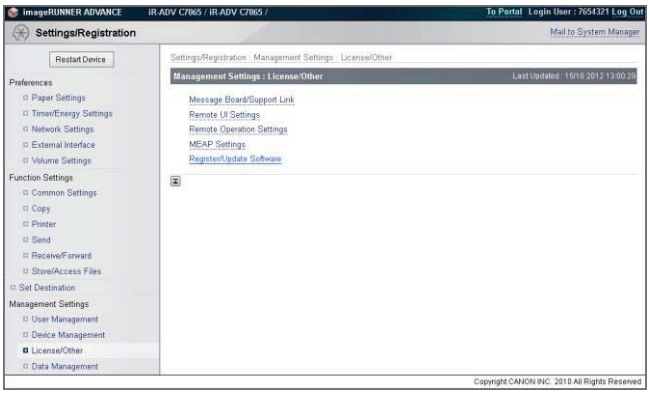
- From the ***Settings/Registration*** menu select the ***Management Settings***.



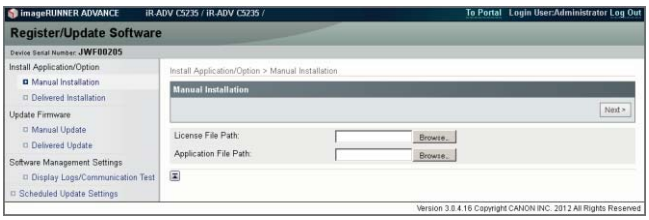
- Select ***License/Other.***



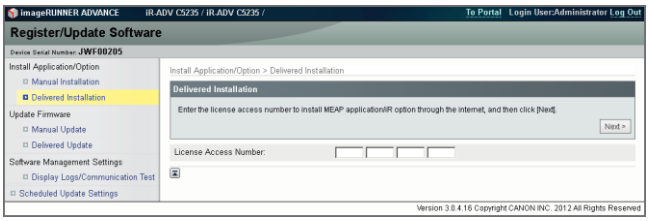
- Select ***Register/Update Software***



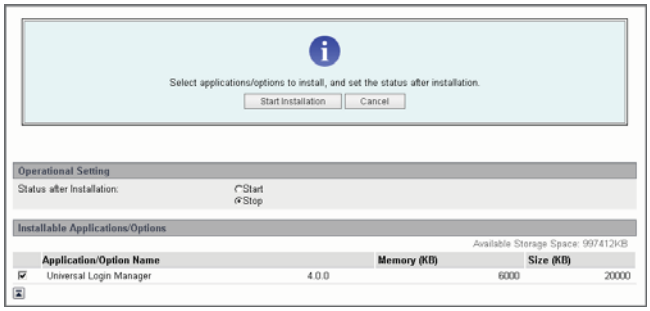
- Click ***Install Applications/Options***.



- Enter the sixteen-digit LAN. Each set of four digits must be entered separately: Universal Login Manager V4.1 LAN: R4ST-R5CP-77RL-JD3D

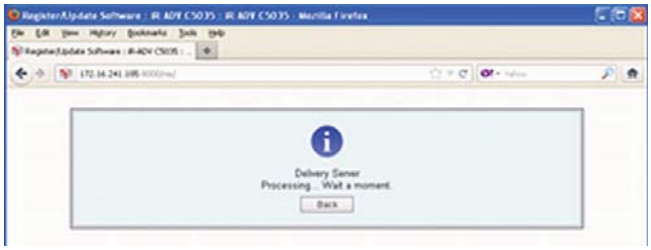


- Click ***Start*** to begin with the installation process.



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

- Read and accept the license agreement. If you cannot comply with the terms of the license agreement you must not continue with the installation.
- The application will be downloaded and installed.



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.

5.3 Manual Installation via Remote UI

The 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

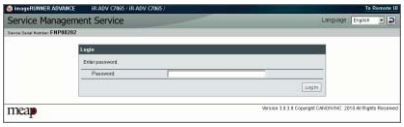
SMS (Service Management Service) is a servlet that enables you to access imageRUNNER ADVANCE devices via a network from a web browser and install or

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 accessibe from your PC.

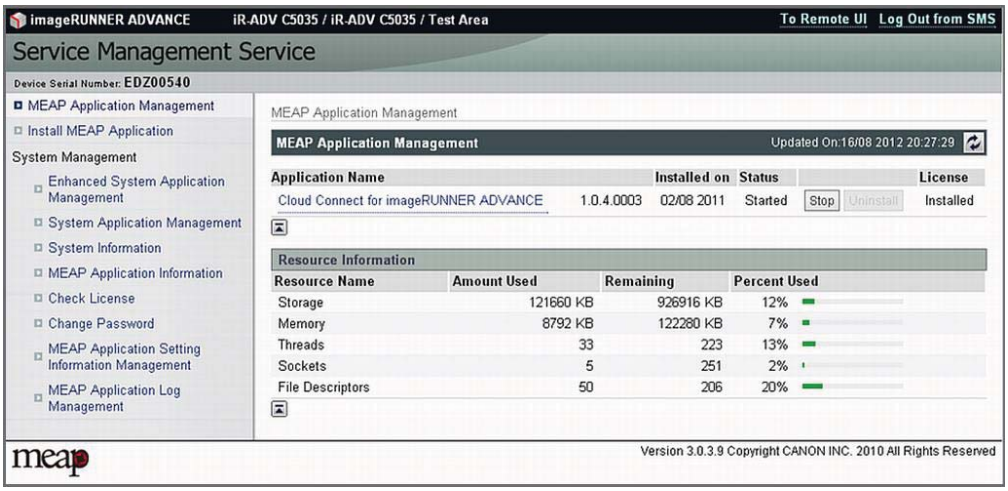
You can download the Universal Login Manager .jar file and the license file from the Canon Software Download Center http://www.support.cusa.canon.com for the USA and from the Canon Extranet ISG Service https://canonextranet.canon.ca for Canada.

For the installation via SMS follow the steps below:

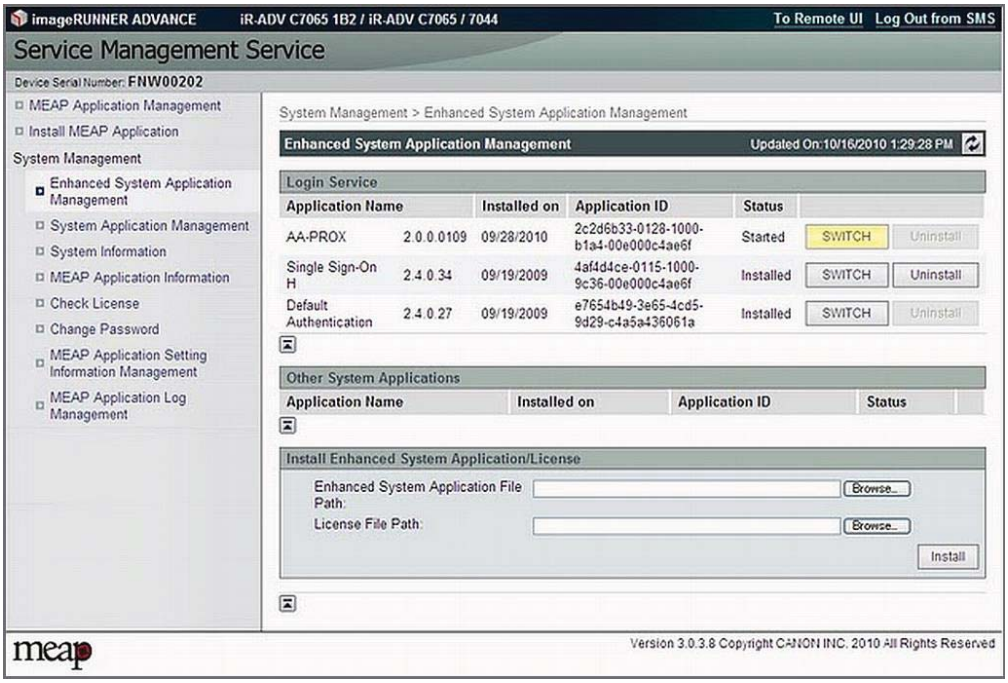
- Log in to the Service Management System (SMS).
  Open your web browser and login to the SMS by entering the following URL:
  http://<ipaddress>:8000/sms
  where <ipaddress> is the IP address of the device on which you wish the Universal Login Manager to be installed.



  Enter the appropriate password (case-sensitive) in the Password field.
  Click the ***Login*** button to login to the SMS.



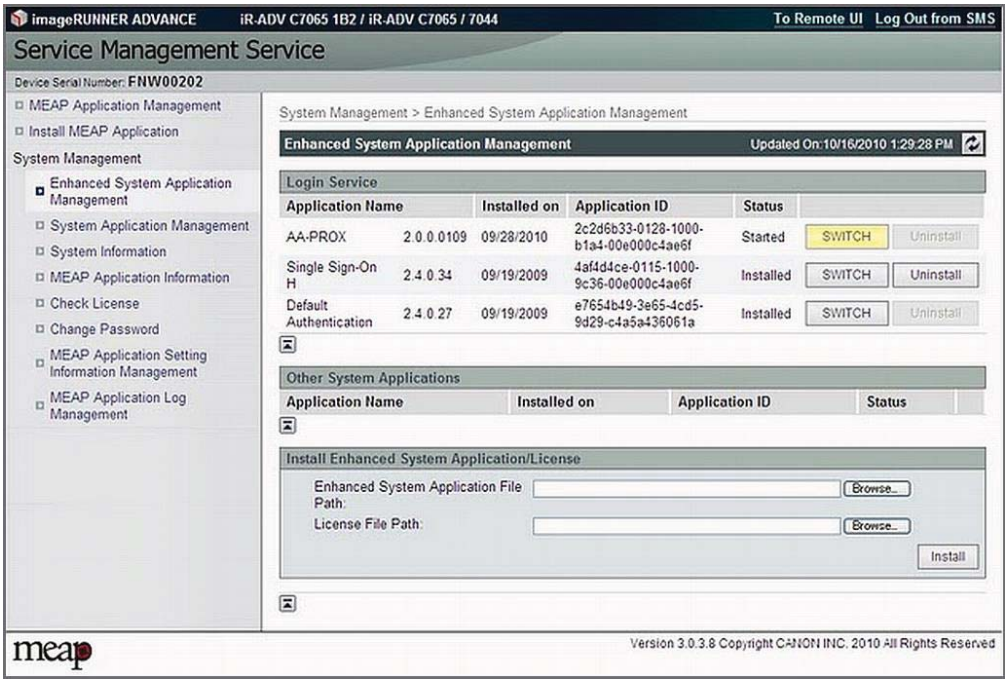
- Select ***Enhanced System Application Management.***



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.

- Browse to the Jar File.
  Click the ***Browse*** button next to the ***Enhanced System Application File Path*** field to select the Universal Login Manager .jar file.
- Enter the license file.
  Before you can proceed with the installation you must provide a license file. Click the ***Browse*** button next to the ***License File Path*** field to select the Universal Login Manager license file (ULM.lic).
- Start the installation.
  After you select the file path, click ***Install*** to proceed.

Click the button ***SWITCH*** to switch to the Universal Login Manager after the next restart.



6 Universal Login Manager 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 ***AD/LDAP***, ***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

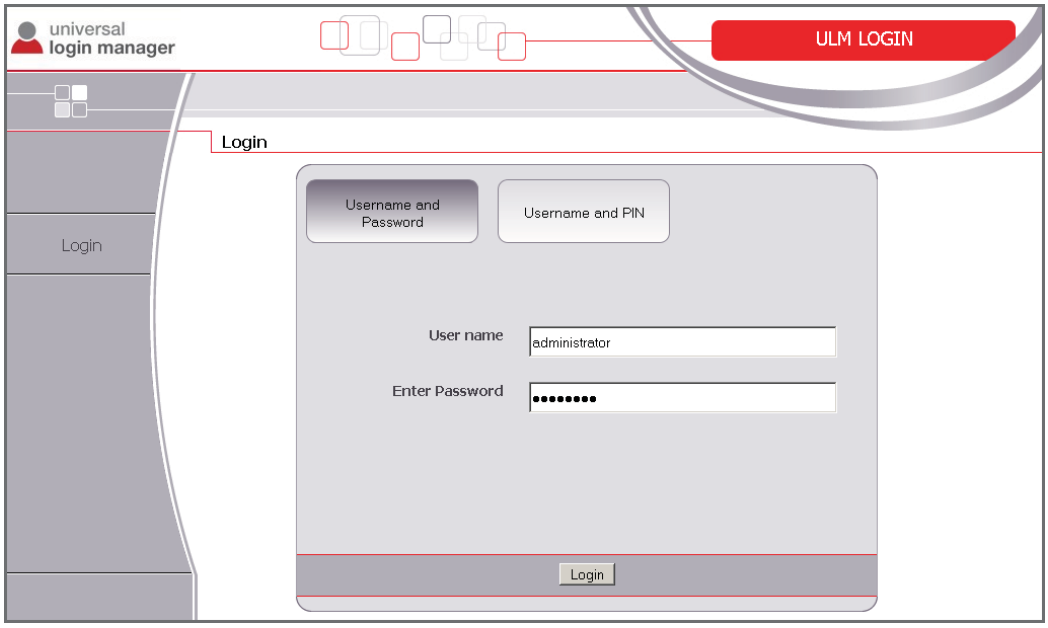
The Universal Login Manager RUI is always shown in the same language as the MEAP display on the device.

6.1 How to login to the Universal Login Manager Administration Tool

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

`http : // <IPaddress>:8000/ulm`

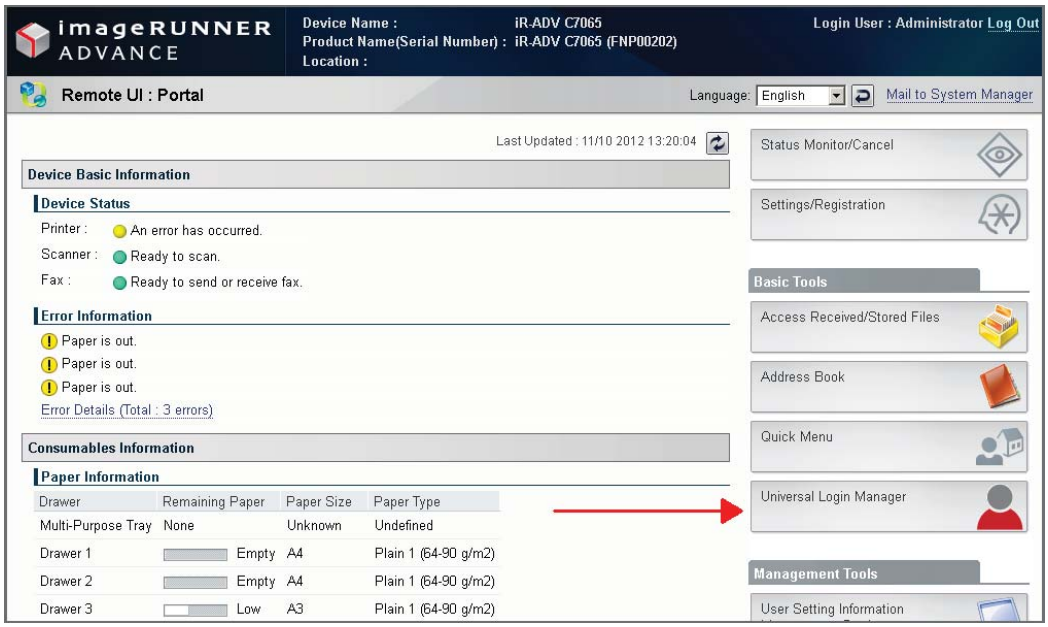
Here you can log in as administrator with the appropriate password. The default password for the administrator is "*password*". The password can be changed on the ***Profile*** page of the Universal Login Manager.



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.



6.1.1 Activation

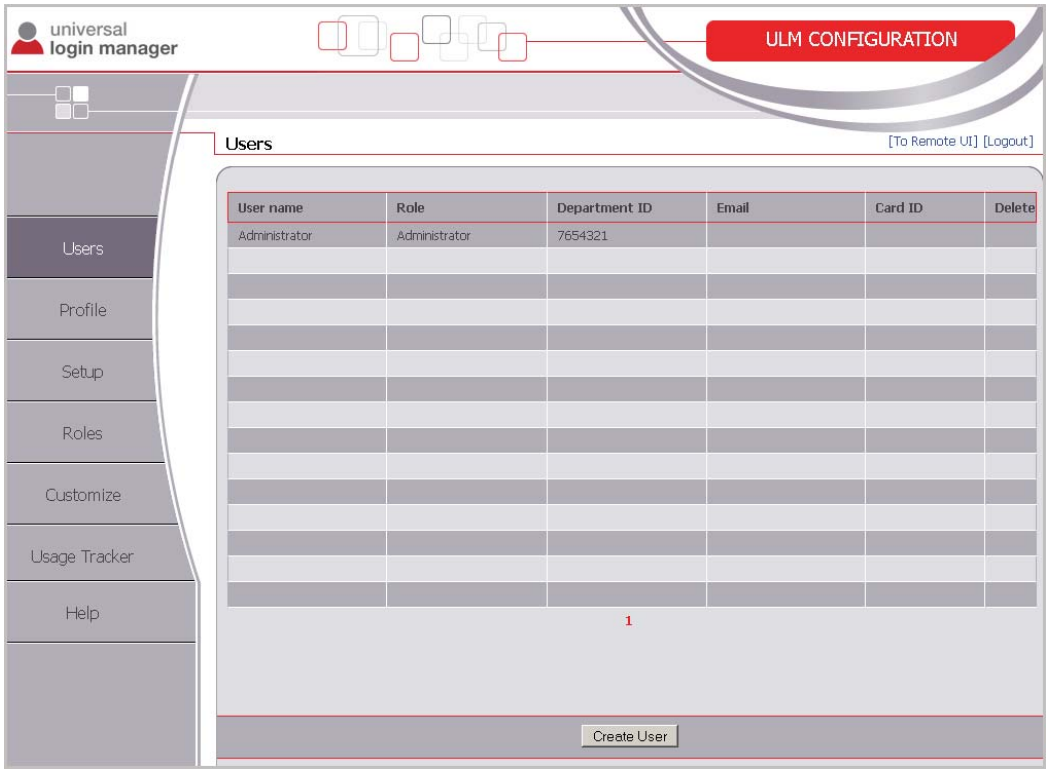
If this is the first time Universal Login Manager is started, it has to be activated. In order to do so, the computer from which you access your device must be connected to the internet. Enter the license code, press the ***Activate*** button and wait for the acknowledgment.

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

6.1.2 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 Universal Login Manager Usage Tracker
• ***Help***	Link to the Online Help

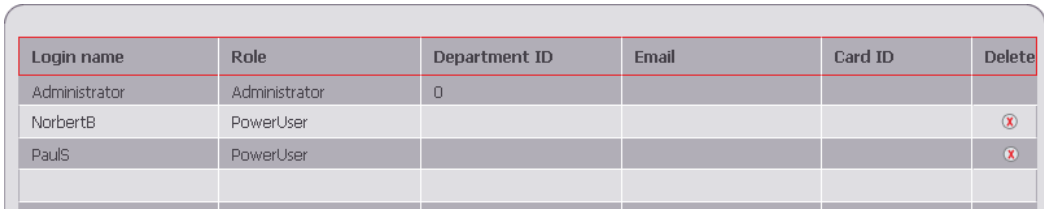


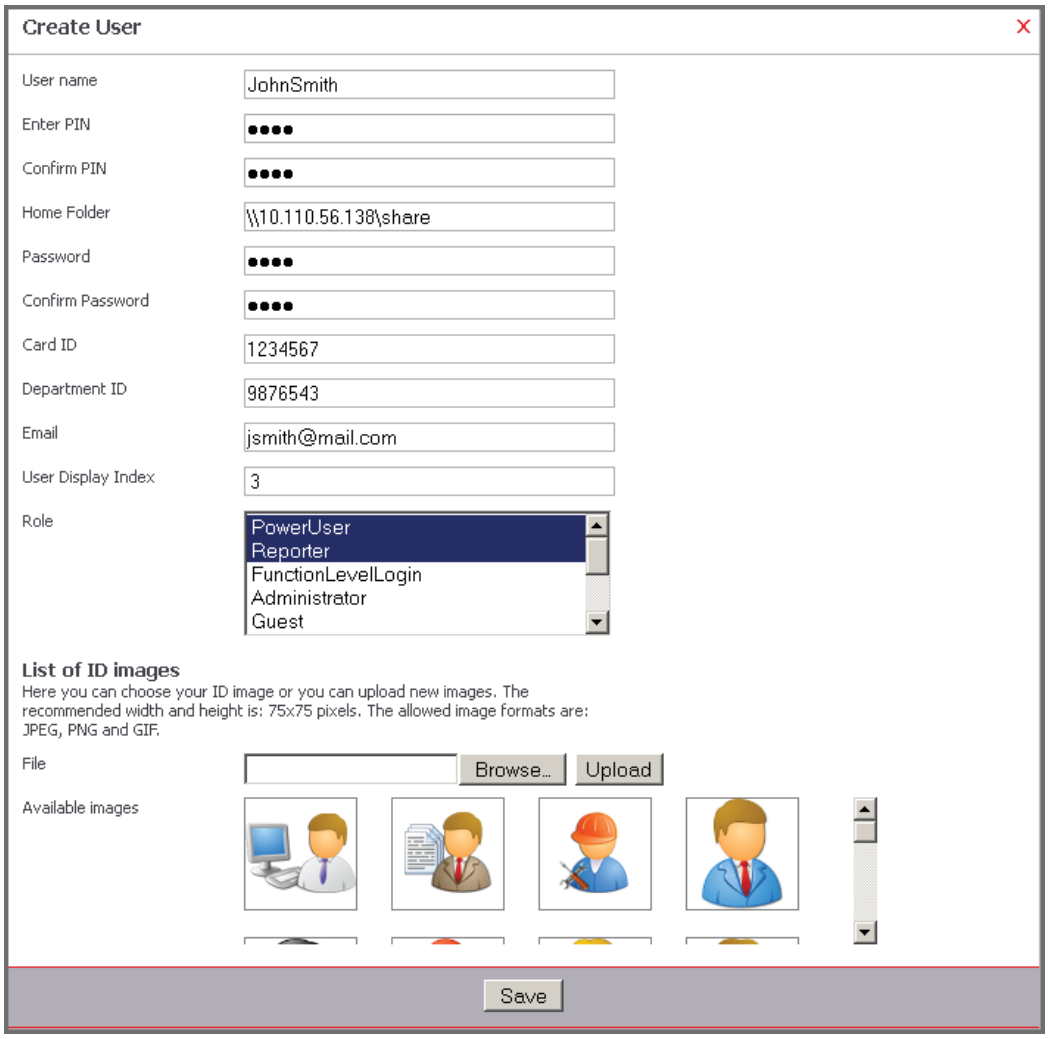
The sub-menus will be described in the following chapters.

6.2 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.





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 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.

Field	Description	Setting Conditions
Password / Confirm Password	The password used for the authentication presentation of type "username/password". Has to be confirmed in the second field.	
Card ID	The card number registered for the user's card.	The format depends on the type of card.
Departm. 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. Bigger images can slow down the user interface considerably.

6.2.1 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.

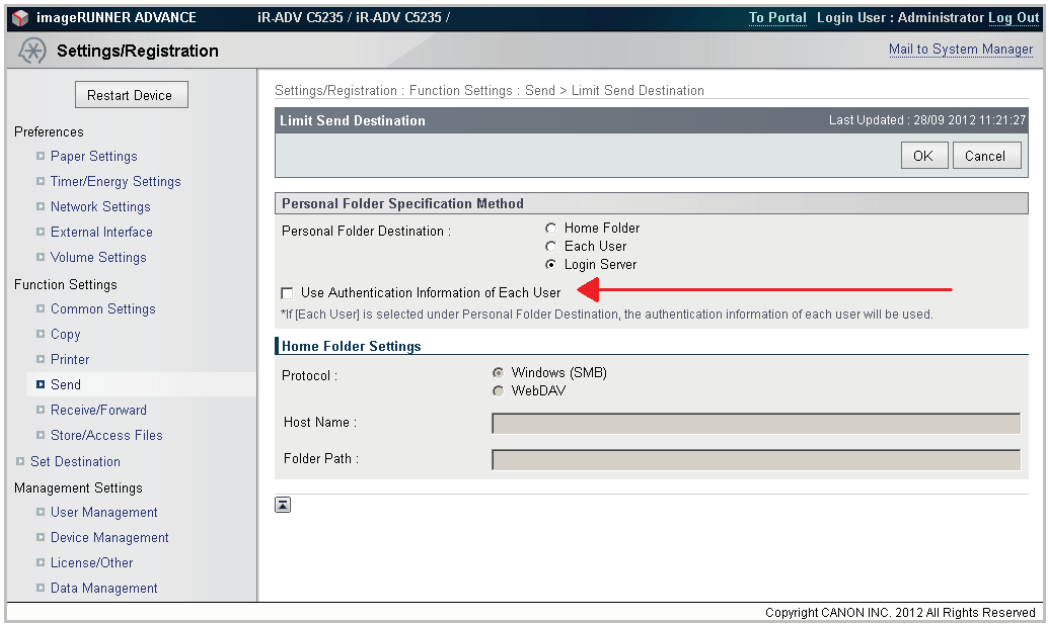
If ***Active Directory*** is used as the authentication provider **with user name/password login type**, the user credentials are automatically filled in every time the function is used.

- 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.

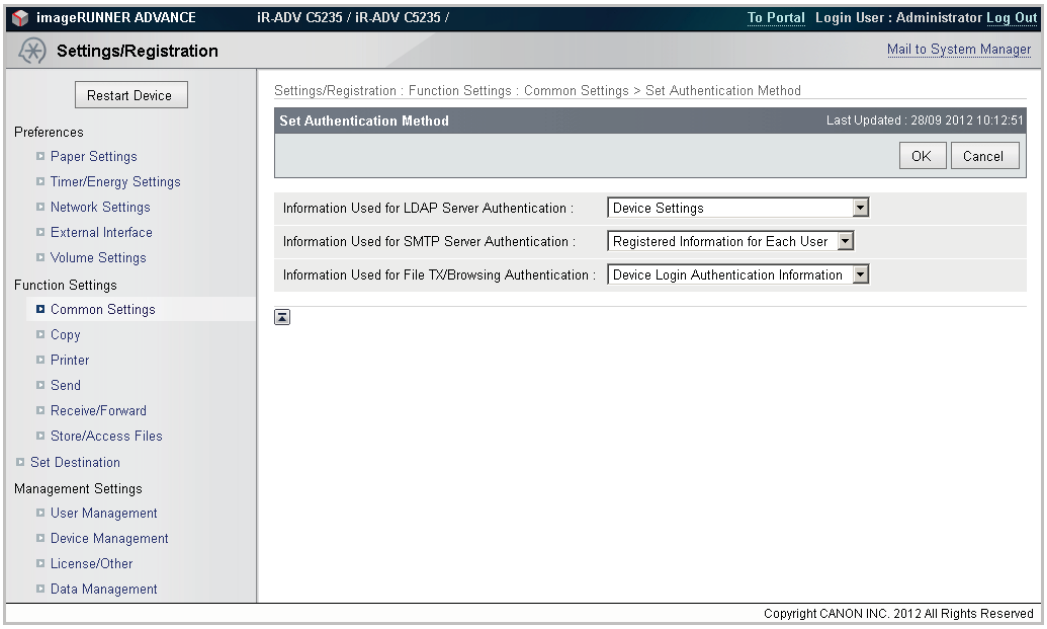
- Log in to the device as system manager and go to ***Settings/Registration*** : ***Function Settings*** : ***Send*** > ***Limit Send Destination***
  In the section ***Personal Folder Specification Method*** select ***Login Server***.
- The setting ***Use Authentication Information of each User*** influences 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***

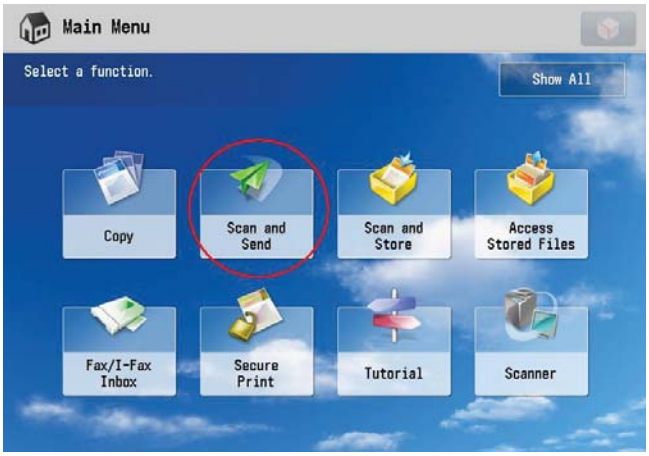
From the drop-down menu ***Information Used for File TX/Browsing Authentication*** select ***Device Login Authentication Information.***



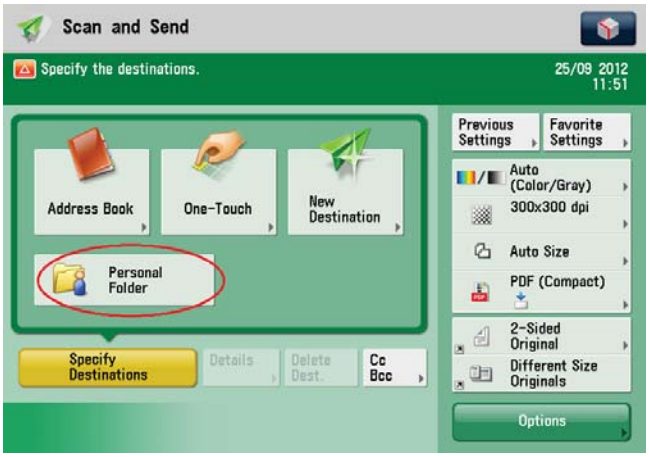
6.2.2 Home Folder Settings on the Device

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

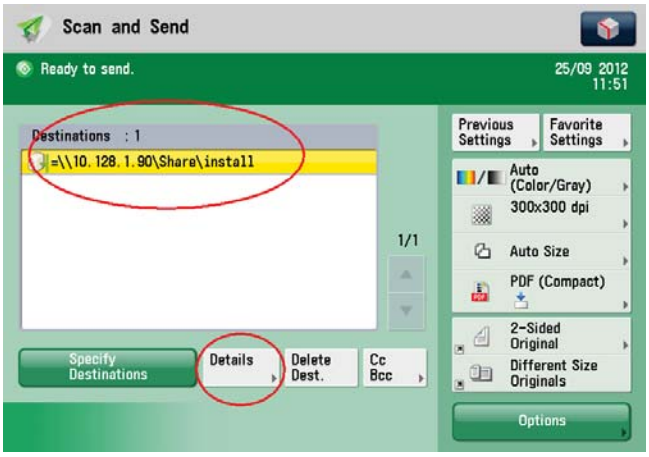
- After logging in the user opens ***Scan and Send***.



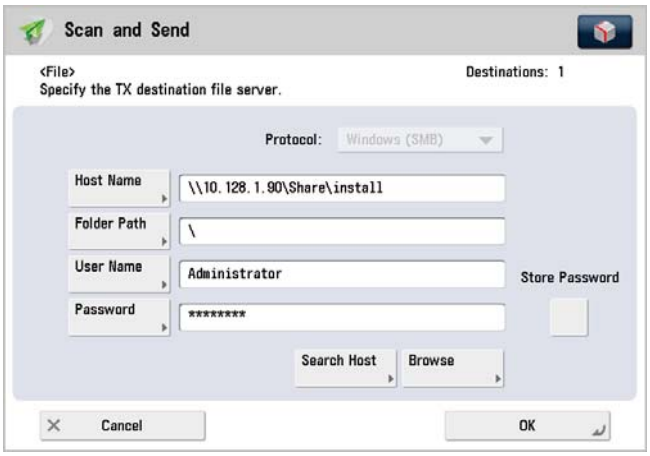
- Here the user opens the ***Personal Folder*** settings.



- 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.



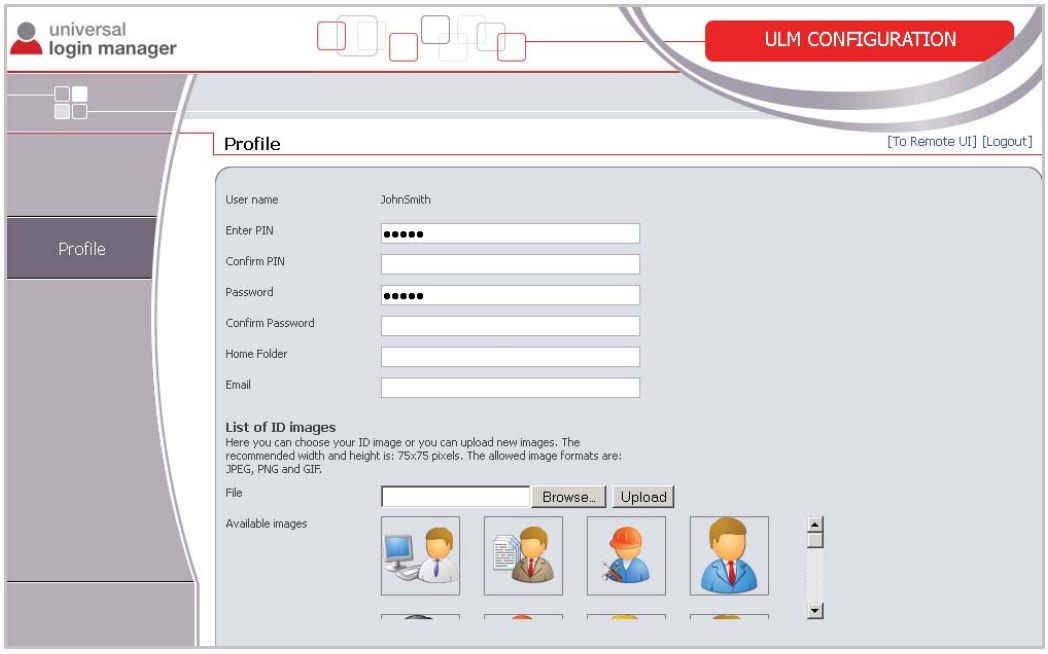
6.3 Profile

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 LDAP 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 21).

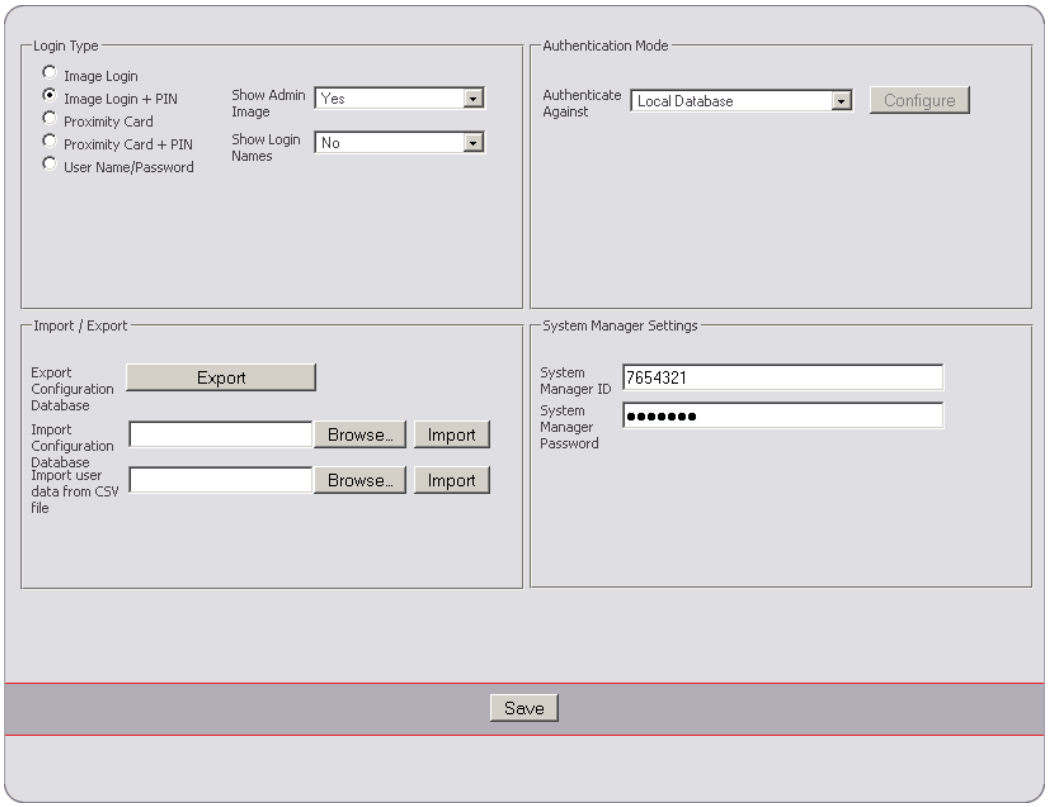


6.4 Setup

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

- Login type
- Authentication mode
- Import and export of the user database

- System manager ID and password



6.4.1 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

6.4.1.1 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.

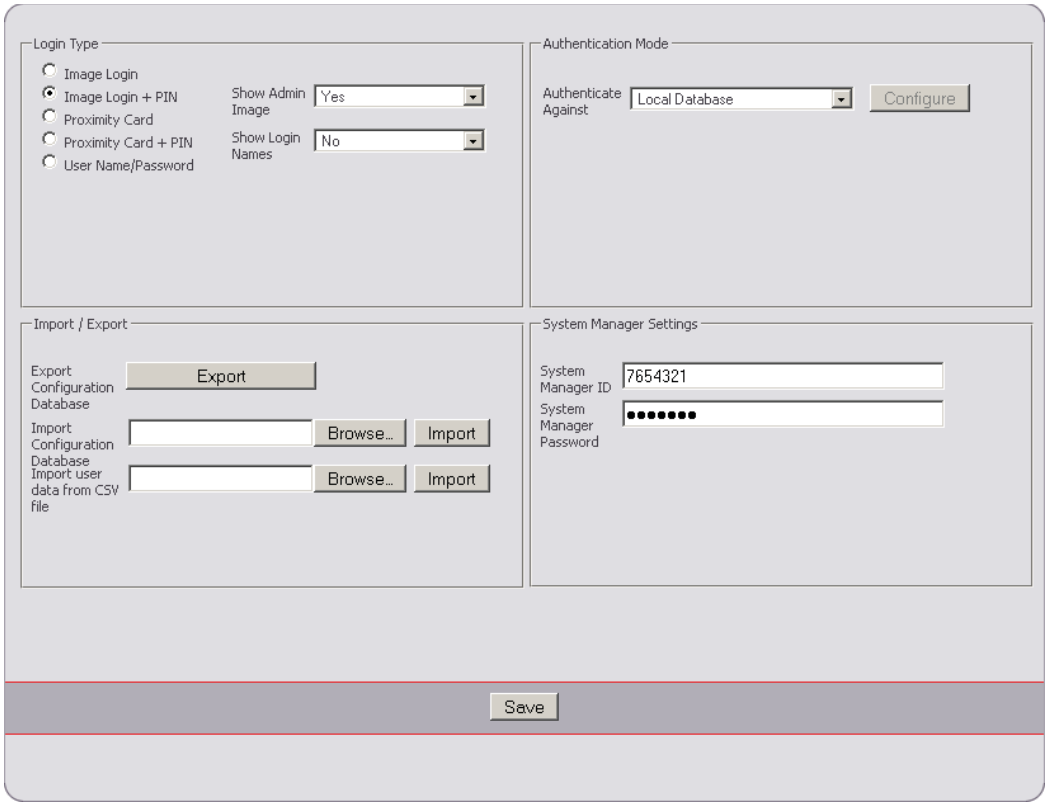
For both login types, up to 48 accounts can be configured. This login method only works with the setting ***Authenticate against Local Database***.

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 MEAP screen. Otherwise, only the ID images are shown.



6.4.1.2 Proximity Card and Proximity Card + PIN Login

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 MiCard PLUS Reader is required for this login type. This reader supports HID Proximity and MIFARE cards out of the box, but can be customized to support more than 35 different card types.

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 LDAP 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:

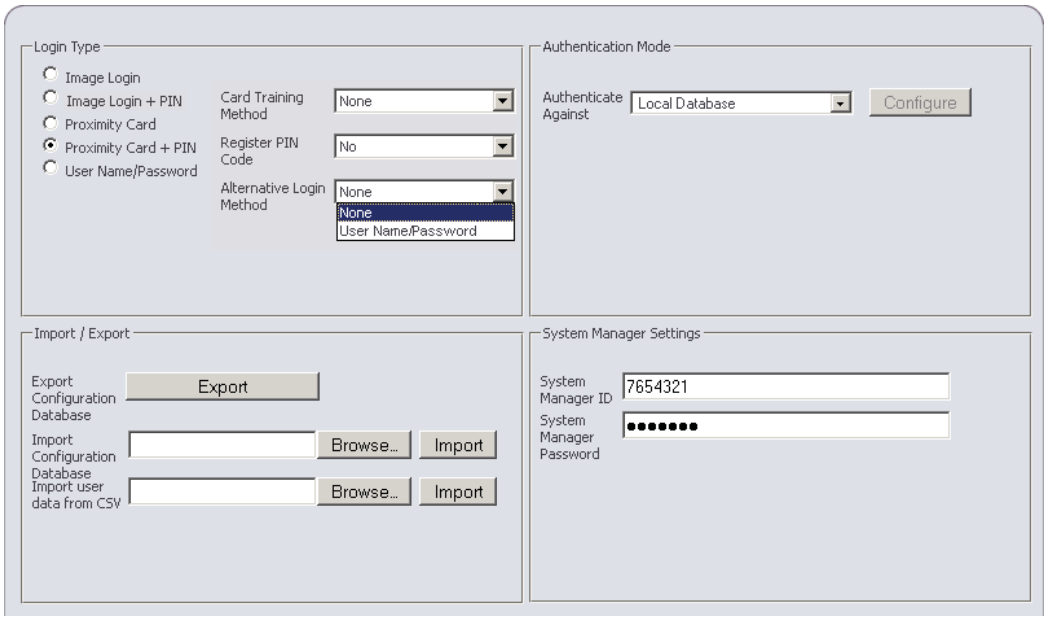
- ***Card training method***
  - ***None*** means that the card has to be registered manually by the administrator.
  - ***User Name/Password*** means that the card is registered by the user authenticating with user name and password.
- ***Register PIN Code*** (only visible for ***Proximity Card + PIN***)
  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 the MiCard PLUS Reader, a migration to uniFLOW is easy to accomplish.

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



6.4.1.3 User Name/Password Login

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.

6.4.2 Authentication Mode

In the ***Authentication Mode*** section, the administrator can configure how the user data is managed. The available options are:

Authenticate against:

- ***Active Directory***
  Connect to an Active Directory / LDAP server. See chapter Active Directory (on page 32) for further details
- ***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.

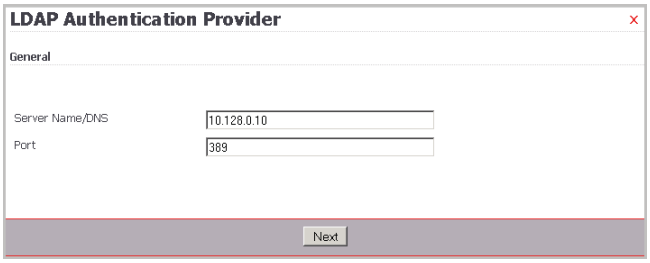
The changes under ***Authenticate Against*** will be saved automatically after selecting an Authentication Provider. Clicking on ***Save*** is not necessary.

6.4.2.1 Active Directory

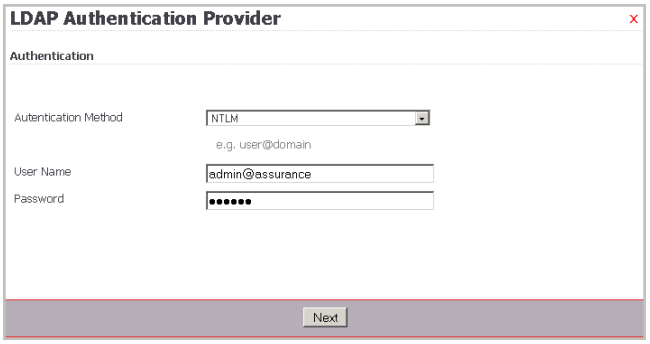
If ***Authenticate Against*** is set to ***Active Directory***, the ***Configure*** button can be used to set all necessary parameters for the connection.

The following screenshots show the steps to establish the connection:

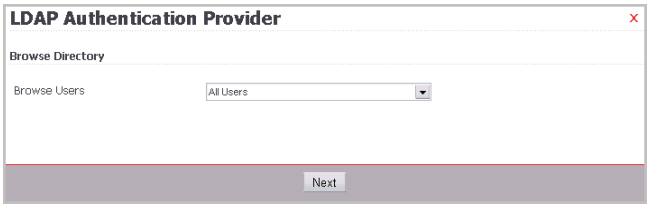
- Enter the server data.



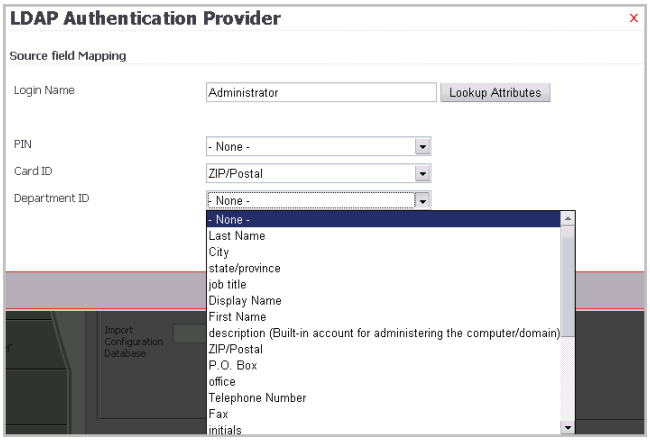
- Enter authentication data for a user who has reading rights in the AD in order to browse the directory tree. Write access is not necessary here. For ***Authentication Method,*** the following methods can be selected: ***NTLM***, ***Kerberos*** and ***LDAP***. The steps described below are identical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



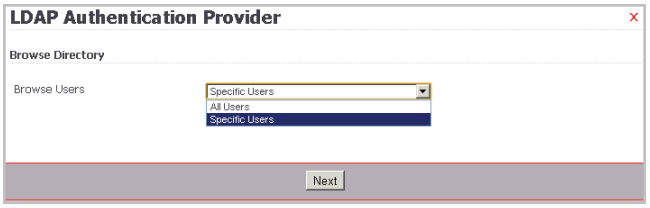
- Select how the directory tree is browsed. Select ***All Users.***



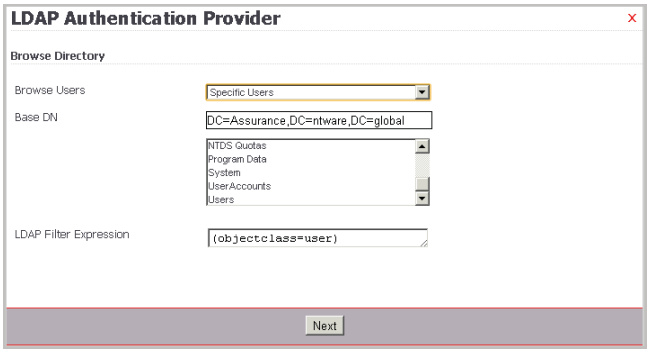
- Now you can simply map existing attributes to the user's profile. Press ***Save + Close*** to finish the process.



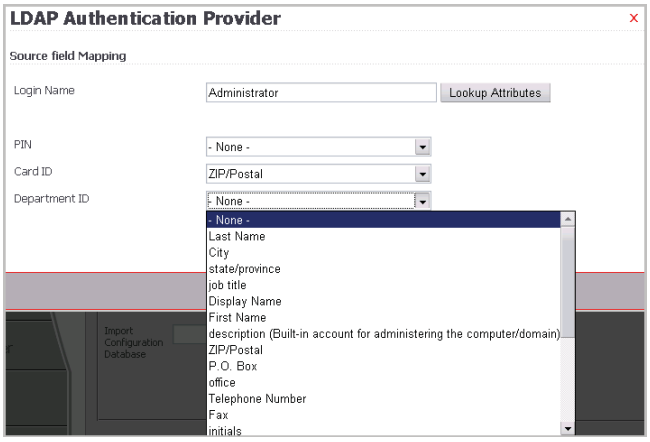
- Alternatively select ***Specific Users*** in one of the previous steps to enable detailed browsing of the directory tree.



- 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 readrights are required, except for changes that are made by users in their own profiles. Therefore the users need write access on their own AD 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.

6.4.3 Import/Export

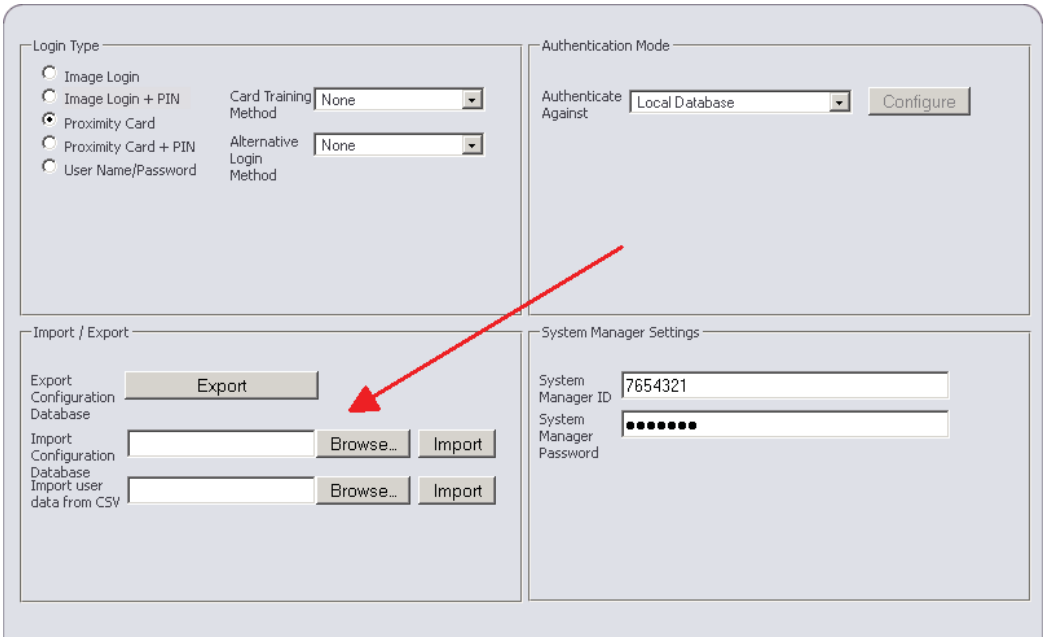
The administrator can export and import the configuration along with the user configuration. This can be done on the Setup screen. All system data including background images, icons, user data etc. will be saved. This works with all database types.

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

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.



It is also possible 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:

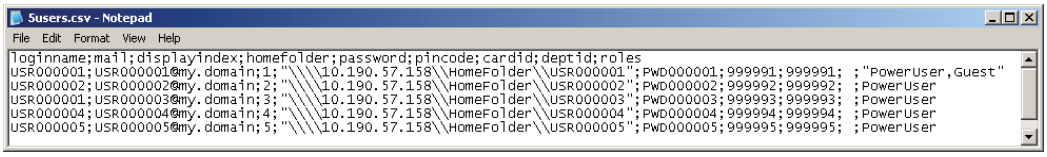
`loginname`, `mail`, `cardid`, `homefolder`, `pincode`, `password`, `deptid`, `roles`, `displayindex`

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"

Normally, these requirements are met when exporting a table as CSV file from Microsoft Excel.

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.



6.4.4 System Manager Settings

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

6.5 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 21)*** 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 Universal Login Manager Usage Tracker. The ***Reporter*** role also has access to the Usage Tracker. This role has been especially created to enable a non-admin user to enter the 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.

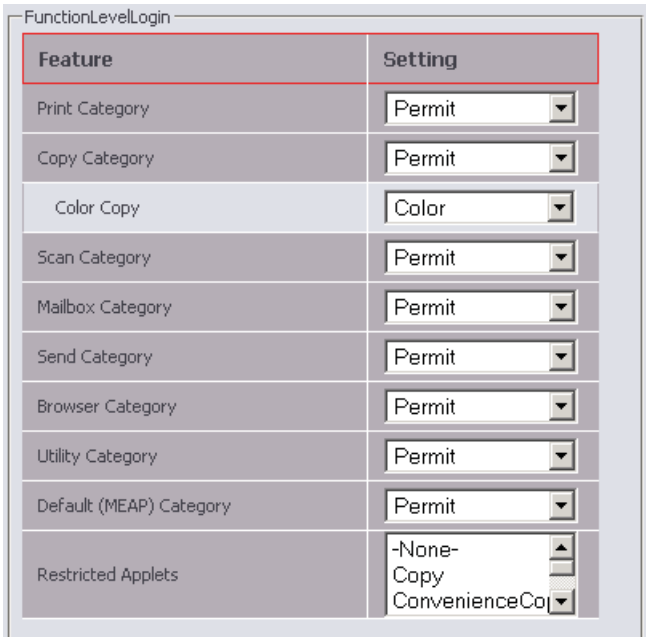
6.5.1 Access Control

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.

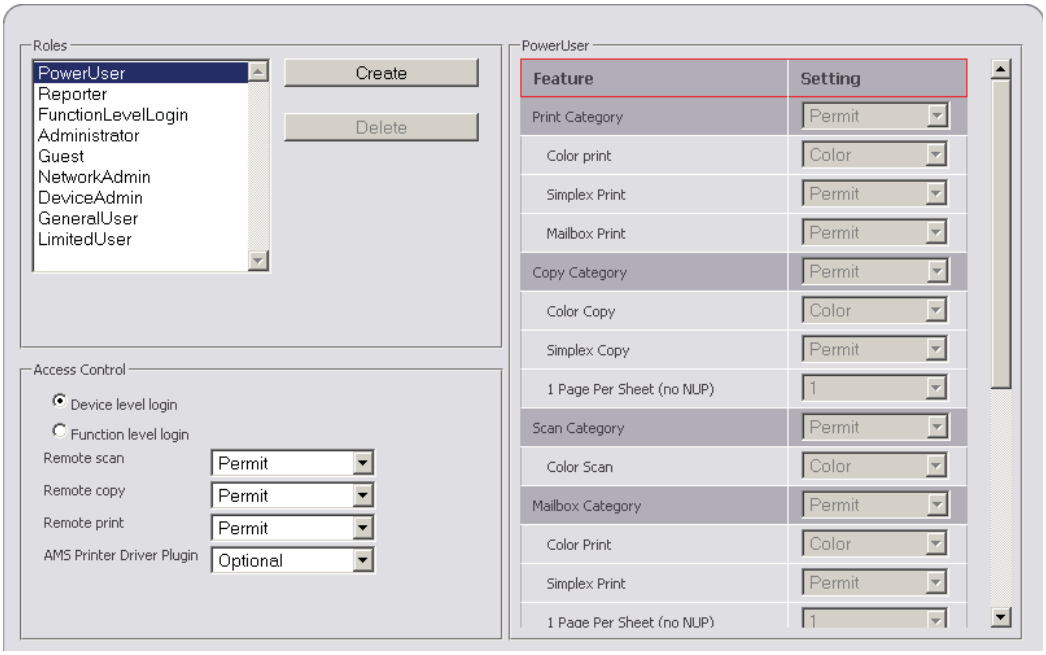


If ***Department ID Management*** is activated on the device, function level login only works if the department ID 9 was created manually without password beforehand.

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 Plugin*** controls, whether the use of this plugin is mandatory in order to use the AMS controlled functions or not.

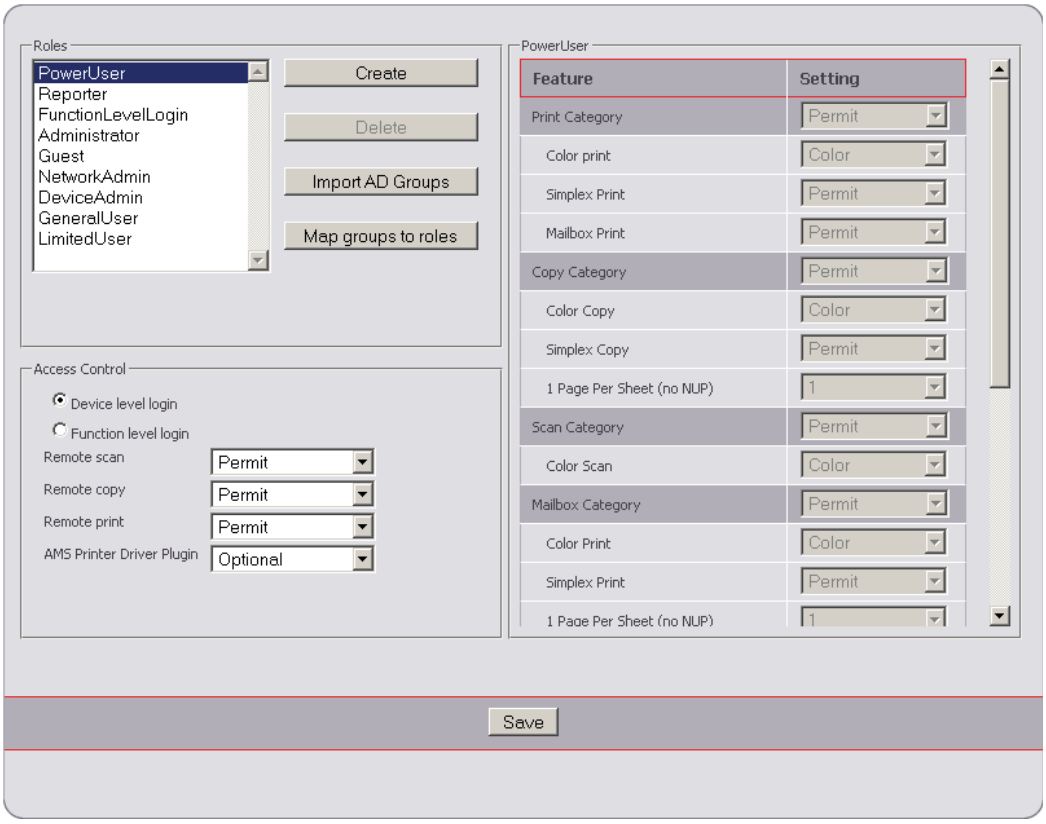
After having finished the configuration press the ***Save*** button to save the settings.

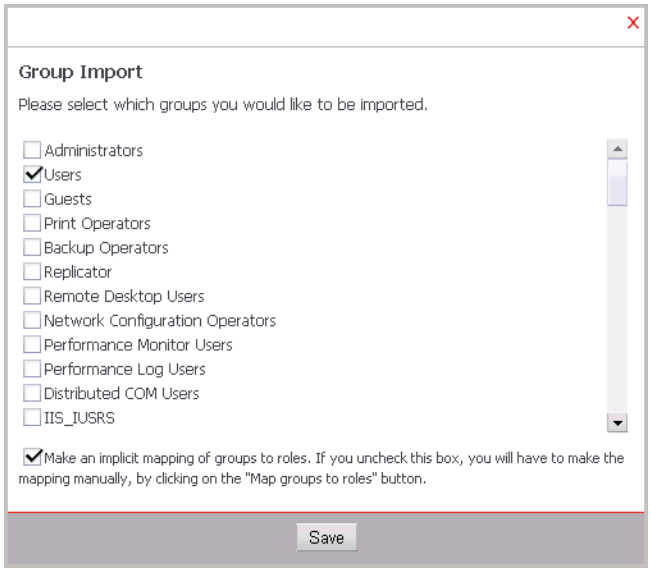


6.5.2 Import and Map Groups from Active Directory

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.

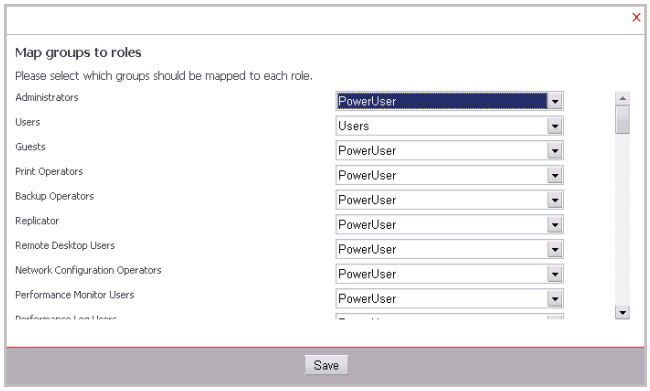




If ***Make an implicit mapping of groups to roles***... is checked, the imported groups are automatically mapped to the newly created roles of the same name. Otherwise the mapping has to be done manually.

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 th 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.



6.6 Customize

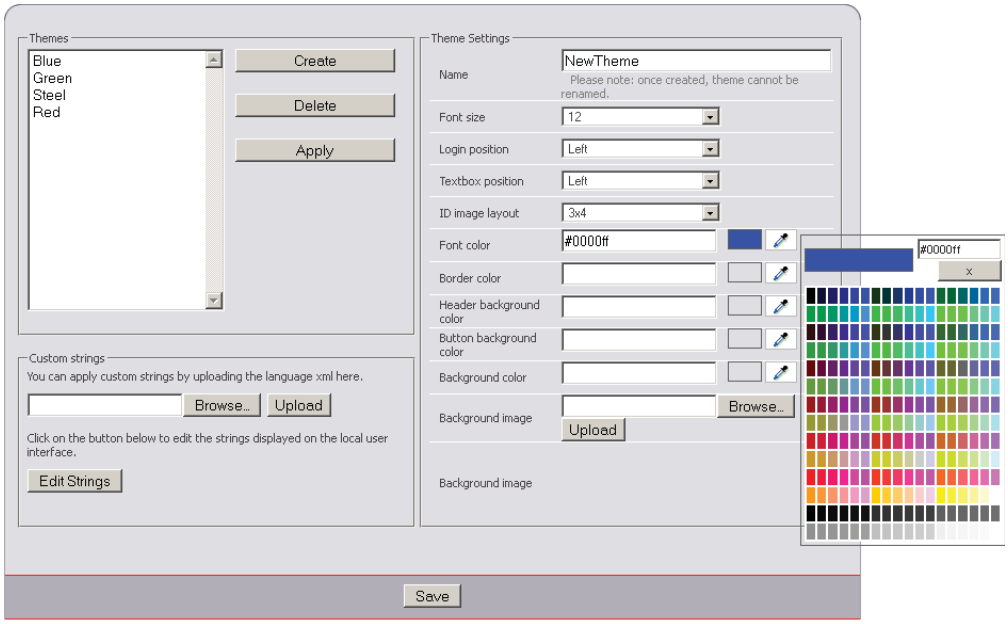
On this screen, the user interface can be customized. This can be done by selecting an existing theme or creating a new one from the ***Themes*** section. On the right side, a name can be entered for a new theme (existing themes cannot be renamed) and several settings like ***Font Size*** or various 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:

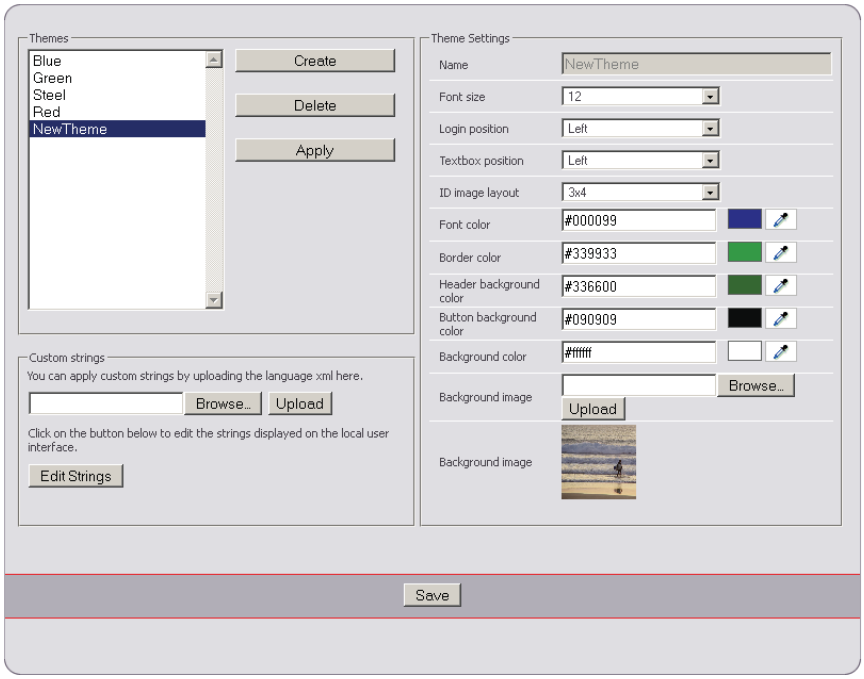
- ***Name*** - The name of the theme. Cannot be changed after a theme has been created.
- ***Font size*** - Font size of the texts shown.
- ***Login position*** - The position of the Login box. Can be ***Left***, ***Center, Right*** or ***Hidden***. If ***Hidden*** is selected, no card symbol will be 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

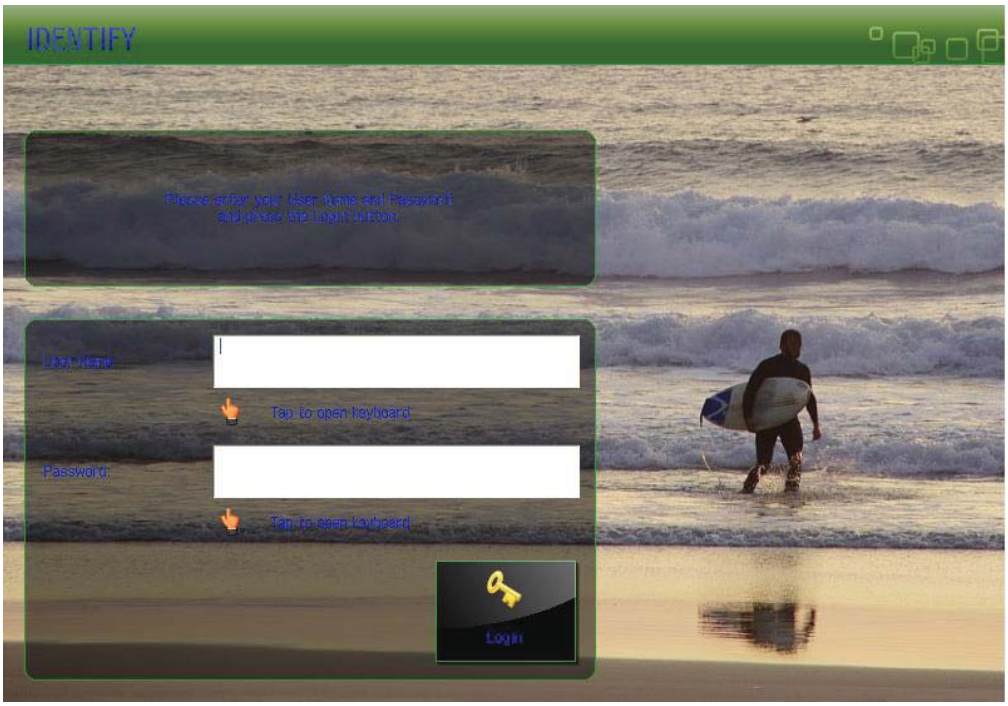
- Press the ***Create*** button and enter a name. Choose the font size you want and decide on the position of the login box and the information text box. Then use the color picker for each of the color fields.



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



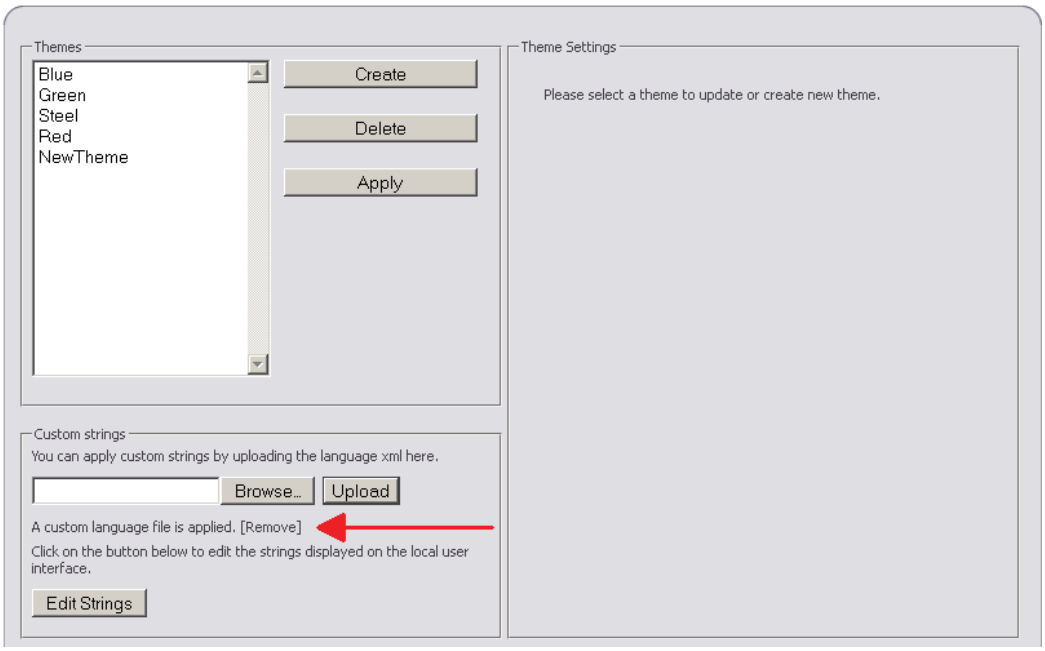
- You can also browse for a background image for the device screen and upload it. Click ***Save*** to apply your settings. Now the new settings are active and your login manager UI has a completely customized design.



6.6.1 Customized Language Strings

It is possible to translate the strings of the Universal Login Manager into the local language if required and upload these to the device. To extract the desired strings from the NT-ware String Localization Tool, please click on the following link: Universal Login Manager String Export http://ntwlabib.dnsalias.com/Stringtable/MomLang.xml?from=40000&to=40999 and save the download locally. Open the file in an XML editor, locate the desired language or create your own language string if necessary. In that case, make sure to use the ISO-639-1 code of the language you want to add. When done, you can upload the localized file in the ***Customize menu*** under ***Custom Strings.*** Browse for the file by clicking on the ***Browse*** button and upload it with the ***Upload*** button. You can remove it again by clicking on ***Remove***. This reactivates the default string table.

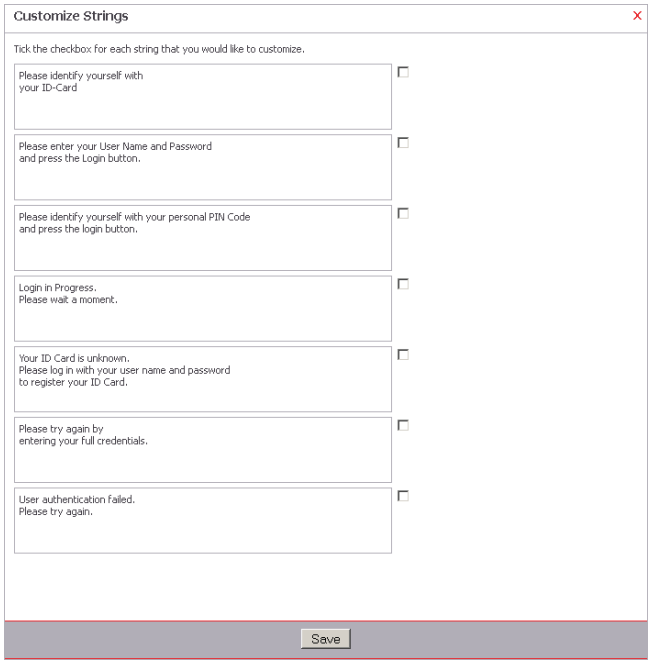
The english language strings must be present in the modified XML file additionally. Otherwise the import of customized strings will not be successful.



The language files are stored locally on the device. If you have multiple devices you need to repeat the above 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 check box next to it. Finish with ***Save***.



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

6.7 Universal Login Manager Usage Tracker

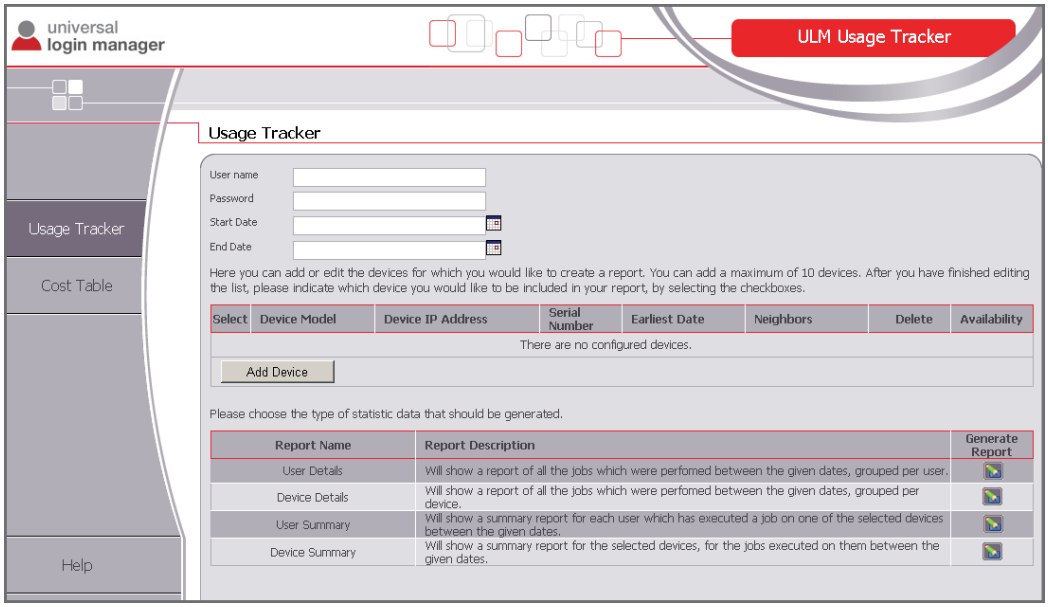
The Universal Login Manager provides the possibility of downloading a Rich Internet Application for tracking the usage of the devices the Universal Login Manager Usage Tracker. This application is run in a local browser on the user's computer. With it the user can manage a list of registered devices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

The link to the ULM Usage Tracker can be found on the ***Usage Tracker*** tab of the Universal Login Manager RUI.

The Usage Tracker has three sub menus:

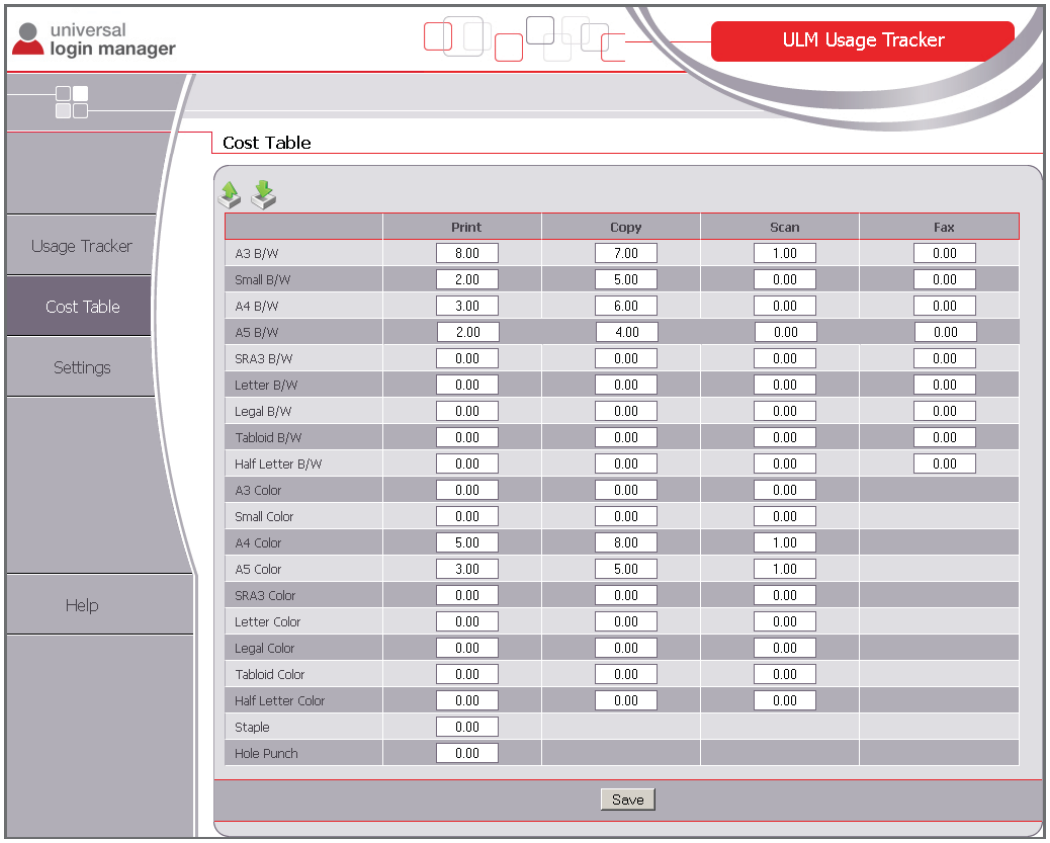
Usage Tracker

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



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.

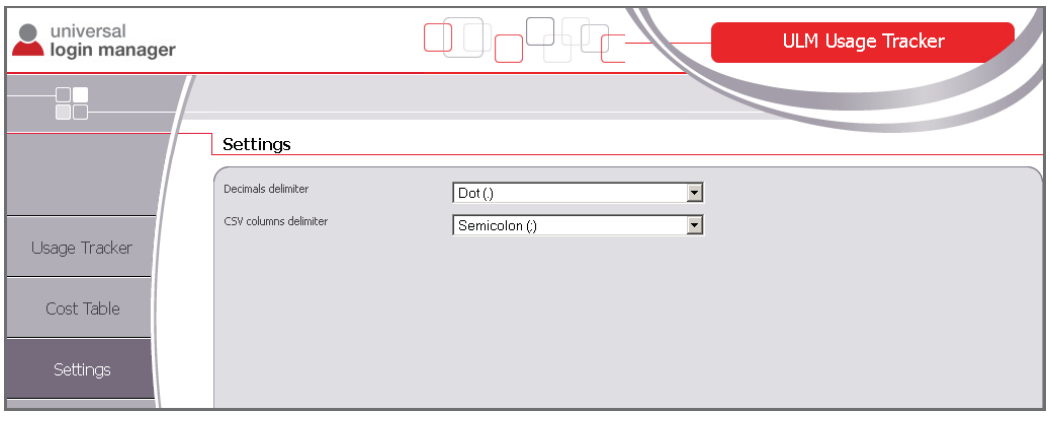


All data like prices or added printers are stored only in the local browser's cache and controlled with cookies. All configured data is lost, if cache and cookies are deleted. To save data, use the export/import functions where available.

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.)



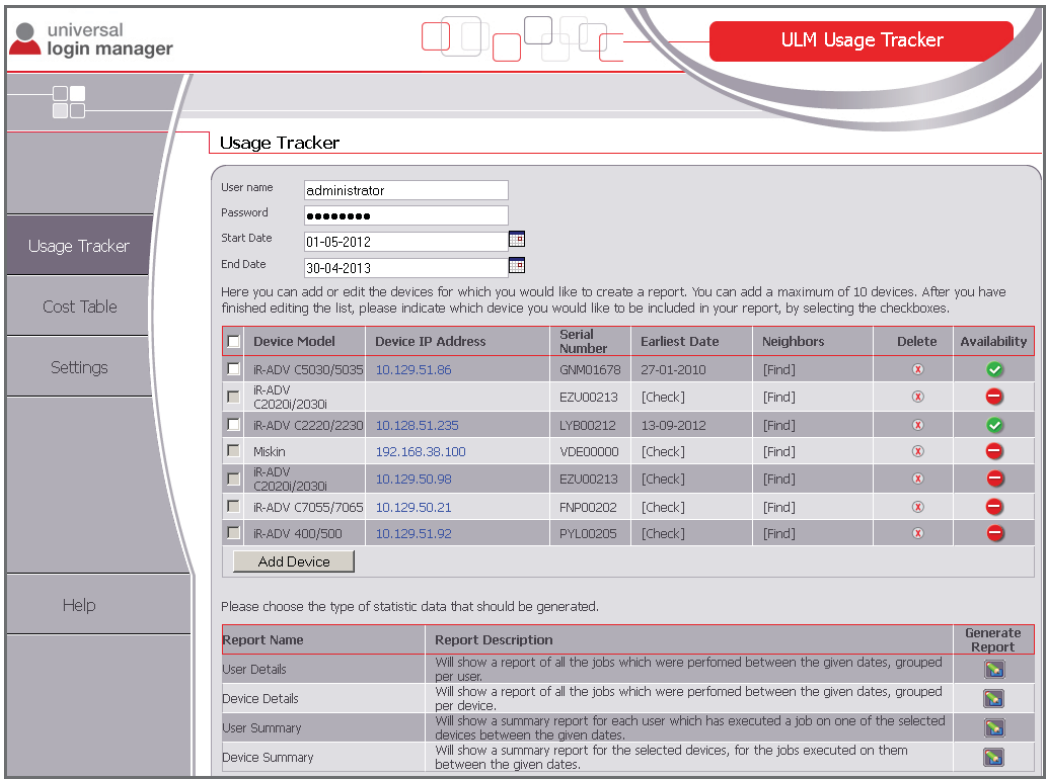
6.7.1 Adding a Device

In order to add a device for which you want to create a report, open the 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 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 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 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.



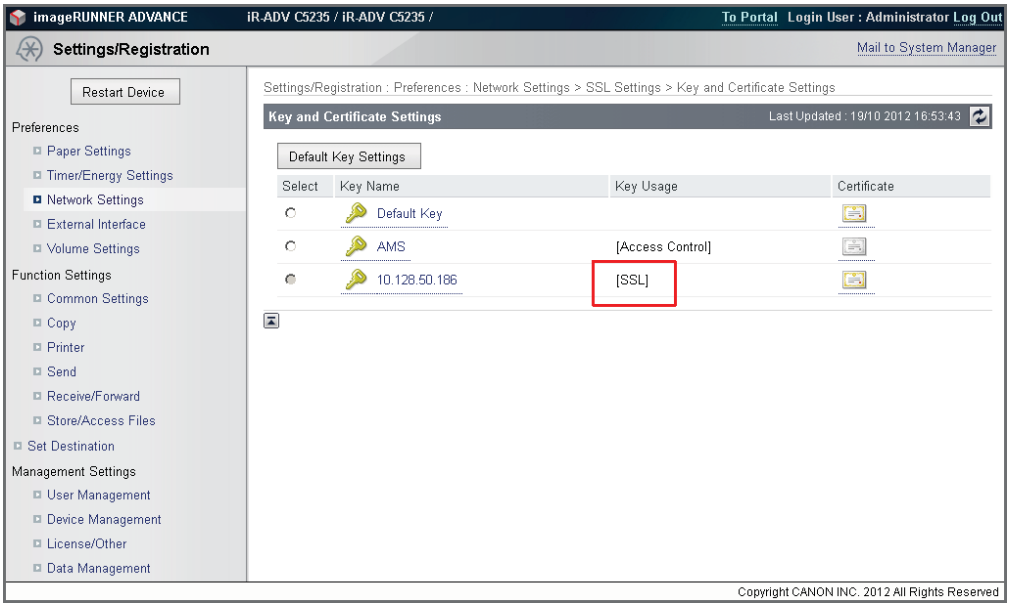
6.7.1.1 Creating a Certificate on the Device

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.

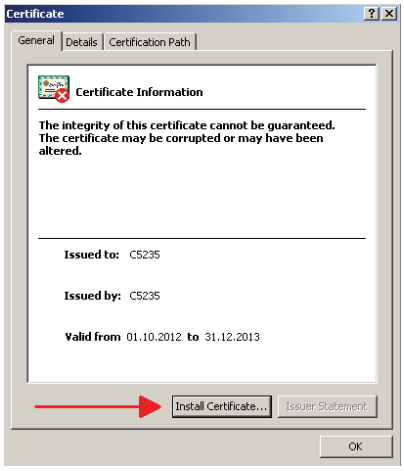
To solve this problem you need to create a new certificate on the device including it's IP address. In order to do this, follow these steps:

- Open the printer'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 another key than the ***Default Key*** was used before, check the radio button in front of ***Default Key*** and click on ***Default Key Settings*** to set it as the standard SSL key. Restart the device.
- 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 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.



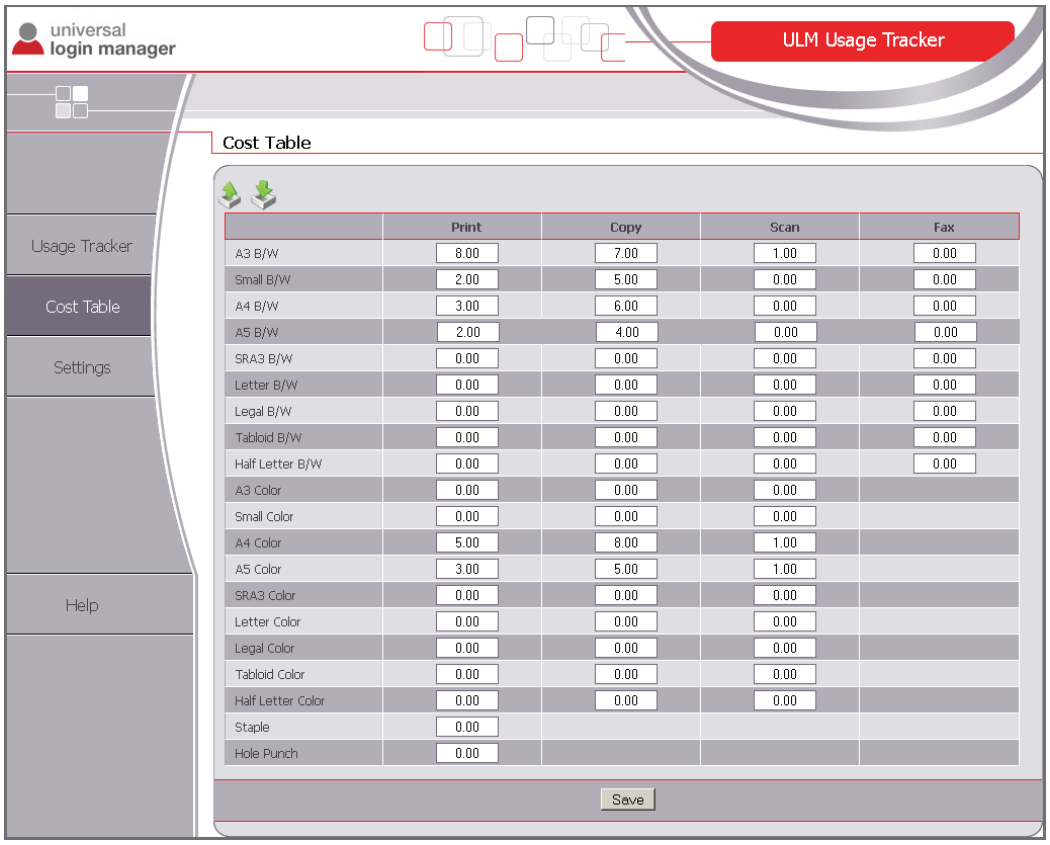
- Start the Certificate Import Wizard by clicking on ***Install Certificate*** and follow the steps.
- After finishing the wizard start the ULM Usage Tracker. The printer is now marked as available in the device list

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

6.7.2 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.

Note that prices have to be entered in order to have meaningful reports.



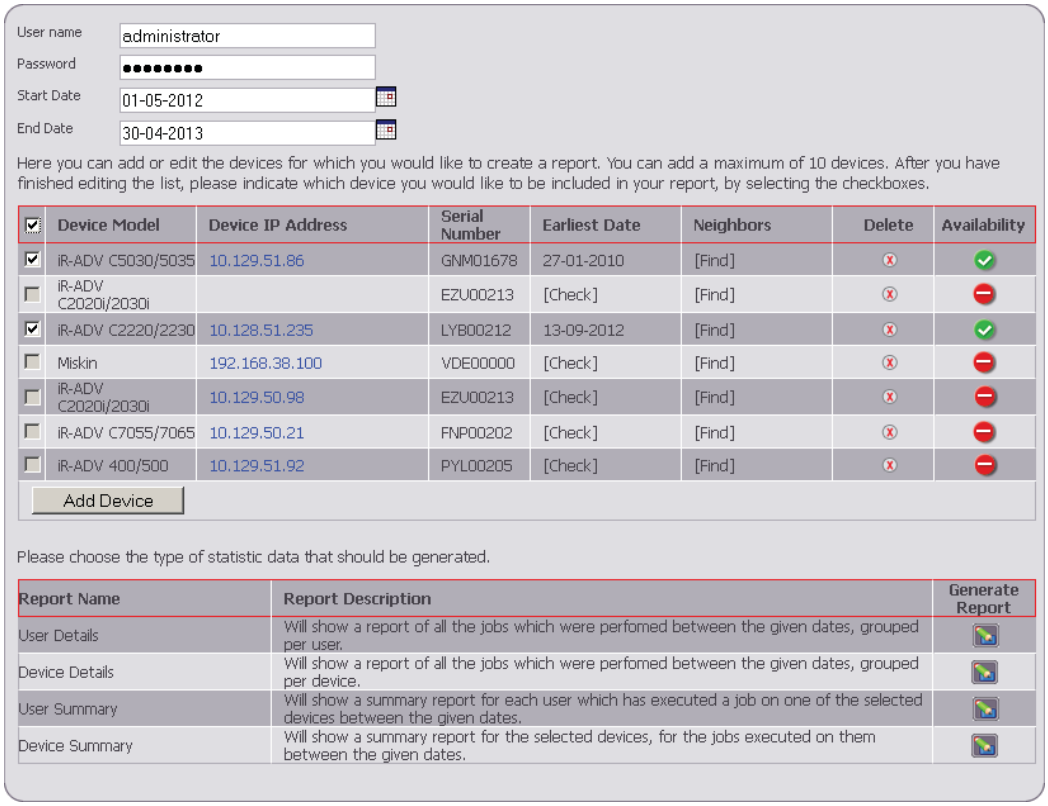
The Cost Table can be exported and imported by using the export and import buttons in the upper left corner of the screen.

6.7.3 Creating a Report

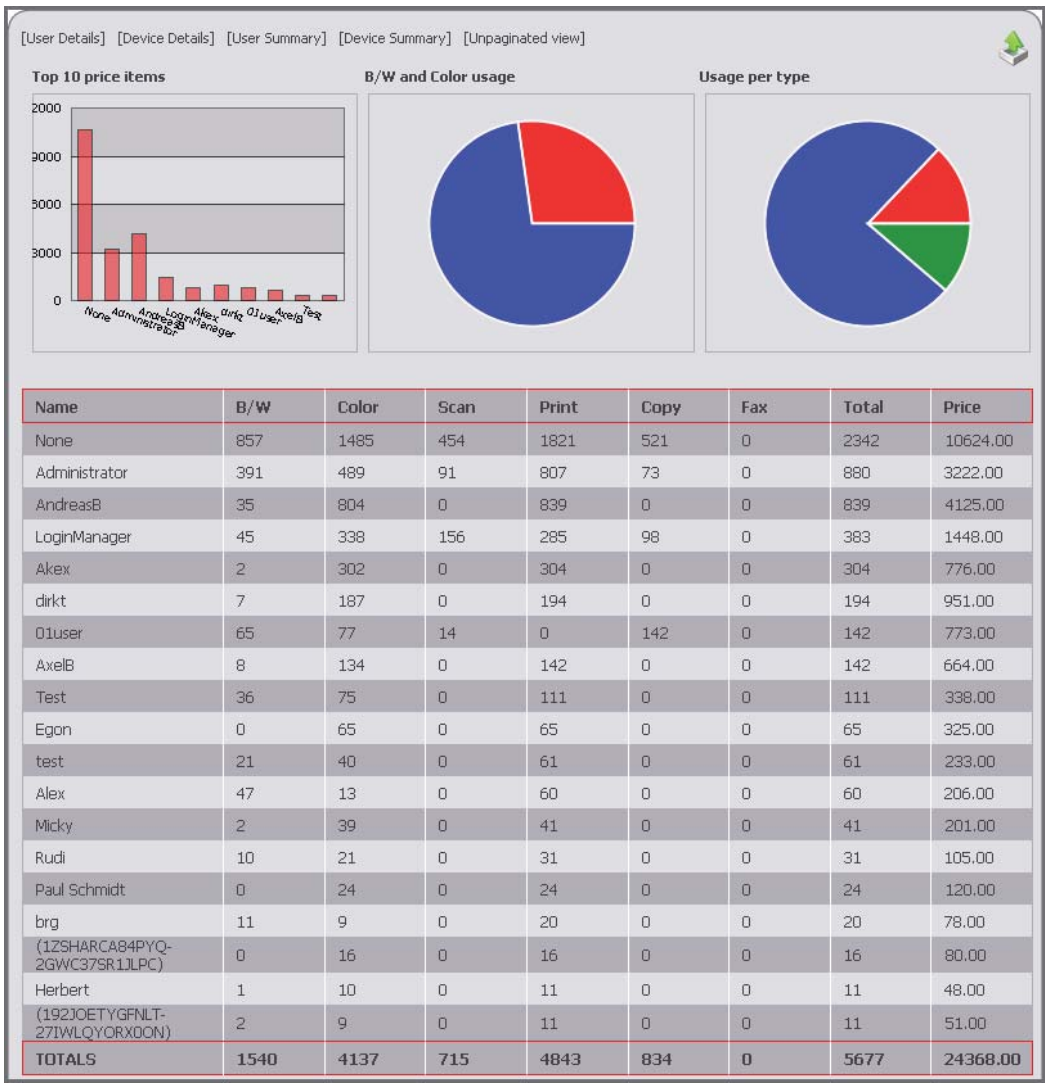
To create a report, proceed as follows:

- Enter a valid user name and password.
- Enter the date range using the Begin 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 V.4.1 or higher.



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 popup 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.



Name	B/W	Color	Scan	Print	Copy	Fax	Total	Price
None	857	1485	454	1821	521	0	2342	10624.00
Administrator	391	489	91	807	73	0	880	3222.00
AndreasB	35	804	0	839	0	0	839	4125.00
LoginManager	45	338	156	285	98	0	383	1448.00
Akex	2	302	0	304	0	0	304	776.00
dirkt	7	187	0	194	0	0	194	951.00
01user	65	77	14	0	142	0	142	773.00
AxelB	8	134	0	142	0	0	142	664.00
Test	36	75	0	111	0	0	111	338.00
Egon	0	65	0	65	0	0	65	325.00
test	21	40	0	61	0	0	61	233.00
Alex	47	13	0	60	0	0	60	206.00
Micky	2	39	0	41	0	0	41	201.00
Rudi	10	21	0	31	0	0	31	105.00
Paul Schmidt	0	24	0	24	0	0	24	120.00
brg	11	9	0	20	0	0	20	78.00
(1ZSHARCA84PYQ-2GWC37SR1JLPC)	0	16	0	16	0	0	16	80.00
Herbert	1	10	0	11	0	0	11	48.00
(192JOETYGFNLT-27IWLQYORX0ON)	2	9	0	11	0	0	11	51.00
TOTALS	**1540**	**4137**	**715**	**4843**	**834**	**0**	**5677**	**24368.00**

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.

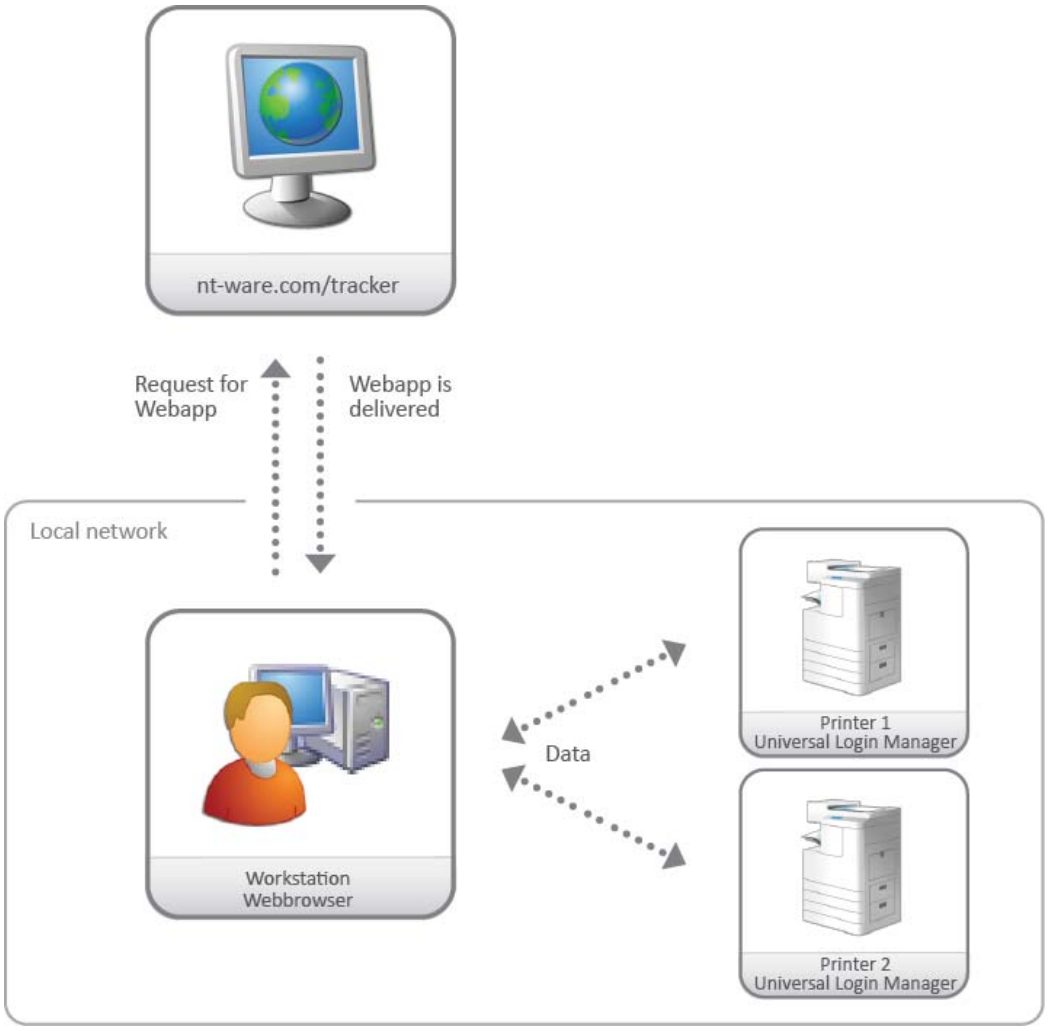
The exported *.csv file uses the delimiters configured under Settings.

6.7.4 Security Aspects

The ULM Usage Tracker is a web app that is executed locally within the browser. When the user opens the 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 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.



Usage Tracker Communication in Detail

- All scripts that run within the 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

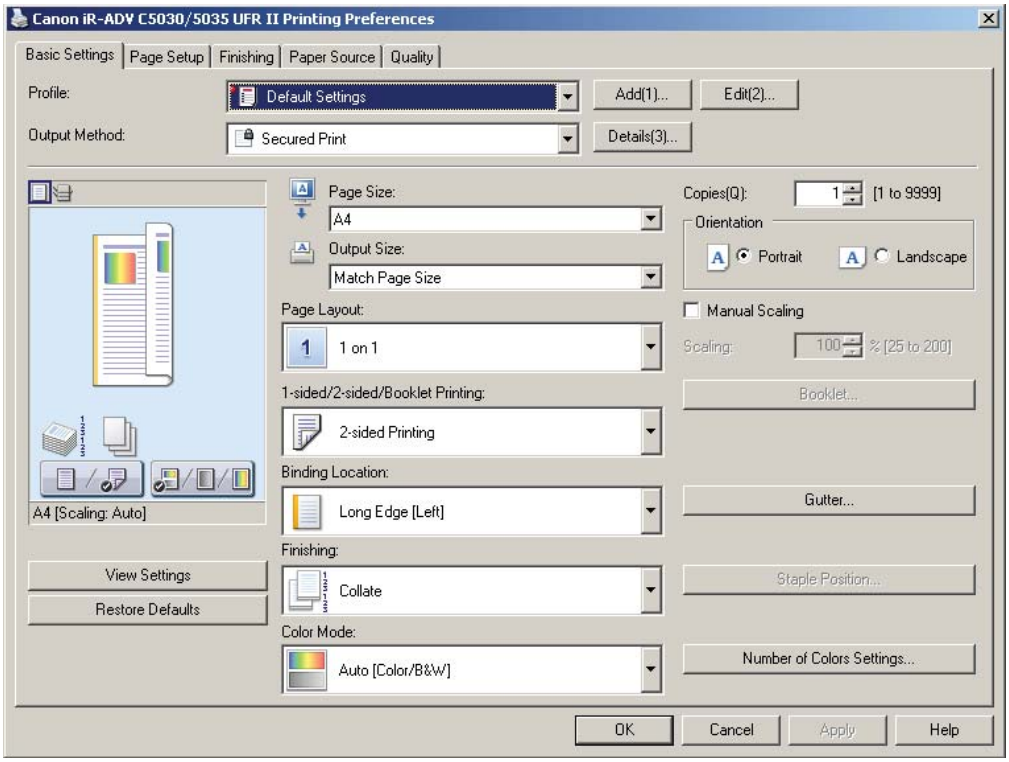
- The browser makes requests to the devices through the HTTP(S) protocol, using JavaScript AJAX calls. The answer is returned in JSON format and is locally parsed by the JavaScript code running in the browser.
- Data transfer between workstation and printer is done via HTTPS. Only if HTTPS is not available for any reason (network configuration, certificates etc.), the system falls back to HTTP.
- Username 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 (on page 47).

7 Secured Print

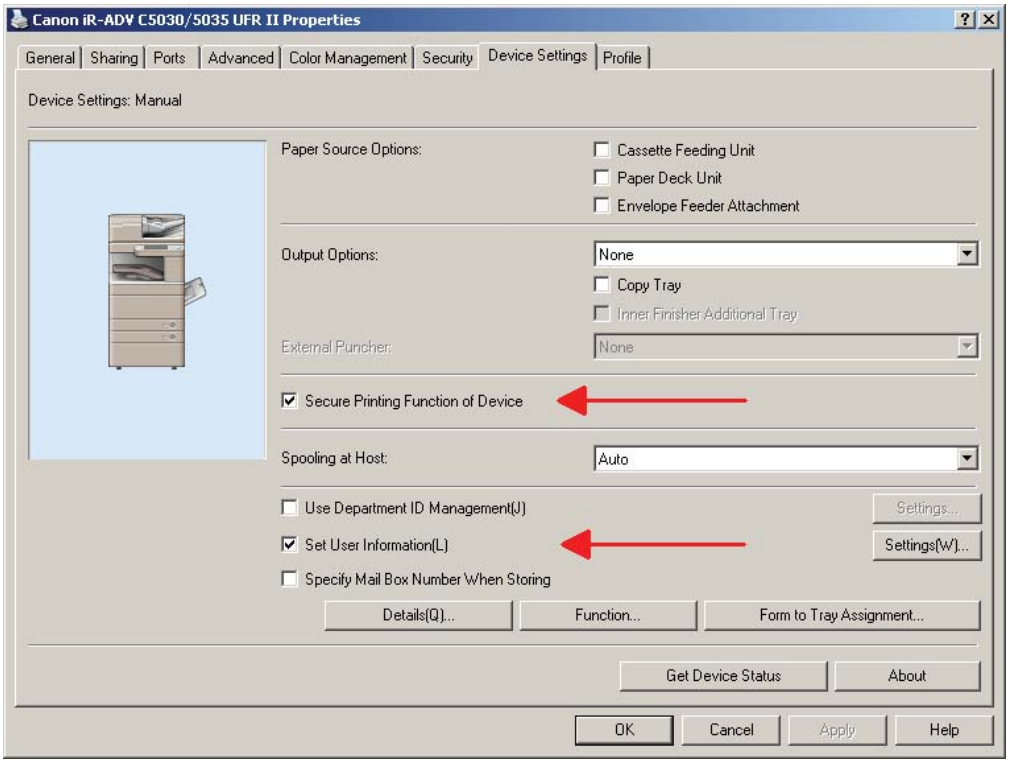
With the Universal Login Manager a user can easily use the built-in ***Secured Print*** function of the device. To do so, the following steps are necessary.

Configure Secured Print

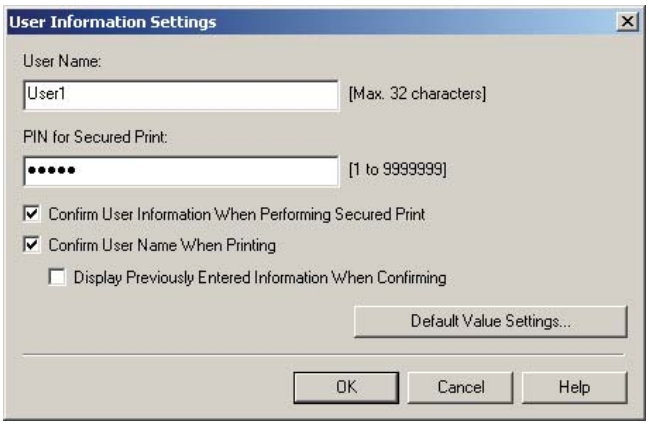
- Install the generic driver for the specific device.
- Open the ***Properties*** of that printer driver.
- On the ***General*** tab open the ***Printing Preferences***. Select ***Secured Print*** as ***Output Method*** and save the settings with ***OK***.



- Open the ***Device Settings*** tab and check ***Secure Printing Function of Device.***



- Check ***Set User Information(L)*** and press ***Apply***. Then click on the ***Settings(W)*** button.

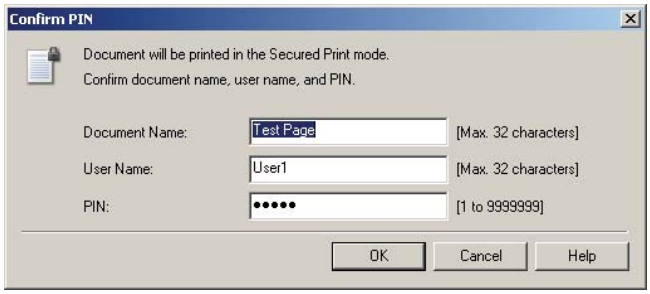


- In the new window enter the user name that is used on the device and a PIN code. The PIN code is used as the default PIN code for new jobs but can also be changed for each print process.

This PIN code is needed to release ***Secured Print*** jobs. The user either has to know this default PIN code or define an own PIN for each print job.

- Check the two confirmation boxes. The user is now asked for credentials when creating a print job as well as when releasing the job at the device. This can be changed depending on the desired level of security.
- Press ***OK*** and close the printer properties.

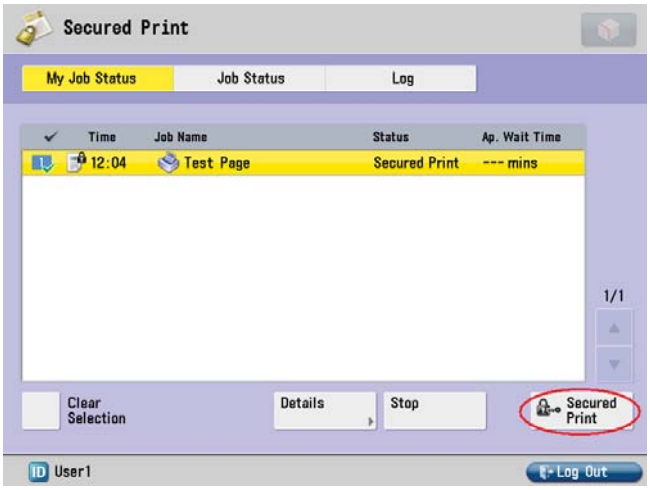
From now on, any print job printed will only be sent to the printer after acknowledging the default values defined above or after entering new credentials for the current job.

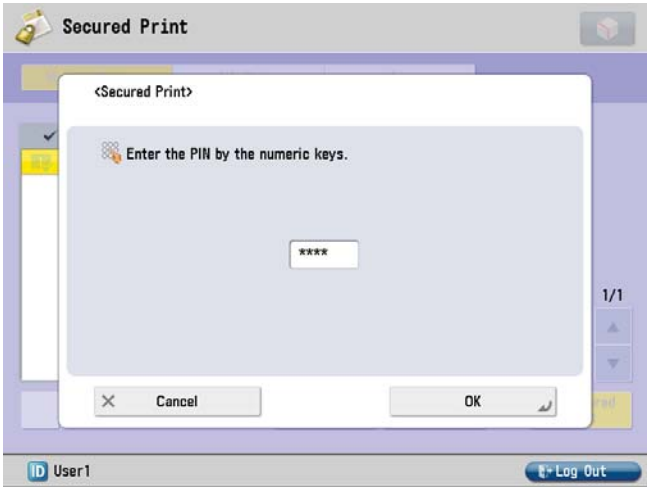


Releasing Secured Print Jobs

- The user logs in to the printer with the Universal Login Manager and taps on the ***Secured Print*** button.

- Now a list is shown with the user's print jobs (***My Job Status***) and can be released by selecting a job and tapping on the ***Secured Print*** button. Here the user enters the PIN that was used when the print job was created and the job is printed out after tapping on ***OK***.



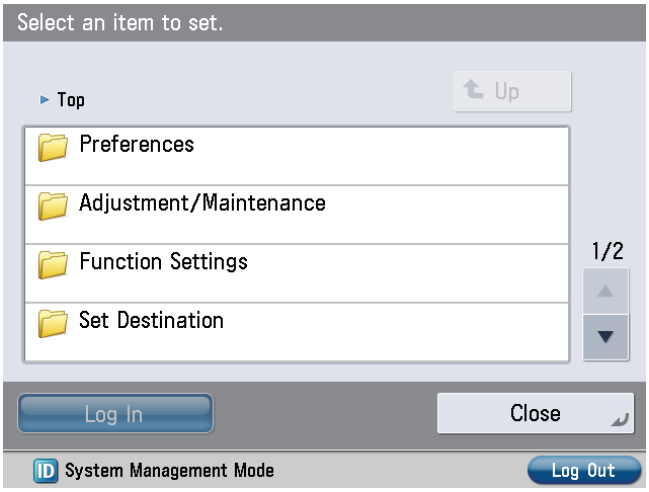


Omit PIN

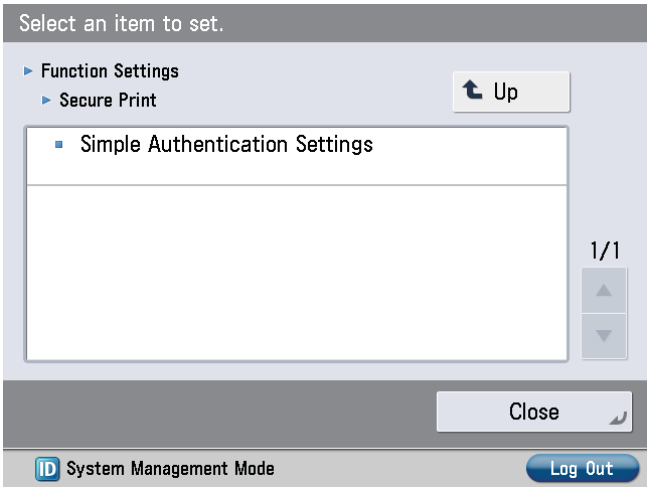
The following ONLY works on Generation 2 devices!

It can be useful to have the print job printed out without having to enter the PIN code at the device. In order to do so, the following settings have to be made.

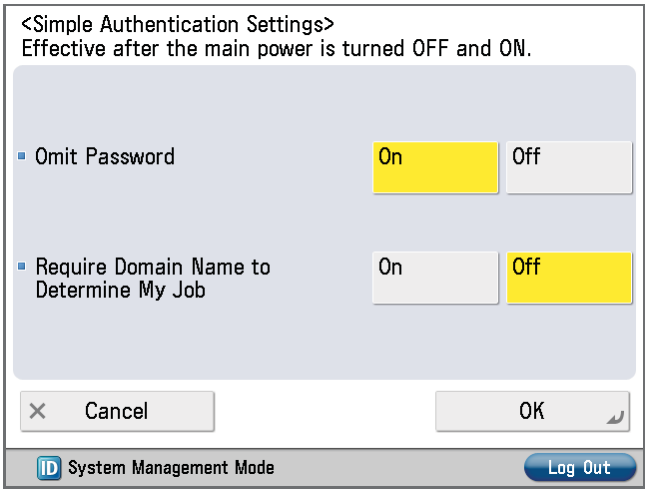
- Open the ***System Management Mode***.



- Open ***Function Settings*** > ***Secure Print*** > ***Simple Authentication Settings.***



- Activate ***Omit Password***.



Now new print jobs will be printed without user interaction under the following conditions:

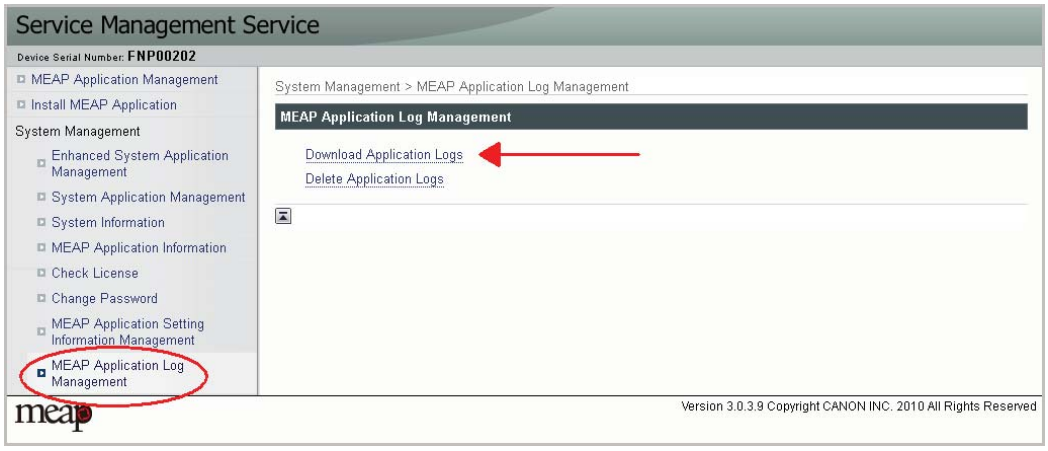
Either enter the PIN 3758211 as the default PIN in the ***User Information Settings*** on the ***Device Settings*** tab or the user enters this PIN for each individual print job.

8 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.

9 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.



10 Appendix

10.1 Hardware

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

Device Name	Firmware Ver.	AMS	Note
imageRUNNER ADVANCE C9280 PRO	v10.23	STD	*1
imageRUNNER ADVANCE C7280i/C7270i/C7260i	v10.23	STD	
imageRUNNER ADVANCE C5255/C5255i/C5250/C5250i/C5240i/C5235i	v06.01	STD	
imageRUNNER ADVANCE C2230i/C2225i/C2220i	v06.01	STD	
imageRUNNER ADVANCE C2220L	v10.23	STD	
imageRUNNER ADVANCE 8205 PRO/8295 PRO/8285 PRO	v02.01	STD	
imageRUNNER ADVANCE 6275i/6265i/6255i	v02.01	STD	
imageRUNNER ADVANCE C9070 PRO/C9060 PRO	v69.03	STD	*1
imageRUNNER ADVANCE C7065i/C7055i	v69.03	STD	
imageRUNNER ADVANCE C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i	v69.03	STD	
imageRUNNER ADVANCE C2030L/C2020L	v32.01	STD	*2
imageRUNNER ADVANCE C2030i/C2025i/C2020i	v32.01	STD	
imageRUNNER ADVANCE 8105 PRO/8095 PRO/8085 PRO	v44.03	STD	
imageRUNNER ADVANCE 6075/6075i/6065/6065i/6055/6055i	v44.03	STD	
imageRUNNER ADVANCE 4051i/4045i/4035i/4025i	v17.02	STD	
imageRUNNER ADVANCE 400iF/500iF		STD	

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

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

10.2 Optional Items

10.2.1 Proximity Card Reader and Card Types

MiCard PLUS and Proximity Card Options

Description	Item Code
MiCard PLUS Reader	3575B353AA

This is a required item when the Proximity Card Login type is selected.

The MiCard PLUS supports HID Proximity and Mifare card types as default. If the user does not have any of the supported proximity cards, we can provide them as listed below.

The MiCard PLUS has to be connected to the USB interface of the imageRUNNER ADVANCE devices. The USB device port option is recommended to house and protect the MiCard PLUS. See chapter USB Device Port (on page 62).

HID Proximity Card

Description	Item Code
HID Card 10 Pack	3575B203AA

Mifare Card

Description	Item Code
Mifare Card 10 Pack	3575B078AA

The users can utilize their own HID or Mifare cards. If the customer already uses a different card type, then you need to change the setting of the card reader through the MiCard Configuration Tool.

10.2.2 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 MiCard PLUS in it.

Products	Supported devices
USB Device Port A1	imageRUNNER ADVANCE 6xxx/8xxx/C7xxx/C9xxx
USB Device Port A2	imageRUNNER ADVANCE 62xx/82xx
USB Device Port-B1	imageRUNNER ADVANCE C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i
USB Device Port-C1	imageRUNNER ADVANCE C2030i/C2030L/C2025i/C2020i/C2020L
USB Device Port-D1	imageRUNNER ADVANCE 4051i/4045i/4035i/4025i
USB Device Port-E1	imageRUNNER ADVANCE C5255/C5255i/C5250/C5250i/C5240i/C5235i/ C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i/ C2230i/C2225i/C2220i/ C2220L

10.2.3 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 all imageRUNNER ADVANCE devices in North America.

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 (UFRII/PCL/PS). The AMS printer driver add-in module is available for download from the Software Download Center http://www.support.cusa.canon.com for the USA and from the Canon Extranet ISG Service https://canonextranet.canon.ca for Canada.

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

Index