



PRODUCT INFORMATION GUIDE

Index

Summary information	4
1. Introduction	5
1.1. What is uniFLOW Online?	5
1.2. Why move print and scan management to the cloud?	5
2. Product description and features	6
2.1. Product architecture	6
2.1.1. Key uniFLOW Online components	6
2.1.2. Various ways to submit print jobs	6
2.1.3. Unique technologies which make the difference	7
2.1.4. Identity management	7
2.1.5. Regional data centers	7
2.2. uniFLOW Online features and functionality	7
2.2.1. Identification at the device	8
2.2.2. Secure Printing	9
2.2.3. Mobile Printing	12
2.2.4. Secure document scanning	14
2.2.5. Scan center	15
2.2.6. Print and copy accounting	16
2.2.7. Cost centers	16
2.2.8. Fleet Management	18
2.2.9. Dashboards	18
2.2.10. Audit logging	19
2.2.11. Home-working support	19
2.3. Technical requirements	19
2.3.1. Bandwidth requirements	19
2.3.2. Requirements for uniFLOW SmartClient	19
2.3.3. Requirements for Direct Secure Print	19
2.3.4. Requirements for Data Collection Agent	19
2.3.5. Browser support	19
2.4. System security	20
2.4.1. Security – uniFLOW Online platform	20
2.4.2. Security – Microsoft Azure hosting platform	21
3. Selling uniFLOW Online	22
3.1. Key customer benefits	22
3.2. Selling points of uniFLOW Online	22
3.3. Product positioning	23
3.3.1. When to sell uniFLOW Online?	23
3.3.2. When to sell uniFLOW?	24
4. Tenant management	25
4.1. Tenant structure	25
4.2. Tenant creation by Canon or a Canon Partner	26
4.2.1. How to create management and customer tenants?	26
4.2.2. Root Administrator	27
4.2.3. Manage user roles	27
4.3. Tenant self-creation	27
4.4. Tenant claiming	29
4.5. Tenant login	29
4.6. Tenant deletion	30

5. uniFLOW Online subscription model	32
6. Service and support operations	33
6.1. Service responsibilities	33

Summary information

Document version	Creation date
Initial Version	December 2015
V9	February 2019
V10	July 2019
V11	September 2019
V11.1	October 2019
V12	December 2019
V12.1	February 2020
V13	May 2020
V13.1	July 2020
V14	September 2020
V14.1	November 2020
V15	December 2020
V15.1	June 2021
V16	September 2021
V16.1	November 2021
V17	February 2022
V18	March 2022
V19	May 2022
V20	June 2022
V21	August 2022
V22	September 2022
V23	November 2022

This guide provides an overview of uniFLOW Online, including the main components of the software, sales information, subscription and tenant management information, and service and support operations.

1. Introduction

1.1. What is uniFLOW Online?

uniFLOW Online is a secure public cloud print and scan solution for businesses of all sizes, facilitating managing their entire print environment. The solution improves document security, controls printing costs and increases productivity while reducing internal IT overheads. It has been designed to meet the needs of businesses that do not want to invest in or manage local servers but still wish to control the printing process and benefit from flexible scan workflows.

uniFLOW Online has been developed on the Microsoft Azure cloud platform, providing businesses with superior enterprise platform security, scalability, and resilience.



1.2. Why move print and scan management to the cloud?

The key drivers for moving print and scan management to the cloud are:

- Reduced print and scan infrastructure costs: no outlay for server hardware, operating system licensing, and associated costs.
- Reduction of costs for system maintenance: the hosting provider takes care of infrastructure and software updates.
- Highly scalable: cloud systems can be easily scaled up according to changing needs.
- Environmental-friendly: reduced power consumption of the print infrastructure.

2. Product description and features

2.1. Product architecture

2.1.1. Key uniFLOW Online components

uniFLOW Online Portal

Here, the configuration and management of uniFLOW Online take place, and reports are created. It is hosted regionally in Microsoft Azure data centers.

uniFLOW SmartClient

The uniFLOW SmartClient is installed on each user's PC and includes the uniFLOW Universal Printer Driver. The uniFLOW SmartClient is used to take over some of the tasks that were typically dealt with by the server, e.g. the storage of print job information, the provision of print job lists, and, depending on configuration, the hold of the print job until the user identifies themselves at the device and releases it.

Universal Login Manager

This software is installed directly on the ULM-enabled Canon device. It controls identification at the machine and displays the list of jobs available to the user and available scan profiles.

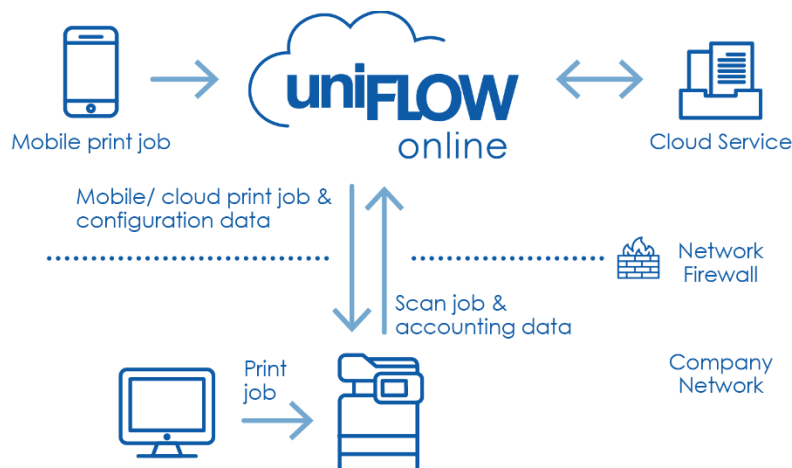
uniFLOW Release Station

The uniFLOW Release Station is a user-friendly touch screen with an embedded card reader used for releasing secure print jobs on most printers.

2.1.2. Various ways to submit print jobs

Users can send their secure print jobs from their desktop PCs using the uniFLOW SmartClient or Direct Secure Print. Print jobs stay within the company network and follow the user from device to device, allowing the release of print jobs on any connected printer (My Print Anywhere). Post printing accounting data is sent to uniFLOW Online either by the uniFLOW SmartClient or the Universal Login Manager installed on the Canon device.

Users can print jobs from mobile devices, smartphones, or tablets by emailing the file to uniFLOW Online or directly uploading the files into the mobile job submission displayed in the tenant dashboard. Files can also be printed from connected cloud services or sent to a queue for later printing. Suppose the file needs to be converted from its native format into a language the printer understands. In that case, the regional data center where uniFLOW Online is hosted will undertake the process (customer data does not leave the data center). More than 40 file types can be converted, e.g. PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, and standard image formats such as JPG and PNG. Once converted, the original file is deleted, and the converted file is held at the regional data center until released or printed.



2.1.3. Unique technologies which make the difference

Cloud technology is very clearly growing, and its strengths are becoming more and more apparent. uniFLOW Online encompasses the whole print and scan environment and allows adaptable configurations to address the demands of different office environments.

One cloud platform for all printing, scanning and device management

uniFLOW Online comprises a broad set of detailed features. It oversees a business' entire print and scan environment. It provides device management with one solution, from secure and mobile printing to advanced scanning and automated filing processes. The modular design makes it easy to expand the print and scan environment with additional features, such as cost center or budgeting while keeping maintenance to a minimum. uniFLOW Online integrates seamlessly into an existing office environment and enhances document and device security.

Versatility in addressing customer demands

Multiple configuration possibilities deal with ever-changing customer demands. A key component is uniFLOW Online's location concept which allows for a different configuration of individual features per location. Locations can vary in print submission pathways, security features, or network setup, including Zero Trust environments. With central management in the cloud, uniFLOW Online makes it easy to keep track of everything.

100% cloud-based infrastructure

uniFLOW Online has been developed from the ground up to enhance the benefits of cloud technology. All tenants are logically isolated from each other, while the public cloud ensures the latest version is always available, providing superior enterprise platform security, scalability, and resilience.

When using uniFLOW Online's innovative technology, there is no requirement for a local server or edge devices. All communications between the different entities can go directly or via the secure cloud, thus eliminating servers and minimizing IT efforts.

2.1.4. Identity management

uniFLOW Online does not store any user credentials such as passwords. Instead, it uses a claims-based approach to identify users, which accepts login credentials from multiple identity providers. However, users do not need to remember complex usernames and passwords. Users sign in via a one-time email link. This simple login and registration process becomes the new default user login method for all new tenants, intended for non-privileged users. Alternatively, administrators can use Active Directory Federation Services (ADFS) to integrate with e.g., Microsoft Office 365 or their own locally hosted Active Directory. The provider type OpenID Connect will integrate with Auth0, Okta, OneLogin™, Ping Identity® and others. In addition, it is possible to make use of shared web identity providers like Google™, Yahoo!® or Windows Live ID.

2.1.5. Regional data centers

uniFLOW Online is hosted at Microsoft Azure data centers distributed globally. The use of multiple Microsoft Azure data centers by uniFLOW Online allows customers to control their data sovereignty. It always remains within the local region, i.e. European customers' data will be stored in Europe, and Australian data will never leave Australia.

uniFLOW Online is hosted in local data centers in Europe, the UK, the US, Singapore, Australia, Japan and China.

More information about Microsoft Azure and its security and compliance features can be found at the website: <https://azure.microsoft.com/en-gb/support/trust-center/>

2.2. uniFLOW Online features and functionality

uniFLOW Online provides the expected functionality required by businesses, such as identification at the device, secure printing, print from cloud, mobile printing, secure document scanning, and print and copy accounting.

2.2.1. Identification at the device

To prevent unauthorized use of the device, the Universal Login Manager locks the control panel until a user identifies at the device. Users can access device functionalities such as copy, print, scan, and fax on identification.

On the Canon imageRUNNER ADVANCE (DX) and Canon imageRUNNER with AddOn Platform line-up, device features can be restricted with the Canon MEAP/ AddOn AMS functionality. The administrator can limit the device's functionality through device policies based on the user login, e.g. scan in color. Restrictions also apply when the network connection is lost and a Canon imageRUNNER ADVANCE (DX)/ imageRUNNER with AddOn Platform is accessed in emergency mode.

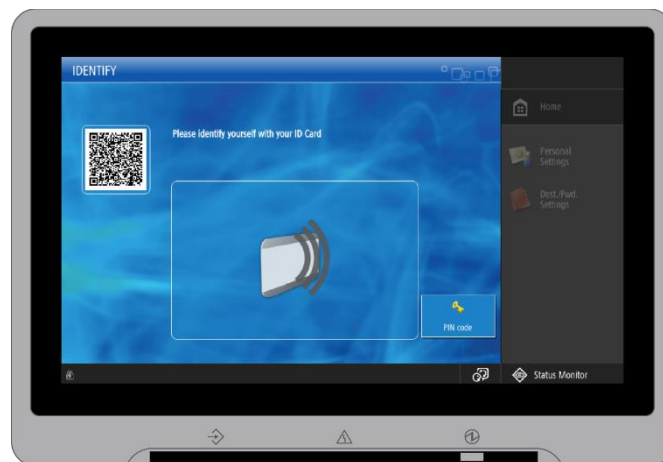
Canon imageRUNNER ADVANCE (DX) and Canon imageRUNNER with AddOn Platform combined with the Canon AMS functionality can extend access through function-level login. In this case, login is only required for specific functions, while the device stays unlocked for others. Functions can also be restricted based on device location, e.g. a business wants to implement the highest security settings for its accounting and HR department, so it needs to limit all device functions for these locations. At the same time, its training center participants need to be able to copy training materials, so copy functions would not be restricted for this location.

Primary login methods as the default method to log in to the device are:

- Image login + optional PIN code
- PIN code
- ID card
- ID card + PIN code
- Dept. ID/ PIN code

If an ID card or ID card + PIN was selected as the primary method, one could also choose PIN code as a secondary login method.

In addition, users can also use their mobile phones for identification instead of their ID cards. Therefore, the NT-ware Mobile Badge BLE 2.0 app must be installed on the phone, and a BLE supporting card reader must be used.



Features supported by uniFLOW Online:

- Primary/ secondary login
- Card or mobile phone registration at the device
- Embedded secure print application behavior (ULM only)
- Customizable login screen (ULM only)
- User creation and user management at the machine (ULM only)

2.2.2. Secure Printing

With uniFLOW Online, users can print confidential documents securely. All print jobs stay in a user's personal secure print queue until they identify and release at a device. For businesses with more than 25 devices, it is recommended to configure locations to keep network traffic low. Print jobs are available on any connected printer within the user's location.

The layout of the secure print queue can be configured on Canon imageRUNNER ADVANCE (DX) and Canon imageRUNNER with AddOn Platform. Finishing options may be altered directly at the device before printing.

uniFLOW Online optionally supports touchless secure job release. After identifying the device, a user will be given the option to release all jobs or cancel this activity. After five seconds, all print jobs will be released automatically.



uniFLOW Online provides different means to send secure print jobs that can be configured per location.

Direct printing in emergency mode

uniFLOW Online ensures that printing will continue if there is a network failure in cloud/cloud configured environments. Users can print directly on a device. If a network outage is detected while printing, a popup informs the user about the issue and offers to send the job directly to an alternative device.

2.2.2.1. uniFLOW SmartClient

The uniFLOW SmartClient is a client application installed on a user's local PC. The initial configuration of the uniFLOW SmartClient for Windows is added to the MSI package, which is then installed on the client's PC. Also, the uniFLOW SmartClient for Mac® is directly installed on a user's client PC. Once installed, print jobs submitted using the uniFLOW Universal Driver (installed in conjunction with the uniFLOW SmartClient) are then held

- by the uniFLOW SmartClient,
- in the cloud (uniFLOW Online),
- on the Canon imageRUNNER ADVANCE (DX)/ imageRUNNER with AddOn Platform with Advanced Space

until the user identifies at the device. As the uniFLOW SmartClient is location-aware, users can move with their client PC between locations. If the automatic location detection fails, a default location can be set, or users can select a location themselves via a pop-up as an alternative to the default location.

The uniFLOW SmartClient includes the uniFLOW Universal Driver. This driver provides a simple interface with advanced printing features regardless of the used printer model. The uniFLOW Universal Driver also encrypts and compresses print jobs as they are sent, reducing network traffic, and enhancing security.

The uniFLOW SmartClient is suitable if the following condition is met:

- Locations with less than 25 devices

2.2.2.2. Direct Secure Print

Direct Secure Print provides secure My Print Anywhere without using client software. The function is provided using the native device force hold functionality of third-generation Canon imageRUNNER ADVANCE (DX) devices.

Print jobs are directly sent to a holder device. While the print job stays with the holder device, the job information is sent to uniFLOW Online. Users can pick up their print job at any supported device within the location. The machine at which the job is released receives the job information from uniFLOW Online and requests the print job from the holder device. This means users will see all their print jobs, including mobile print jobs, in a single queue from where each one can be released.

Direct Secure Print is suitable if the following conditions are met:

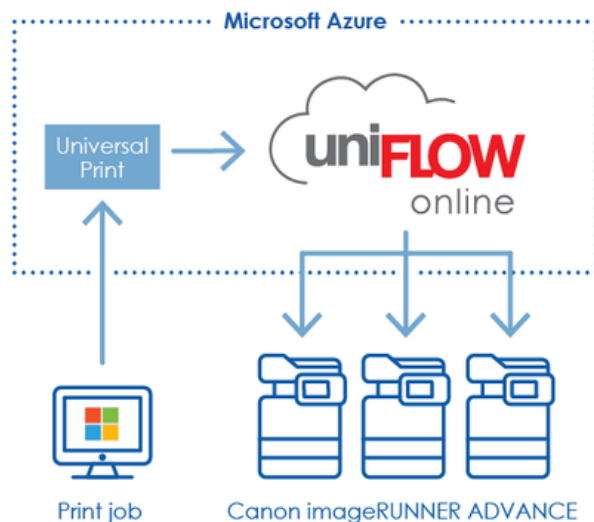
- Locations with less than 200 users/ less than 25 devices
- Locations, where users typically stay within their location
- Locations that consist purely of third-generation Canon imageRUNNER ADVANCE (DX)

2.2.2.3. Support for Google Chrome™ printing

uniFLOW Online supports Google Chrome OS™ or browsers running on any other operating system. The Google Workspace™ administrator can apply printing defaults and print restriction policies, as the tenant root settings are used. The Chrome OS extension allows sending print jobs directly to uniFLOW Online. Secure Printing/ My Print Anywhere allows job release at any device after identification. Finishing options can be applied at job submission, and even more are available on the device.

2.2.2.4. Support for Universal Print by Microsoft

Universal Print, developed by Microsoft, is a print service hosted in Azure for business or educational establishments of any size. uniFLOW Online connects natively with Universal Print. Users will use Windows print infrastructure and a single universal queue to submit their job. Secure Printing/ My Print Anywhere allows job release at any device after identification. Finishing options can be applied at job submission, and even more are available on the device. All printers are handled centrally in uniFLOW Online, including bulk device registration. As both Universal Print and uniFLOW Online are hosted in Microsoft Azure data centers distributed across the globe, data sovereignty is always provided. Customer data remains within the local region, and print spool files cannot be shared between different data centers.

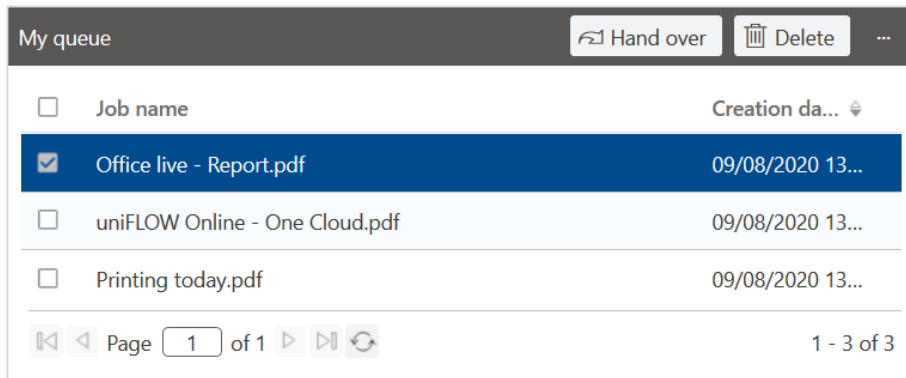


2.2.2.5. Print job delegation

Print job delegation helps to hand over print jobs to colleagues easily. It might be necessary for multiple reasons to delegate print jobs. For example, a home office user delegates a contract that other colleagues need in the office, or a manager delegates letters to the secretary, which are then printed and physically mailed.

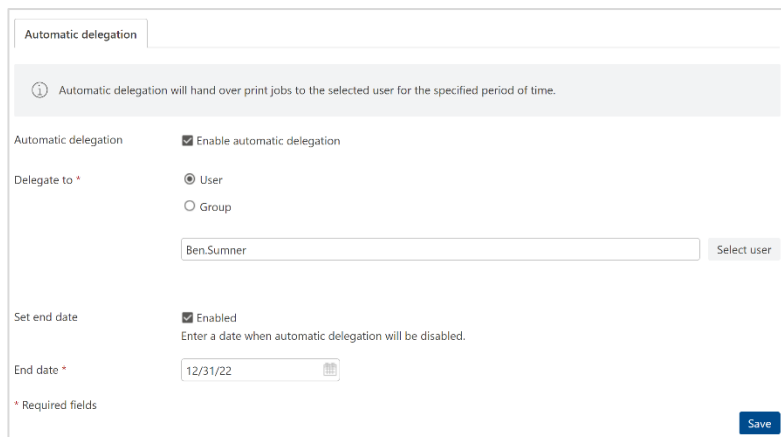
Hand over print jobs manually

Handing over print jobs to a colleague is easy. A user selects one or multiple jobs which shall be delegated and hits the 'Hand over' button. A recipient is chosen from a list of users to hand over the print job. Once delegated, the recipient receives an email notification and can release the print job from their queue. The print jobs are charged to the delegator.



Automatic print job delegation

The "Delegation" extension allows you to share all print jobs with other users automatically. The administrator can enable automatic print job delegation on a user basis. Documents can then be delegated to a user or group. An end date can be set optionally. Users are informed via email if they are added as recipients/ if they have been removed as recipients/ if new recipients have been added to their account/ if recipients have been removed from their account.



2.2.2.6. Universal Output Queue

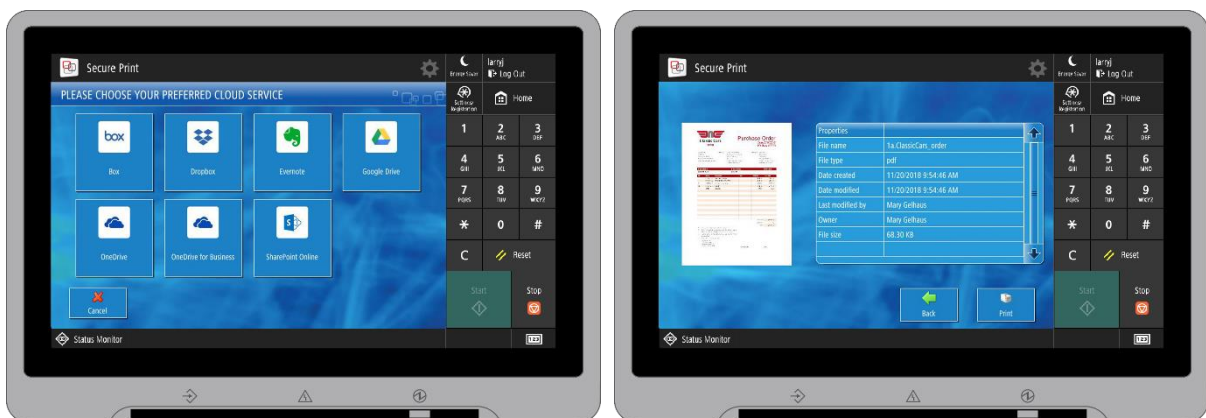
The Universal Output Queue allows direct printing to any device without installing device-specific drivers. A user's selection can be remembered for a specified time. The Universal Output Queue is an option that can be activated via the Extensions menu and enhances the capabilities of the uniFLOW SmartClient. It reduces time deploying print queues and drivers to end users and is entirely printer-independent; any network printer can be integrated. Administrators and users do not need to manage printer drivers when new devices are added.



2.2.2.7. Print from cloud

Documents stored in a cloud service can be accessed after identification at connected ULM devices and printed or saved to the queue for later printing. Both options will download the document to the tenant and convert it into a file format recognizable to the printer before release. The following cloud services are available: Box, Dropbox, Evernote®, Google Drive™, Microsoft OneDrive/ OneDrive for Business, Microsoft Teams and Microsoft SharePoint Online.

A job preview is available and finishing options may be altered directly at the device before printing.



2.2.3. Mobile Printing

As mobile devices become commonplace in business, printing from a PC is no longer sufficient. uniFLOW Online permits users to send jobs from mobile devices.

Regardless of how the print job was submitted, it will be placed in the user's secure print queue as though it had been sent from their desktop. Following identification at the device, a user views a single list of jobs sent from both PC and mobile devices. If a user selects a mobile job, it is pulled from the uniFLOW Online portal and printed on the device. All mobile print jobs are displayed in the dashboard's 'My Queue' widget. While the job remains in the secure print queue, users can also delete the print job using the widget.

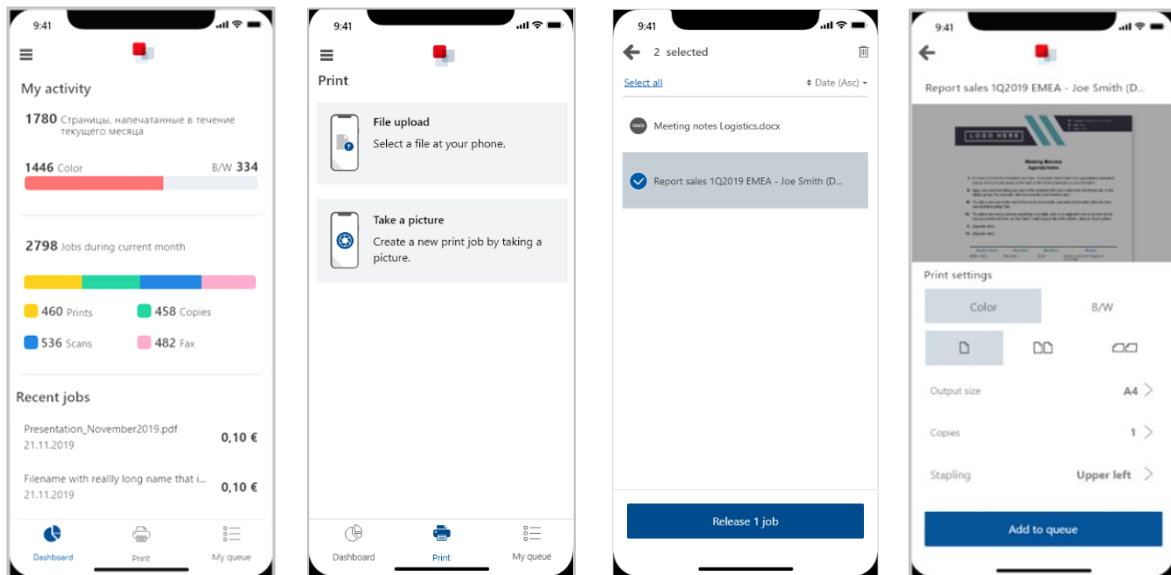
2.2.3.1. uniFLOW Online Print & Scan app

The uniFLOW Online mobile app allows users to submit and release jobs from their Android™ or iOS® devices. The app becomes available by downloading it from the Google Play Store (Google Play and the Google Play logo are trademarks of Google LLC.) or from Apple's App Store (App Store and the App Store logo are trademarks of Apple Inc.). The app includes a dashboard that displays statistical information about the current user's print behavior.

The uniFLOW Online Print & Scan app offers fast print job submission:

- File upload; selecting a file from the phone
- Picture; a new print job by taking a picture with the phone
- 'Open in...'; printing directly from within other applications
- Long press on the app icon

Finishing options can be set within the app. My Print Anywhere ensures print job availability on every device. Current print jobs can also be accessed and released on any device from any vendor via the app. When releasing a print job via the app, the user must scan the QR code at the machine. Thus, Secure Printing is enforced. QR codes can be generated for any printer from any vendor with a valid subscription.



2.2.3.2. Web upload and email printing

Print jobs are either submitted via web upload within the uniFLOW Online tenant or sent to an email address (e.g. mobileprint@<tenant_domain_name>.<region>.uniflowonline.com). uniFLOW Online supports the highest security standards with OAuth 2.0. OAuth 2.0 authentication supports configured external email providers for incoming and outgoing emails. It is supported for Microsoft 365 and Gmail™ by default. Additional email providers can be added via custom configuration.

Users are identified by their email addresses, whereby a user can have multiple email addresses. Print jobs are converted from the native format to one recognizable by the printer upon receipt.

2.2.3.3. Mobile Printing for guests

Print jobs are sent to an email address (e.g. mobileprint@<tenant_domain_name>.<region>.uniflowonline.com). Upon receipt of the email, the following will occur:

- 1) Guest users will receive an email with instructions on retrieving their print job and a temporary Job Code.
- 2) Print jobs are converted from the native format to one recognizable by the printer.

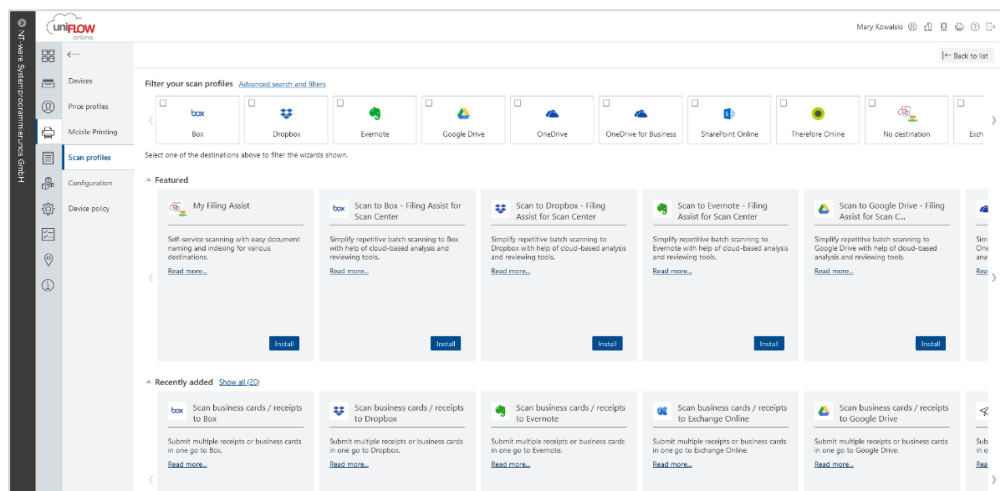
Mobile submissions are stored in the uniFLOW Online data center. Administrators can configure to print the email body text, the attachments, or both. Also, default behaviors such as duplex and B/W can be set.

2.2.4. Secure document scanning

With uniFLOW Online, users can scan documents directly from most Canon multi-functional printers supporting the Universal Login Manager. The lean and intuitive user interface of the workflows helps to bring about immediate gains in productivity. The scan workflow 'Scan to Myself' is pre-created. Users can also scan to SAP® Concur® or one of the following cloud-based destinations: Box, Dropbox, Evernote®, Google Drive™, Microsoft Exchange Online, Microsoft OneDrive/ OneDrive for Business, Microsoft Teams, Microsoft SharePoint Online, Raku-Raku Seisan (Japan) and Therefore™ Online. In addition, scanning to the user's desktop, an on-premises network folder, or a preset email address is possible. Access to scan profiles can be restricted to individual users or groups. To reduce the need for user interaction, document-splitting rules can be enabled, i.e. documents are split after every 'x's page when there is a blank page or when a barcode is recognized.



Administrators can define default scan settings and output formats within the uniFLOW Online portal. The following settings can be applied: simplex/duplex, image mode, color mode, scan resolution, scan automatically, continue automatically, show preview, file format, business card/receipt-scanning, blank page removal, barcode recognition, document splitting (blank page, barcode, x-page, file size). Other output settings can apply through document type selection: despeckle, deskew, dark border removal, and orientation detection. Next to scan settings, the following output formats are supported: TIFF, PDF, cloud-compressed/ device-compressed PDF, searchable PDF (IRIS OCR/device OCR), encrypted PDF, Microsoft Word, Excel and PowerPoint. The scan template library provides a tool to easily install complex and straightforward scan workflows.



Scans can be distributed to a specific target folder or to the previously selected folder of a scan destination to simplify recurring scan processes. Users can also browse through the root of their destination chosen to select their folder of choice. Additionally, specific folder rules for cloud-based scan destinations can be set to reduce

the time spent at the device, thus boosting productivity. Rules like folder hierarchy and folder naming can be applied to every user. If folders do not exist, they are created during the scan process.

uniFLOW Online also integrates with the native scanning features of the device and supports the device's scan-to-email/scan-to-myself functionality.

2.2.5. Scan center

The scan center accelerates the structured storage of documents by learning document types and recognizing OCR blocks. File name and folder path rules based on document content can be applied and required metadata can be identified automatically. The scan center allows manual job delegation or, upon configuration, automated delegation after a specific time.

Filing Assist – automated batch scanning

Filing Assist with automated batch scanning is perfect for repetitive scan processes of similar document types such as

- Invoices
- Picking lists
- Delivery notes
- Offers

Multiple users can easily use learned scan workflow templates to store documents in a structured way. The administrator presets all job properties, e.g. scan destination, root folder rule, file name rule, file format and required metadata. In the ideal case, documents are already trained and metadata is filled when the document appears in the scan center. The user must only approve documents to be sent to the scan destination.

My Filing Assist – self-service scanning

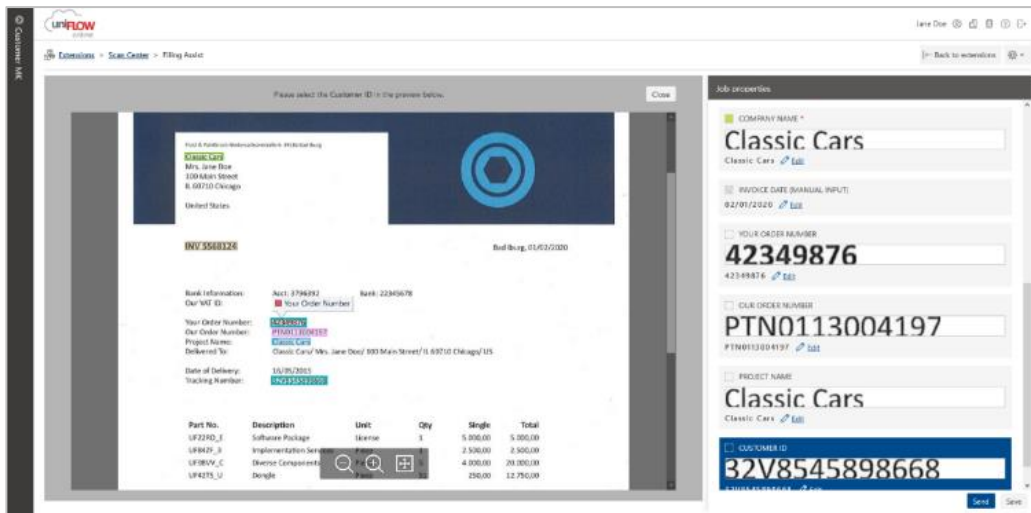
The end user-driven scan workflow template 'My Filing Assist' aims to improve non-repetitive and user-individual scan processes. The end user sets job properties within the scan center. These include the scan destination, root folder, file format, file name, and selected scan destination metadata. Each document type must be trained by the end user once; identical document types are recognized.

The screenshot displays the configuration interface for a scan job. It is organized into several sections:

- Destination:** Includes a 'Scan Destination *' field set to 'GoogleDrive' and a 'Root folder selection /Invoices' field.
- Output settings:** Includes a 'File format *' field set to 'PDF cloud compressed'.
- Attributes:** Features a 'FILE NAME (MULTIPLE SELECTION) *' field. Below it is a preview of a document with the text 'Classic Cars' and '42349876'. The preview shows the document's content as it would appear in the scan center, with a blue header and a white body containing the text. Below the preview, the filename 'Classic Cars_42349876' and an 'Edit' link are visible.

A legend at the bottom left indicates that an asterisk (*) denotes required fields.

Once a new scan becomes available in the scan center, uniFLOW Online will inform the user. The user can select job properties such as metadata. The metadata manager facilitates metadata selection as it allows to define the format type. The ability to save matching updates towards a learned document can be restricted to specific users or groups. Denied users will only be able to apply changes to the 'current document'; i.e. changes will not apply to other rematching documents. If the user does not process/ confirm the scan job, it is sent after 24h to the user's email address.

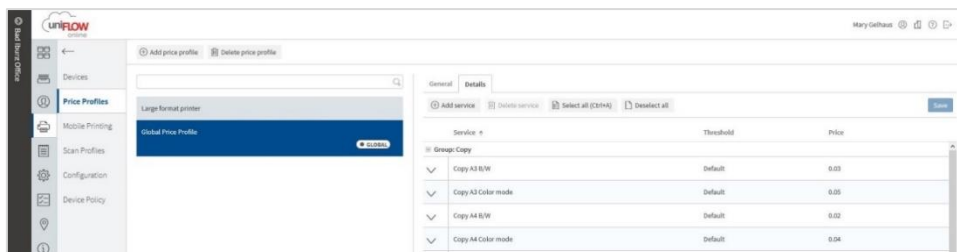


2.2.6. Print and copy accounting

On identification, additional copies or scans made on the device can be apportioned to the user or department. Print jobs originating on a PC are tracked according to the user or department login details.

With ULM-enabled Canon devices, job logs are collated (using CPCA) and sent to the uniFLOW Online portal to compile the reports. With non-Canon devices connected to a uniFLOW Release Station, print/ copy data is forwarded by the uniFLOW SmartClient. Note that a copy cable is required for enabling copy counting on non-Canon devices.

When uniFLOW Online is used as an accounting-only solution, it can also record completed jobs printed on other devices; the uniFLOW SmartClient is utilized to forward the accounting information to the uniFLOW Online portal. Print job titles are sent to the uniFLOW Online portal; however, the administrator can configure this to be excluded in any reporting. The cost for print, copy and scan jobs are set within the uniFLOW Online portal; different printers can be allocated individual price profiles.

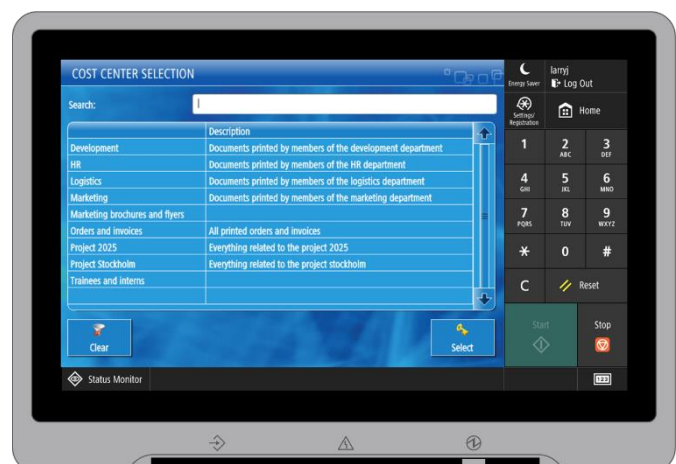


2.2.7. Cost centers

Cost centers allow deciding on a per-job basis which budget should be charged with a print or copy job. The cost center extension allows for creating and managing cost centers so that users can charge jobs to different projects or cases rather than to one department or user account.

A user can select cost centers at print job submission after device login. Alternatively, default rules can be applied. In case multiple rules have been configured, the following order applies to the cost center selection (from top to bottom):

- Cost center selection after device login
- User defaults



- Device defaults
- Location defaults

Access to cost centers can be restricted on a per-user/ per-group basis, ensuring users only see those cost centers relevant to them at the device.

2.2.7.1. Budgeting support

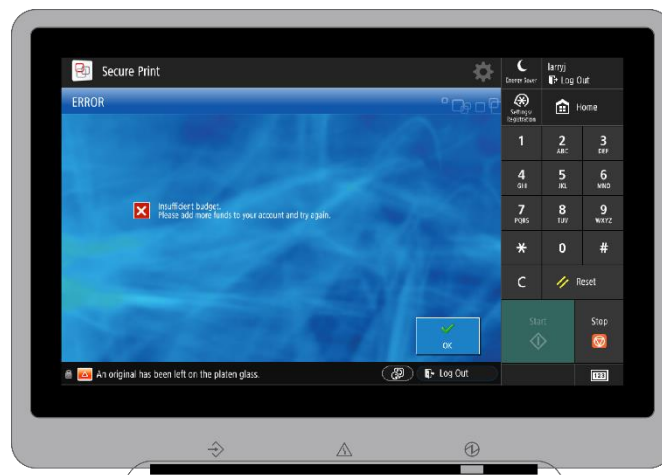
Budgets are the perfect way to charge users for the costs of their print and copy activities. If the budget is exceeded, printing/copying can be stopped altogether, and users are notified that their funds have run out. Balances can be recharged automatically by utilizing Microsoft PowerShell scripts, by using PayPal™, or a cashier can add funds manually to a user's account where a personal cash-based system is required.

Double wallet system

The double wallet system differentiates between primary and secondary wallets. Thus, it is possible to set, e.g. the amount of the primary wallet manually on special events or automatically on regular occurrences to a defined amount. The primary wallet is first charged for print and copy costs. In environments where these activities are not offered for free, e.g., schools or public, users can top up the secondary wallet with a personal budget. The secondary wallet is accessed only after the primary wallet is depleted or has insufficient funds.

Insufficient budget

Users see their remaining budget when accessing the device. uniFLOW Online will calculate which jobs can be printed with the remaining budget and reject the job(s) exceeding a user's budget.



Canceled print or copy jobs

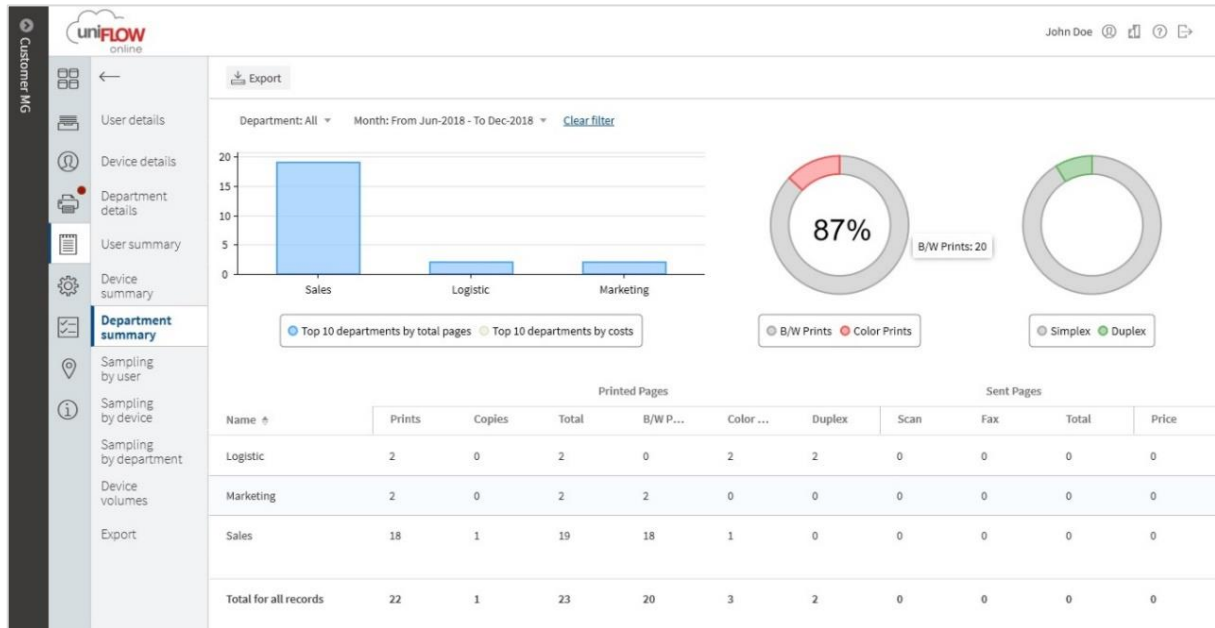
Jobs might be canceled due to technical issues such as paper jams. The resulting amount of canceled print or copy jobs will automatically be refunded and shown in a relevant transaction entry. Each copy session lasts for a specific period, and possible refunds will be calculated after the session end, which can take up to 30 minutes.

With budgets enforced, print jobs cannot be released in emergency mode, i.e., the device cannot reach uniFLOW Online, and users cannot print directly from cloud sources; instead, they need to 'Save to queue' before printing. Budgets can be enabled/ disabled for individual users/ groups or locations only to bypass the restrictions.

2.2.7.2. Reporting

A business's print, copy, fax and scan usage are of little use unless the information can be collated into reports. The uniFLOW Online portal contains graphical report types that a customer can create - user details, device details and summary, sampling by department and many more. Report contents can be changed instantly by selecting filters, e.g., specific users, groups, printers, or date ranges. Choosing a location through the panel on the left side of the UI will only show data relevant to that location. The detailed reports display the last 100 jobs per user, device or department. Summary reports show the last year's data, and sampling reports reveal

data from the last six months. All data from these reports and monthly raw data for the previous six months can be easily exported into CSV format. In addition, it is possible to export the data to various cloud storage services automatically.



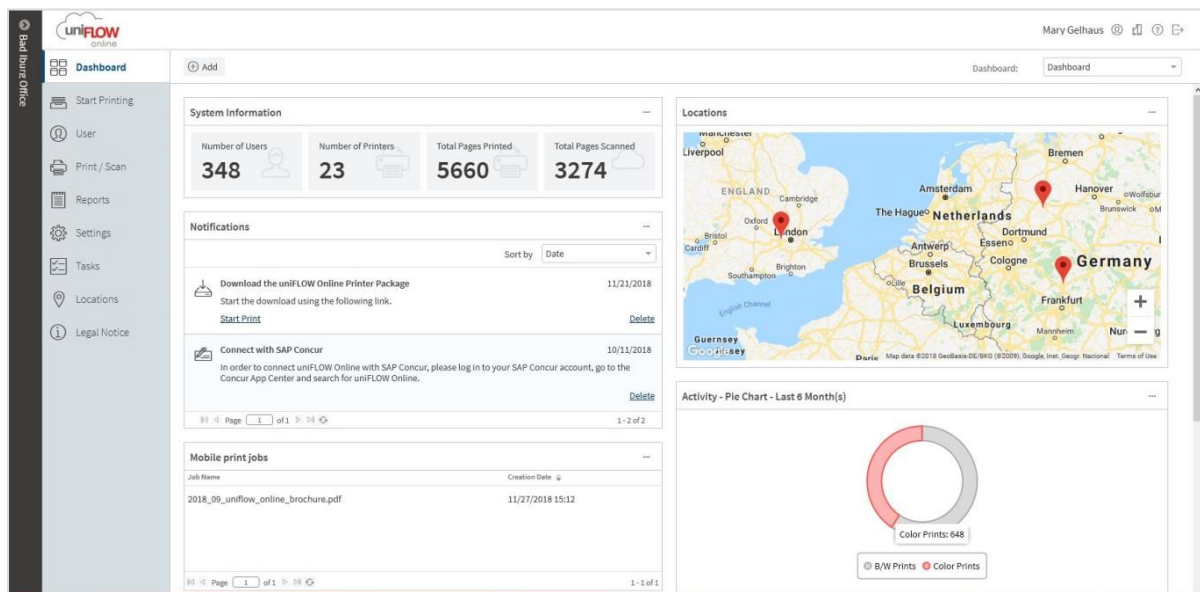
Access to reports can be restricted, though users can see their printing usage when logging onto the portal. This personal page displays a breakdown of the user's most recent jobs and a historical trend chart.

2.2.8. Fleet Management

Fleet Management offers an easy toolset for organizations to manage their printer fleet of Canon imageRUNNER ADVANCE DX devices. Personalized dashboards with powerful widgets give administrators a detailed overview of their printer fleet. Meter readings are collected automatically from these devices, and notifications on status changes can be sent. Fleet Management reporting will reveal the actual running costs, and CSV export is available.

2.2.9. Dashboards

The dashboard is where widgets that collect and visualize data from various uniFLOW Online pages are located. Multiple dashboards can be configured, and widgets may be dragged and dropped as required, enabling the design of dashboards to meet personal needs.



2.2.10. Audit logging

Audit logs can record administrator and user actions and help to identify, in the event of a security problem, the cause. If enabled, uniFLOW Online can collect logs such as operation history in the tenant or device login history. The administrator can retrieve audit logs via a CSV file during any six-month period.

Please note that by default, the audit log functionality is disabled. If the uniFLOW Online audit log functionality were to be enabled, a pre-sales (PS) request would have to be raised via the NT-ware Customer Portal. Only specific enterprise customers with more than 100 paid device subscriptions are eligible. Upon receiving the request, the NT-ware Business Development team will review and decide on a case-by-case base if the request will be accepted or denied.

2.2.11. Home-working support

With working from home almost becoming the default these days, uniFLOW Online also supports users working in a home-office environment by connecting Canon PIXMA/ MAXIFY inkjet printers. It is possible to track jobs printed from the company laptop and reimburse them with the connection.

In addition, home-office workers can utilize the same scan to myself and Filing Assist scanning workflows as if they were in the office. With this, they can scan a document on their Canon PIXMA/ MAXIFY inkjet printer, so it becomes available either in their email or in the scan center for further processing.



Scanning into a fixed Microsoft Team or Channel is also possible to allow home-office workers to collaborate with their teams utilizing Canon inkjet devices efficiently. The administrator must configure additional scan profiles when scanning to different Teams/Channels.

2.3. Technical requirements

2.3.1. Bandwidth requirements

A working internet connection is required to access the uniFLOW Online portal. This is the responsibility of the customer. No special bandwidth rates are necessary.

Bandwidth is consumed with initial configuration data and accounting data transfer to the cloud. Both actions employ tiny data packages with minimal consumption of bandwidth. An internet connection is required when retrieving mobile print jobs sent via email to uniFLOW Online. Regular secure print jobs can remain on the local network, so only print job information communication between the uniFLOW SmartClient and the device is handled via the cloud. Depending on the configuration, regular secure print jobs can also be sent via the uniFLOW SmartClient to uniFLOW Online. When a company decides to use this option, then a high consumption of bandwidth can be expected.

2.3.2. Requirements for uniFLOW SmartClient

Please check the uniFLOW Online tech data sheet for the requirements on the uniFLOW SmartClient.

2.3.3. Requirements for Direct Secure Print

Please check the uniFLOW Online tech data sheet for the requirements on Direct Secure Print.

2.3.4. Requirements for Data Collection Agent

Please check the uniFLOW Online tech data sheet for the Data Collection Agent (DCA) requirements.

2.3.5. Browser support

Please check the uniFLOW Online tech data sheet for the supported browsers that can be used to access the uniFLOW Online UI/ register the uniFLOW SmartClient/ configure the Universal Login Manager/ configure the uniFLOW Release Station.

2.4. System security

2.4.1. Security – uniFLOW Online platform

As with any cloud solution, system security is of critical importance. The following design elements of uniFLOW Online ensure that maximum protection is achieved.

No passwords are stored in uniFLOW Online

uniFLOW Online does not store any user credentials such as passwords. Instead, it uses a claims-based approach to identify users, which accepts login credentials from multiple identity providers. The default provider is Microsoft Azure Active Directory. Alternatively, administrators can use Active Directory Federation Services (ADFS) to integrate with e.g. Microsoft Office 365 or their own locally hosted Active Directory. In addition, it is possible to make use of OpenID Connect logins like AuthO, Okta, OneLogin™, Ping Identity or shared web identity providers like Google™, Yahoo!® or Windows Live ID. Provided the customer's local Active Directory is connected, any password changes or user additions are automatically updated and recognized in uniFLOW Online. For privileged roles, Multi-Factor Authentication is required.

Multi-Factor Authentication (MFA)

To safeguard access to uniFLOW Online and prevent unauthorized access, MFA has been implemented for those users with uniFLOW Online accounts with a privileged role to enhance overall system security. MFA requires these users to identify using two different identification mechanisms; a known credential (username and password) and a physical device (a token generator/mobile phone) to protect users from unauthorized persons trying to access their uniFLOW Online account.

Secure Printing, where all print traffic must stay within the company network

By default, uniFLOW Online stores print jobs on users' local PCs using the uniFLOW SmartClient. Supporting Canon imageRUNNER ADVANCE (DX) and Canon imageRUNNER with AddOn Platform can also be used for local print job storage. Thus, all print traffic can stay within the company network. Print jobs are only released to a selected printer once a user has identified at that device. The spool file is deleted automatically from a user's PC once printed or following a preset period.

Secure printing in Zero Trust environments with micro-segmentation

Zero Trust models protect digital environments by maintaining strict access controls and not trusting anyone inside or outside the network by default. Client PCs are not trusted, and thus, print jobs cannot be sent directly to a device. Instead, uniFLOW Online will be the mediator. After user identification and print job selection, uniFLOW Online sends the print job directly to the device for secure print release. The print files are deleted automatically from uniFLOW Online once printed or after a preset period.

Mobile print jobs are sent via the uniFLOW Online Print & Scan app

Users can print jobs from their mobile devices, smartphones, or tablets by sending the file to be printed via the uniFLOW Online Print & Scan app. In addition, mobile jobs can also be sent via email or web upload. Should the file need conversion from its native file format into a language, the printer can process; this will happen within the regional data center hosting the uniFLOW Online service, i.e. customer data does not leave the data center. Once converted, the original file is deleted. The converted file is held within the regional data center until the user selects it to be released/printed or until they are automatically deleted after a preset time.

uniFLOW Online only stores minimum data

Only accounting data and configuration information are sent to the uniFLOW Online tenant outside the company network. By default, print jobs' file names are not uploaded to uniFLOW Online, which removes another potential security risk. Other sensitive information, e.g. ID card or PIN numbers stored in users' accounts, are encrypted via a one-way salted hash to enhance security. Mobile print jobs and documents printed from cloud services and thus sent via the cloud are converted and held within the regional data center until they are released/printed or automatically deleted after a preset time.

Helping to comply with GDPR

uniFLOW Online helps increase document security and supports the administrator in fulfilling user rights related to GDPR. Administrators can easily collect all users' data by downloading a JSON file and handing it over to the user, using their right of access. The delete button erases all user data from the UI, active databases, and

databases holding deleted versions and object histories. The accounting data of these users is displayed in one consolidated 'Deleted Users' report, and related print job names are anonymized.

Non-default password support

New uniFLOW Online tenants are created with a unique password that needs to be changed by the administrator upon the first login. uniFLOW Online also takes over the password management for device applets, i.e., the Universal Login Manager or Release Station. A unique password is generated and pushed to connected device applets together with the behavior update. Furthermore, PIN codes used by users for device identification are also auto-generated. This increases security, as it protects against attacks done by botnets.

Audit log on request

Audit logs can record administrator and user actions and, in the event of a security problem, help to identify the cause. Audit logs will be enabled, and keep log data for six months upon specific customer request. The administrator can retrieve audit logs via CSV file.

No customer tenant data is shared with Canon or Canon partners

Customer data is stored in uniFLOW Online according to statutory requirements. Customer data is not shared with third parties, including Canon or Canon partners selling the service. Canon/ the Canon partner can gain insights into customer names and expiry dates of licenses. The customer's user names, details, and print data are only visible to the individual customer or if a temporary service account was created.

uniFLOW Online is hosted in regional Microsoft Azure data centers

uniFLOW Online is hosted in Microsoft Azure data centers distributed across the globe. The multiple Microsoft Azure data centers used by uniFLOW Online allow customer data to respect data sovereignty. The customer data remains within the local region, i.e., European customers' data will always be stored in Amsterdam's European data center. In contrast, US customers can be sure their data will never leave the US.

More information about Microsoft Azure and its security and compliance features can be found on the website: <https://azure.microsoft.com/en-gb/support/trust-center/>.

2.4.2. Security – Microsoft Azure hosting platform

Microsoft Azure provides businesses with the data security, privacy, control and transparency they require. Security and privacy are embedded in the Azure platform and have used the Security Development Lifecycle (SDL) protocol from initial planning to solution launch. The Operational Security Assurance methodology provides the security guidelines for the operational processes, while Privacy by Design governs how Microsoft builds and operates products.

Microsoft Azure uses multiple safeguards to protect customer and enterprise data. These security practices and technologies include:

- **Identity and access management** – The Azure Active Directory helps ensure that only authorized users can access the environment, data, and applications. It provides a multi-factor identification process for a highly secure sign-in.
- **Encryption** – Industry-standard protocols are employed to encrypt the data that travels between the devices and data centers and internally within the data centers
- **Secure networks** – The Azure infrastructure relies on security practices and technologies to connect virtual machines and on-site data centers while blocking unauthorized traffic. Azure Virtual Networks extend your on-site network to the cloud via a site-to-site virtual private network (VPN). ExpressRoute can also create a cross-premises connection when the internet is required.
- **Threat management** – Microsoft Antimalware protects Azure services and virtual machines. Microsoft also employs intrusion detection, denial-of-service (DDoS) attack prevention, penetration testing, data analytics, and machine learning to strengthen its defenses and reduce risks constantly.
- **Compliance** – Microsoft complies with international and industry-specific standards and participates in rigorous third-party audits to verify security controls.
- **Physical security** – Azure runs in geographically distributed Microsoft facilities and shares space and utilities with other Microsoft Online Services. Each facility is designed to run 24 x 7 x 365 and employs various measures to protect operations from power failure, physical intrusion and network outages. The data centers comply with industry standards for physical security and availability, e.g. ISO 27001. They are managed, monitored and administered by Microsoft operations personnel.

3. Selling uniFLOW Online

3.1. Key customer benefits

Prevent unauthorized use of the device and increase document security

uniFLOW Online enables administrators to allow access to printers to authorized users only to prevent data breaches and misuse as the device is locked so that print, scan, copy and fax functionalities are unavailable to unauthorized visitors or employees. Furthermore, scanned PDF documents can be encrypted through password protection, ensuring the security of digital documents.

Improve office productivity

Increase employee productivity by providing mobile printing facilities, print from cloud and scan profiles. uniFLOW Online simplifies mobile printing, no matter how users want to send their print jobs. Print from cloud enables access to documents at the device from where they are stored and removes yet another work task for the user. Users can print wherever they need to and scan directly to themselves, Google Drive™, or various cloud-based scan destinations, making processes much faster and more productive. Scan profiles are directly available and follow the user from device to device

Gain control over your costs

uniFLOW Online makes costs visible, which means greater control of the organization's environment. Administrators can see exactly what users and departments are spending, who is spending it, and how to recover costs. This overview helps establish print policies that will save costs and increase efficiency.

Reduce the impact on the environment

uniFLOW Online can help reduce environmental impact and support sustainability initiatives by optimizing printing procedures and improving internal processes that rely heavily on paper. This solution prevents unnecessary paper waste as users can only print what they need. uniFLOW Online can help reduce power consumption by eliminating 'Always On' print servers.

3.2. Selling points of uniFLOW Online

By combining a powerful cloud platform with several unique uniFLOW technologies, uniFLOW Online is a unique software solution that enables businesses to transform their on-site infrastructure into a cloud-based print and scan management system.

Innovative cloud platform

The entire configuration and management of uniFLOW Online take place in the public cloud. Administrators log in to the cloud portal to manage users, groups, printers and running reports on device usage. No local servers must be purchased, maintained or managed. Each uniFLOW Online instance is logically separated from other instances via tenant isolation. That way, it can be assured that no personal data is mixed up with data from, e.g. other accounts.

One single print queue

The uniFLOW Universal Driver provides one single print queue for users to print their jobs regardless of the printer model. It provides a simple interface for secure and direct printing, with advanced printing features that encrypt and compress print jobs, thus reducing network traffic and enhancing security. Users can release their desktop, mobile and cloud print jobs from a single print queue.

Local processing of print jobs






User's print jobs can be processed on the client's PC or a supporting Canon imageRUNNER ADVANCE (DX) / imageRUNNER with AddOn Platform and retained securely until required. When print jobs are transferred to the printing device, they are always compressed and protected. Due to their nature, mobile print jobs and print jobs from other cloud services are always processed in the cloud. Furthermore, uniFLOW Online also allows the processing of regular print jobs in the cloud.

Control device identification

The Universal Login Manager is installed directly on the Canon device and communicates with uniFLOW Online and the uniFLOW SmartClient to control device identification. Once identified, the user's secure print queue and available scan profiles are displayed. There is also the opportunity to change finishing options directly at the device, saving valuable time. For any other device, the uniFLOW Release Station connects to uniFLOW Online directly.

3.3. Product positioning

While there is some overlap in functionality between uniFLOW Online and the other uniFLOW products, such as uniFLOW Online Express, an entry-level solution, or uniFLOW for SMB, there are also apparent differences.

					
Architecture	Cloud-based	Cloud-based	Server-based	Server-based	Server-based
Number of users	Unlimited	Unlimited	Max. 500	Max. 500	Unlimited
Number of devices	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Access control	✓	✓	✓	✓	✓
Secure printing		✓	Optional	✓	✓
Mobile printing		✓	Optional	✓	✓
Scanning	Simple	Advanced	Superior	Optional	Superior
Filing Assist for scanning		✓			
Cost Tracking	Advanced	Advanced	Superior	Superior	Superior
Cost center		✓	✓	✓	✓
Budgeting		✓	Optional	✓	✓
Device Management		✓	✓	✓	✓
Workflow engine			Optional	Optional	✓
Print Room Management					✓

3.3.1. When to sell uniFLOW Online?

uniFLOW Online suits businesses of all sizes, including branch offices with print and scan management requirements (access control, secure printing, mobile printing, secure document scanning, cost tracking), who do not want to/ are unable to invest in or manage any local servers.

It can be sold to customers who require:

- Cloud-based infrastructure without any local server involvement
- Device access control/ device function restriction
- Secure printing across all Canon devices supporting Universal Login Manager and any other device using the uniFLOW Release Station
- Direct printing to almost any network printer
- Print job submission from anywhere (including Mobile Printing for guests)
- Secure document scanning workflows
- Filing Assist/ My Filing Assist
- Print, scan, copy and fax accounting on Canon MFDs
- Single-level cost center support
- Fleet Management

3.3.2. When to sell uniFLOW?

It might be preferred to sell uniFLOW/uniFLOW for SMB/ uniFLOW Capture if the following differences in functionality play a role:

uniFLOW suits better for customers who require:

- Secure printing across multi-vendor devices using uniFLOW Embedded Applets
- Locally hosted mobile printing, i.e., Apple AirPrint®
- Superior scanning, e.g. secure and personalized scan workflows/ scan processing, advanced workflow configuration
- Print Room integration (including job ticketing, central job management, web-based document make-ready)
- Scalability in terms of features and modules
- Customers requiring customization of the product to their specific requirements

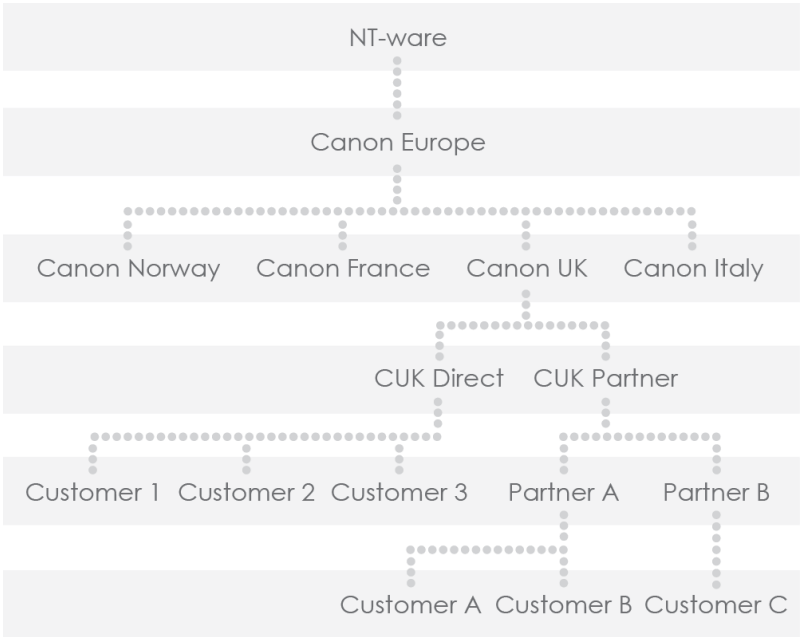
4. Tenant management

4.1. Tenant structure

uniFLOW Online features a multi-tenancy software architecture, differentiating between management and customer tenants. A management tenant can have any number of child tenants. A management tenant is needed when multiple customer tenants must be managed via one tenant; for instance, Canon and Canon partners manage several customers. In contrast, a customer tenant is for end customers only. Customer tenants cannot create or manage other tenants. The hierarchy structure of customer tenants differentiates between tenants created by Canon or a Canon partner and self-created customer tenants (uniFLOW Online Express tenants).

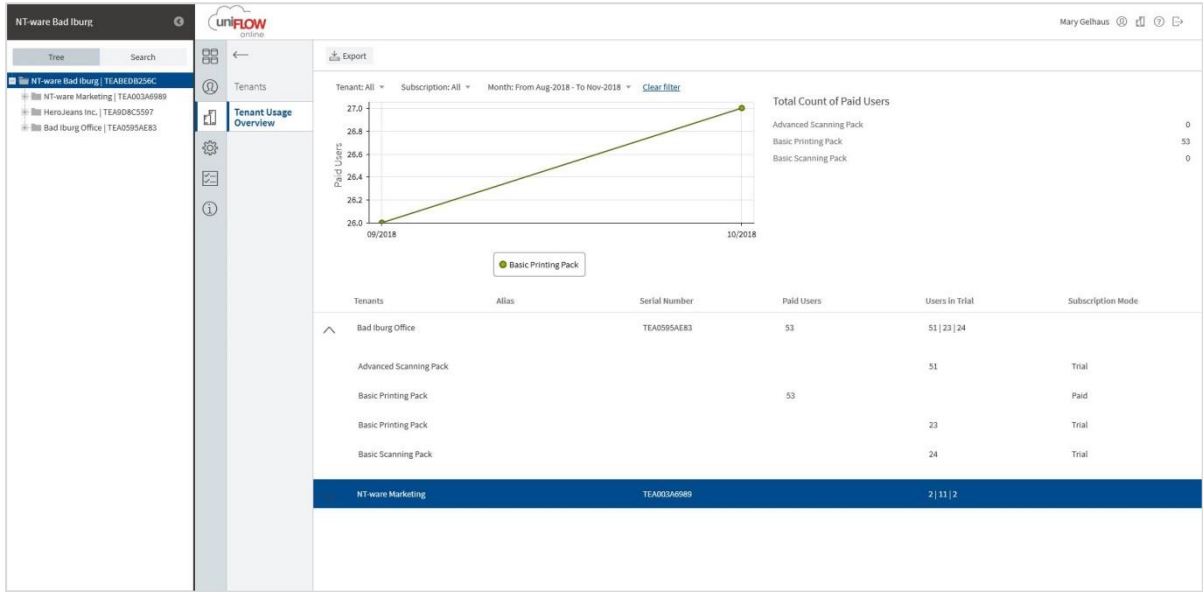
Tenants are generally held in regional data centers to ensure customer data does not travel from one regional data jurisdiction to another. For example, the tenant hierarchy (Canon, partners, customers, etc.) under Canon USA will be physically hosted within the USA. In contrast, the tenant hierarchy under Canon Europe will be physically hosted in the Netherlands. It is impossible to move customer tenants from one data center to another. If required, NT-ware can host a tenant for a US customer in the uniFLOW Online deployment based in the Amsterdam data center. It is also possible that uniFLOW Online will be deployed in multiple data centers in the USA or Europe (e.g. US data centers can be hosted in West Virginia and/ or California).

The management of tenants is either handled locally by Canon NSOs/ local partners. An example of the hierarchical tenant structure is shown below.



In contrast, the self-created customer tenants are so-called 'free floating' tenants who are not part of the tenant structure, as shown above. Only if the tenant serial number of a Canon/Canon partner tenant has been filled in during the registration process, the newly created tenant is part of the main tenant structure. Each tenant is isolated from both its associates and parent company. It is only possible for a parent to access a child tenant via a temporary service account or a user account with the Partner Admin role selected. Temporary service accounts can be created for users from an upper tenant. If required, an expiration date can give temporary access to the tenant, e.g. to provide tenant support or during the initial tenant setup. The administrator can also revoke a service account at any time. A user with the Partner Admin role can also access the tenant to provide, e.g. tenant support. The user has similar access rights as the administrator except for access to user information. No user-related information is available due to user privacy and security aspects.

A tree view showing all child and sub-child tenants is available. The tree view lists the tenant serial number and an alias name to provide an overview of all existing child tenants. If a temporary service account has been created, the service account user can also gain immediate access to the sub-tenant via the tenant tree view. Reporting capabilities for post-pay tenants (EMEA, Australia and Japan) offer Canon and Canon partners a more precise insight regarding the actual subscription usage by customer tenants. Management tenants have an overview of their child tenants and information regarding the subscription mode, serial number, alias name, and active users, allowing for a better insight into subscription details and active usage of uniFLOW Online. In addition, the menu item "Billing" is available in management tenants for downloading the customer tenant's usage information, whereas the audit log aims to track all subscription changes made to a customer tenant.



Benefits of a tenant management system

- Canon and Canon partners can run trials independently
- There are no logistical requirements to deliver subscriptions, i.e., no emails, CDs, etc.
- Immediate provision of subscriptions upon receipt of PO
- Canon partners have complete visibility of all their customers
- Customer and partner data is secure/ confidential, so the parent tenant cannot view it without granting access to it

4.2. Tenant creation by Canon or a Canon Partner

4.2.1. How to create management and customer tenants?

In the uniFLOW Online Portal, the Root Administrator and other authorized administrators of a management tenant can create additional child tenants upon successful identification. Separate wizards are available for both tenant types (management tenant and customer tenant) to guide the creator through a straightforward setup process. Administrators can directly define the subscription of that tenant within the wizard, e.g. feature set and active users. Upon successful creation of the child tenant, an email will be sent to the user who created the tenant and the email address of the Root Administrator of the new tenant. The system automatically generates a tenant serial number. This tenant serial number is unique for a specific tenant and is required for several purposes, e.g. post-sales support.



The Tenant serial number will be a combination of letters and numbers, prefixed with 'T<##>', to indicate that it's a Tenant serial number (rather than a traditional uniFLOW base serial number), plus two letters identifying the data center. Examples:

- TEU000001 - A Tenant SN in the EU Amsterdam data center
- TUS000001 - A Tenant SN in the US – West Virginia data center
- TJP000001 – A Tenant SN in the Japan data center
- TSG000001 – A Tenant SG in the Singapore data center

4.2.2. Root Administrator

A 'Root Administrator' user is always created when creating a new tenant. The administrator role of the Root Administrator cannot be changed. There will be a maximum of 1 Root Administrator per tenant. Users with the administrator role have special privileges like the ability to create new users and reports. It is always advised to create a second administrator.

Suppose the root administrator of a tenant changes or the original password email has not been received. In that case, a management tenant can change the root administrator's email address or trigger to resend the confirmation with a new password. This can be done in the 'Root Administrator' tab next to the 'General' tab in the management tenant, displaying the tenant-info email address and root administrator details (name, username, email address). The 'Root Administrator' tab is only available if the tenant runs either in trial mode, ready for trial mode, or expired mode, and no other users and devices have been added.

The screenshot shows the 'Root Administrator' configuration page. At the top, there are three tabs: 'General', 'Subscriptions', and 'Root Administrator'. Below the tabs, a message states: 'You are able to modify the root administrator account for this tenant because this tenant runs in trial mode, no devices have been added and no other user than the root administrator exists.' The form contains the following fields:

- Current Email:** JKohlstedte@nt-ware.com
- New Email:** A text input field containing 'e.g. john.doe@companydomain.com'. Below the field is a red warning icon and the text 'This field is required'.
- New Email Confirmation:** A text input field containing 'e.g. john.doe@companydomain.com'.
- Password:** A text input field. Below it is a password strength indicator: 'Use between 8 and 16 characters, and at least 3 of the following: lowercase characters, uppercase characters, numbers and special characters: #5%^&*_-+=[]{}|:~?^~*()';
- Repeat Password:** A text input field containing 'Confirm Password'.

At the bottom left, there is a warning icon and the text: 'Leaving the password field empty will generate a random one. An email containing the generated password will be sent to the provided address.' At the bottom right, there is a blue 'Save' button.

4.2.3. Manage user roles

The administrator can define the role per user during the user creation process, currently differentiating between user and privileged user roles. The available user roles differ between management and customer tenants. For management tenants, the following user roles are available: administrator, fleet manager, partner administrator, report manager, subscription manager, tenant manager, and user administrator. For customer tenants, the following user roles are available: administrator, budget manager, cost center manager, device system manager, fleet manager, partner administrator, report manager, and user administrator. Based on the predefined role, users have different access rights. Next to creating users, the administrator can disable a user to withdraw access to uniFLOW Online temporarily.

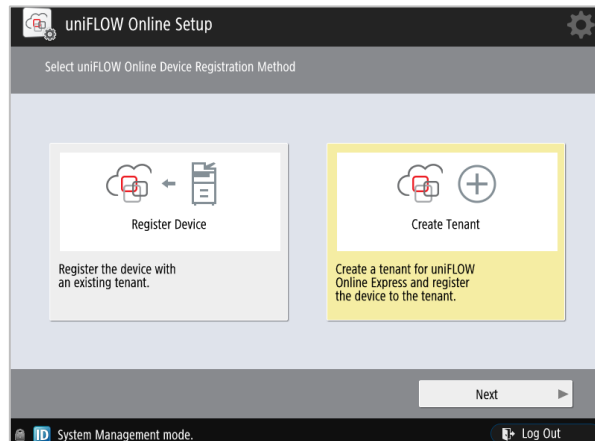
4.3. Tenant self-creation

With the launch of uniFLOW Online Express, every customer can self-create a customer tenant with the features available in uniFLOW Online Express. To create a tenant, the customer's administrator can go to the NT-ware hosted website for tenant self-creation or utilize the uniFLOW Online setup button on Canon

imageRUNNER ADVANCE (DX) with firmware 3.7 and later version/ on Canon imageRUNNER with AddOn Platform.

Tenant self-creation utilizing the uniFLOW Online setup button at the device

After selecting the 'uniFLOW Online Setup' button, an administrator can register a device or create a tenant. A new uniFLOW Online Express tenant can be created using the tenant creation wizard, and the device directly connects to this tenant. The administrator receives the tenant information as a printout and email (pre-inserted email address required). An administrator can access the uniFLOW Online portal and add or change the registration data on the initial login using tenant information.



Tenant self-creation via NT-ware hosted website

The tenant self-creation website is accessible via the following link:
<https://www.uniflowonline.com/express/registration/>

On there, the administrator must fill in the following information:

- Username and email address of the administrator
- Company sector
- Address
- Country
- Tenant name
- Optionally customers can enter the serial number of their Canon/ Canon partner tenant

After the customer has submitted the form, a tenant is automatically created in the regional deployment (e.g. the European deployment, the US deployment, etc.) to which the customer belongs (based on the country he has selected). At the same time, a 'Thank you' message is displayed, advising the customer that a uniFLOW Online Express tenant has been created and the browser can be closed. Simultaneously two emails are sent to the provided email address. One contains the tenant link, the username and the 'uniFLOW Online First Steps' guide, and one with a temporary password. Upon the first login, the user is requested to log in with the provided username and password and change their password.

The self-created tenants are so-called 'free floating' tenants who are not part of the tenant structure described above. Only if the tenant serial number of a Canon/ Canon partner tenant has been filled in during the registration process, the newly created tenant is part of the main tenant structure.



Please note:

Whenever a self-created tenant in the US deployment is created based on the country selection 'US, Canada, Mexico, or any country in the Americas,' a Dealer S/N must be provided.

4.4. Tenant claiming

To upsell the customer to a regular uniFLOW Online cloud module with paid subscriptions or to help the customer with the setup, the self-created customer tenant must be moved under the tenant structure of a Canon/ Canon partner. This can be done by claiming the self-created customer tenant. The tenant manager of a management tenant first asks the customer to enable the 'Allow to connect to a partner' switch in their tenant settings menu and requests the customer's tenant serial number.

Once the customer has enabled the switch, the dealer/NSO tenant manager needs to enter the tenant serial number of the customer tenant in the 'Claim Customer Tenant' function of the tenant's menu.

TENANT SETTINGS

General Subscriptions

Email marketing@nt-ware.com

Phone

Company Sector

Address Niedersachsenstraße 6, 49186 Bad Iburg

Country Germany

Serial Number TINTERNALLEB07CAC

Allow to connect to a partner

Enable this setting to allow a dealer to manage your account and provide services for it. For further information about this setting, please contact your local dealer.

Language English

Save Cancel

After submitting the claim, the customer receives an email with a link to approve/deny the claim. Once the customer has approved the claim, the tenant is moved under the tenant structure of the management tenant.

CLAIM CUSTOMER TENANT

Customer Tenant Serial Number

Please note that "Allow to connect to a partner" needs to be enabled before in the customer tenant settings. Also, an email requesting confirmation will be sent to approve this request.

Save Cancel

4.5. Tenant login

To access the tenant, the administrator has to log in. Each tenant has a "Root Administrator" assigned during the tenant creation process. The account is created as a 'uniFLOW Online Account' in the uniFLOW Online Azure AD infrastructure and is not tied to any local IT administrator account upon setup. The Root Administrator can access the tenant from other identity sources such as the customer's local Active Directory, Office 365 domain, OpenID Connect logins like AuthO, Okta, OneLogin™, Ping Identity, or shared logins such as Google. The process of connecting other identity providers is explained in the Online help.

4.6. Tenant deletion

uniFLOW Online provides two options for uniFLOW Online admins to delete a customer tenant. The first one is the automatic customer tenant deletion after 180 days of inactivity. The second one is the manual customer tenant deletion request that management tenant administrators can submit.

Automatic tenant deletion

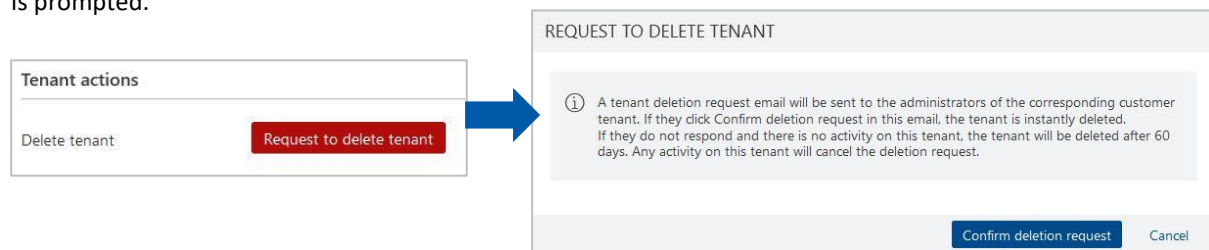
Automatic tenant deletion is executed after 180 days of no activity if no active subscriptions exist. After 120 days of no activity, all tenant and management tenant administrators are informed of the impending tenant deletion. If no countermeasures are taken, e.g., login to the tenant, all the tenant and management administrators will be informed that the tenant has been deleted after 180 days of no activity.

Manual tenant deletion

A management tenant administrator can also initiate a manual tenant deletion. This is only possible if the tenant has no active subscriptions. If active subscriptions exist, these must be discontinued before tenants can be deleted.

A tenant administrator must perform the following steps to submit a tenant deletion request:

1. Select a tenant to be deleted in the tree view
2. Hit the 'Edit' button, click 'Request to delete tenant', and click on 'Confirm deletion request' when a pop-up is prompted.



3. Upon receiving the deletion request email, the customer tenant administrator has to click the confirmation link in the email to confirm the deletion.
4. After entering the captcha data, the tenant administrator must click 'Confirm'. If the customer tenant deletion was successful, the confirmation is received via the browser, and the tenant is irreversibly deleted.



When deleting a tenant, the following data is deleted:

- The tenant
- Accounting data/ CSV report data
- All user accounts, identities, and the root administrator
- All other configuration data, e.g., Microsoft SharePoint Online/ Microsoft OneDrive for Business, Application ID, and Secret

Legal requirements stipulate the following data must be retained:

- The billing history
- Data populated up the hierarchy

5. uniFLOW Online subscription model

The customer tenant will have a certain number of user or device subscriptions available when licensed. The user/ device subscriptions are "named subscriptions" specific to the user/ device and are not "floating" or "concurrent." The following user subscription packs are currently available: 'Basic Printing,' 'Basic Scanning' and 'Advanced Scanning.' The following are available when using device subscriptions: Cloud Print & Scan Type 1/ Type 2, Cloud Image Processing Type 1/ Type 2, Cloud Link Print Connection Type 3.

For tenants in pre-pay mode (Americas and Singapore), the maximum number of users/ devices are set for a tenant by NT-ware logistics. For tenants in post-pay mode (EMEA, Australia and Japan), the parent tenant can set the maximum number of users/ devices connected to a child tenant. Users with the administrator role can assign user/ device subscriptions to the tenant up to the maximum defined users/ devices in the customer tenant. For pre-pay, this number is called the 'Maximum user count'/ 'Maximum device count.' Suppose a child tenant has already assigned users/ devices to a subscription. The parent tenant cannot decrease the 'Maximum user count'/ 'Maximum device count' below the number of already assigned users/ devices. E.g. a parent tenant sets the 'Maximum device count' for 'Cloud Print & Scan' to 15. If the child tenant then assigns 15 devices to that subscription, the parent tenant cannot change the 'total of device licenses' to 14 but can only increase the value.

Subscription	License Information
Cloud Print & Scan Device type 2	PENDING Activated: 0 of 1
Cloud Image Processing Device type 1	IN TRIAL Activated: 1 of 2 Valid until: 07/31/2020
Cloud Image Processing Device type 2	READY FOR TRIAL Activated: 0 of 0



Please note:
Subscriptions can only be assigned to customer tenants.

Please refer to the uniFLOW Online subscription guide and the tech data sheet for all the details of the subscription model and user/ device subscriptions.

6. Service and support operations

6.1. Service responsibilities

While uniFLOW Online operates on the Microsoft Azure infrastructure, each body has specific responsibilities to guarantee the successful operation of subscribed software/ service.

NT-ware responsibilities

- Maintain the uniFLOW Online infrastructure in the Microsoft Azure data centers (including any patches and software upgrades required for system enhancement).
- Ensure customer data stored in one regional data center is not moved to another data center.
- Notify Canon about any service outages promptly.
- Alert customers regarding subscription expiration.
- Maintain audit logs, including version changes, User ID, and date/ time.
- Ensure only authorized NT-ware staff can access uniFLOW Online backend infrastructure and make system changes.

Customer responsibilities

- Provide internet service that is required to access uniFLOW Online.
- Provide Operating System licenses and hardware required to run the uniFLOW SmartClient locally on PCs or laptops.
- Pay any subscription fees for different identity provider services.
- Pay for any security-related software required for a local PC or laptop.
- Backup of local PC or laptop.

Canon/ Canon Partner responsibilities

Canon/ Canon Partner must provide adequate staff training to perform the correct installation and configuration for uniFLOW Online (including uniFLOW SmartClient rollout and Universal Login Manager/ embedded Universal Login Manager installation).

Escalation path

Canon/ Canon Partners will follow the same escalation route for uniFLOW Online as uniFLOW (via the NT-ware Customer Portal).



Microsoft, Active Directory, Azure, Excel, Exchange Online, Microsoft 365, Microsoft Teams, OneDrive, One Drive for Business, PowerPoint, SharePoint Online, Windows and Word are either registered trademarks or trademarks of Microsoft Corporation and of the Microsoft group of companies in the United States and/or other countries.

www.uniflow.global
www.uniflowonline.com
www.syshub.global