

Celiveo 365

Cyber-Secure

- **AI Doc Management**
- **Cloud Pull Print**
- **Smart Scan to Cloud**

White Paper

https://www.celiveo.com

October 2026 – v2.0

Celiveo 365

©2026 Celiveo

Creating business solutions helping people to work, wherever

Revisions

Version	Date	Author	Comments
1.0	**20251001**	**BL**	**1st Edition**
1.1	**20260102**	**LD**	**2nd Edition**
1.2	**20260302**	**AA**	**3rd Edition**
1.3	**20260306**	**AA**	**4th Edition**
1.4	**20260422**	**LD**	**5th Edition**
2.0	**20261001**	**LD**	**6th Edition**

All product names, trademarks and registered trademarks are the property of their respective owners. All company, product and service names as well as logos used in this document are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement or recommendation.

Important: This document is non-contractual and Celiveo reserves the right to modify any specifications without advance notice.

About Celiveo 4
1. Executive Summary 5
2. Why Celiveo 365? 6
3. The Business Case for Celiveo 365 7
4. AI Document Management, Building a Corporate Memory 8
5. High Security Cloud Print, low IT 10
Business Aspects 10
Technical Aspects 11
Microsoft Windows Protected Print (WPP): A New Standard for Secure Printing 18
Printers and MFP support 19
6. Secure Scan to email, OneDrive 23
7. Easy and fast printer onboarding 25
Printer Discovery & Assessment Utility: Enabling Risk-Free Cloud Migration 26
8. Flexible and Secure User Authentication 27
Secure Guest Printing with Customer-Controlled Identity 28
Security and Governance Benefits 29
9. Empowering Location-Based Print Management and Security with Geotagging 29
10. Print rules 33
11. AI-DLP 34
12. Advanced Printer Tracking and Reporting by Power BI 36
13. Subscription 38
14. Celiveo 365 Web Admin Console 39
15. Ports, protocols and flows 42
16. Logs and Audit 46
17. Documents encryption 48
18. Security 49
19. GDPR, CCPA and Privacy Law Compliance by Design 51
20. Elasticity for Enterprise-Grade Performance 53
21. Service Level Agreement (SLA), RTO and RPO 54
Celiveo Service Level Agreement (SLA) 54
Recovery Time Objective (RTO) 56
Recovery Point Objective (RPO) 57
Operational Governance and Customer Responsibilities 57
22. Your Deployment Options 58
Shared resources with dedicated SQL database, on Celiveo Azure tenant 58
Dedicated resources and endpoints on Celiveo Azure tenant 59
Dedicated resources and endpoints on your Azure tenant 59
23. Supported Languages 60
24. Features list 61
Index 65

About Celiveo

Celiveo is creating business solutions helping people to produce, process and manage documents with full security, wherever they are. This offer starts with the most cyber-secure Cloud Pull Print and Scan solution, making it possible to print and scan through the Cloud with no local infrastructure and the highest Zero-Trust-Access security.

Celiveo is certified for ISO27001:2022 (full scope, no exception) and ISO9001:2015 for all its activities and SaaS offers.

Celiveo is organized into 4 sales and support structures:

- Celiveo EMEA
- Celiveo Americas (covering USA and Latin America)
- Celiveo Canada
- Celiveo Asia Pacific

You can contact them through the Celiveo web site at https://www.celiveo.com by clicking the links available at the bottom of the web page.

This international structure makes Celiveo one of the few Enterprise-Class print management software publishers capable of delivering service and support globally. Our solution is also localized in 20 languages to meet customers' needs.

When most solutions are for small and medium business, our clients are mostly large enterprise companies with high security, mobility and cost reduction requirements who find in Celiveo 365 a true Cloud, scalable, innovative and utterly secure solution.

This document describes the Celiveo 365 SaaS, how it can move your whole secure print and scan document management to the Cloud, for small to large global organizations.

1. Executive Summary

Celiveo 365 is a transformative, cloud-native SaaS platform designed to streamline corporate knowledge, document and print workflows for medium to large enterprises, creating both saving and extra profit by saving up to 2 hours of work per knowledge employee per day.

Built on Microsoft Azure and seamlessly integrated with Microsoft Universal Print and Entra ID, its Cloud Print Edition eliminates traditional document output infrastructure like print servers, drivers, and agents, delivering significant cost savings, enhanced security, and productivity gains.
Celiveo 365 Enterprise Edition adds comprehensive AI-powered information and document management, addresses the challenges of document chaos, inefficient searches, and insecure printing. Business benefits include rapid ROI, up to 1,000% in the first year, productivity improvements that reclaim hours per employee daily by automating document handling and reducing print volumes by up to 50%.

Celiveo 365 can be deployed in just one hour, requires truly little training and leverages Azure PaaS for elastic scalability, Zero-Trust security, and generative AI for intelligent processing.
All while ensuring compliance with standards like GDPR, HIPAA, and ISO 27001:2022.

This white paper explores the business and technical aspects of each edition, with a focused emphasis on the AI Document Management in the Enterprise Edition.



2. Why Celiveo 365?

In today's digital workplace, organizations face escalating challenges with document proliferation—generating over 10,000 documents daily in large enterprises, with data volumes growing 22% annually. Employees waste an average of 1.8 hours per day searching for information, leading to productivity losses exceeding $25,000 per employee yearly. Traditional print and document systems exacerbate these issues with insecure processes, high costs, and siloed data. Celiveo 365, developed by Celiveo—a global leader in high-security cloud solutions—addresses these pain points through a fully integrated, Azure-native platform.

Launched as an extension of Microsoft Universal Print, Celiveo 365 empowers the modern workplace by combining secure cloud printing with optional AI-driven document intelligence. It supports deployments of 10 to over 100,000 users, requiring no on-premises infrastructure, and delivers a serverless, driverless experience. The platform's two editions cater to varying needs: the Cloud Print Edition for foundational print management, and the Enterprise Edition for advanced AI capabilities that build a shared corporate knowledge base. This integration not only reduces printing and manual processing by 70% but also accelerates decision-making through instant, AI-powered insights.

3. The Business Case for Celiveo 365

Adopting Celiveo 365 yields transformative business outcomes, particularly for knowledge-intensive industries like finance, healthcare, and legal processing a lot of information and documents.
Key drivers include:

- **Cost Efficiency of Cloud Print and Scan Management**: Eliminates print servers and infrastructure, no more print driver, no more print agent on PC, cutting total cost of ownership (TCO) by up to 70%. Organizations can achieve break-even in a few months, with annual savings of up to $2 million for 1,000 users through suppression of print management IT infrastructure, reduced printing, toner/paper waste, and manual labor.
  Print TCO and ROI calculator: https://www.celiveo.com/printroi

- **Productivity Gains from AI-powered Document Management**: Automates corporate information searches and workflows, reclaiming 15 minutes to 2 hours per employee daily. This translates to over 450 hours saved annually per user, reducing interruptions (up to 275 daily) and enabling faster decisions with 50% quicker approvals. ROI calculators show 1,000%+ ROI in Year 1, driven by time savings, error reduction (90% in manual processes), and optimized Azure storage. For example, a 1,000-user deployment might turn a $182,000 investment into $3–4 million in returns.
  AI Document Management ROI Calculator: https://www.celiveo.com/roi

- **Compliance and Risk Mitigation**: Ensures adherence to GDPR, HIPAA, CCPA, and ISO 27001:2022, lowering compliance costs by 30% through AI-driven data loss prevention (DLP) with the highest accuracy in detecting sensitive information (PII and PHI).

- **Scalability, Agility**: Supports elastic growth for millions of documents daily, with one-day deployment and no IT training required. It adapts to your business and fosters collaboration via a shared knowledge base, improving team efficiency and employee satisfaction.

- **Environmental Impact**: Thanks to AI Document Management, reduces paper consumption by 70%, aligning with sustainability goals.

Pricing is subscription-based per active user/month, with flexible upgrades.

Organizations can start with Cloud Print and scale to Enterprise with AI-powered Document Management without disruption, decoupling from legacy systems for phased adoption.

4. AI Document Management, Building a Corporate Memory

Celiveo 365 AI Document Management: User-Driven, Zero-Trust Corporate Memory Built for Microsoft 365

Celiveo 365 Enterprise Edition redefines enterprise AI document management by placing the user firmly in control of what enters the corporate knowledge base — delivering a secure, cost-efficient, and hallucination-resistant solution that transforms how organizations capture, protect, and retrieve institutional intelligence.

At the heart of the system is an elegantly simple capture mechanism: any employee can decide, in real time, that a document, email, report, web page, or any on-screen content is worth preserving simply by pressing **Ctrl + P (Windows) / Command + P (macOS) or File > Print**. This instantly captures the information/document through Celiveo 365's cloud print queue, where it is intelligently processed and added to the organization's private AI knowledge base. No complex workflows, no additional software, no training required. The user becomes the active curator of corporate memory.

Uncompromising Security and Data Sovereignty

Every captured document and its associated AI embeddings are stored **exclusively inside the customer's own Microsoft 365 tenant**. Celiveo support and engineering teams have zero visibility or access to customer documents or knowledge. Each file is encrypted at rest using customer-managed keys stored in **Azure Key Vault** within the same tenant, ensuring that even in the unlikely event of a platform breach, data remains inaccessible to anyone outside the customer's organization. Information never leaves the tenant boundaries, is never shared with third parties, is never used to train external AI models, and never traverses public networks unprotected. This architecture achieves true data residency and sovereignty while maintaining full compliance with ISO 27001:2022, GDPR, HIPAA, SOC 2, and CCPA.

Instant, Verifiable Access Through the Celiveo 365 Teams Agent

Once captured, knowledge becomes immediately actionable. Every employee can open Microsoft Teams and simply ask questions in plain English — "What were the key terms of the Q4 deal with Acme Corp?", "Summarize the latest regulatory changes affecting our European projects", or "What were the main risks identified in the 2026 strategic review?" — and receive accurate, concise summaries or detailed reports powered by Azure AI. Crucially, every answer includes direct, one-click

links to the original source documents for immediate verification, eliminating the trust issues common with other generative AI systems. The knowledge base remains private, auditable, and fully under the customer's governance.

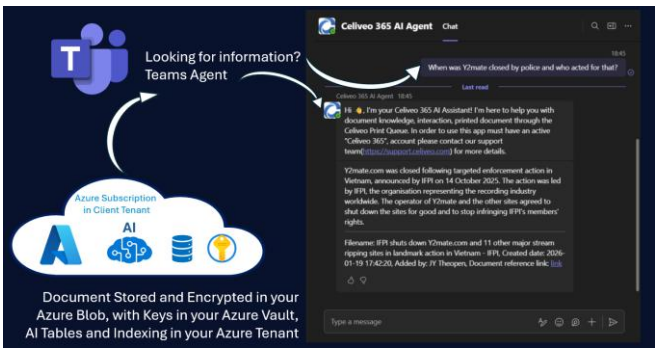
A Game-Changing, Cost-Effective Architecture

By leveraging the existing cloud print queue as the intelligent ingestion pipeline, Celiveo 365 introduces a fundamentally different philosophy: **only user-selected, high-value content is processed**. This delivers three powerful advantages:

- Dramatically lower costs — far fewer documents are sent to Azure AI compared to blanket scanning or auto-capture solutions.
- Significantly reduced hallucinations — the AI works exclusively on verified, business-critical material chosen by domain experts.
- True user empowerment — employees actively shape the corporate memory instead of passively feeding an indiscriminate system.

The combination of **Cloud Print Queue → Secure Azure AI Processing → Natural-Language Teams Interface** creates an intuitive, enterprise-ready "corporate brain" that is both more secure and more economical than traditional document AI platforms.





In an era where data volume grows exponentially while trust in AI remains fragile, Celiveo 365 stands apart by making security, user control, and cost efficiency non-negotiable foundations of intelligent document management. Organizations gain a living, breathing, verifiable knowledge repository — built by their own people, protected by Microsoft 365, and accessible in seconds — without the risks, complexity, or expense of conventional solutions.

Celiveo 365 AI Document Management is not just another AI tool. It is the secure, user-centric foundation for the modern intelligent enterprise.

5. High Security Cloud Print, low IT

The Cloud Print Edition serves as the foundational layer of Celiveo 365, focusing on secure, efficient cloud-based printing. It targets organizations seeking to modernize print infrastructure without advanced document intelligence. This edition can be upgraded seamlessly to Enterprise for added AI features.

The aim of the Celiveo 365 solution is to:

- Remove the whole print management infrastructure, remove print servers, move to Cloud
- Remove print-related applications and drivers from PC, to reduce IT workload and support
- Secure printers, MFPs access and documents printing throughout the company
- Provide Pull Print capability with full roaming, mobile print and print on home office printers
- Provide Direct IP Printing capability from Windows and mobile devices
- Allow users to secure-print easily from anywhere on PC and mobile devices
- Help to optimize the number of printers and copiers throughout the company
- Help end-users in their use of printers and copiers, to locate the most appropriate printer
- Inform users and management about print and copy usage and cost, as well as savings
- Provide accurate tracking information as $, CO^2 and tree-equivalence units

Business Aspects

From a business perspective, the Cloud Print Edition delivers immediate value by eliminating legacy print servers and drivers, reducing TCO by up to 50%. It supports cost control through usage tracking, bill-back, and print rules that curb waste, potentially halving print volumes.
A complete TCO calculator is available for you at https://www.celiveo.com/printroi

Key advantages include:
Operational Savings: No charges for Cloud traffic or storage (beyond Azure and Universal Print credits), with predictable per-user pricing. Home office and mobile printing enhance remote work, while Power BI reporting enables data-driven decisions for cost recovery.
Risk Reduction: Military-grade security prevents data breaches, with compliance readiness for sensitive industries. Offline resilience applied to advanced smart printers and MFP ensures business continuity during outages.
Flexibility and Growth: Scalable for diverse environments (Windows, macOS, iOS, Android, Chromebook), it supports BYOD policies with total security backed by Entra-ID. ROI is amplified by quick setup—eliminating servers in days—and an upgrade path to AI capabilities without migration.

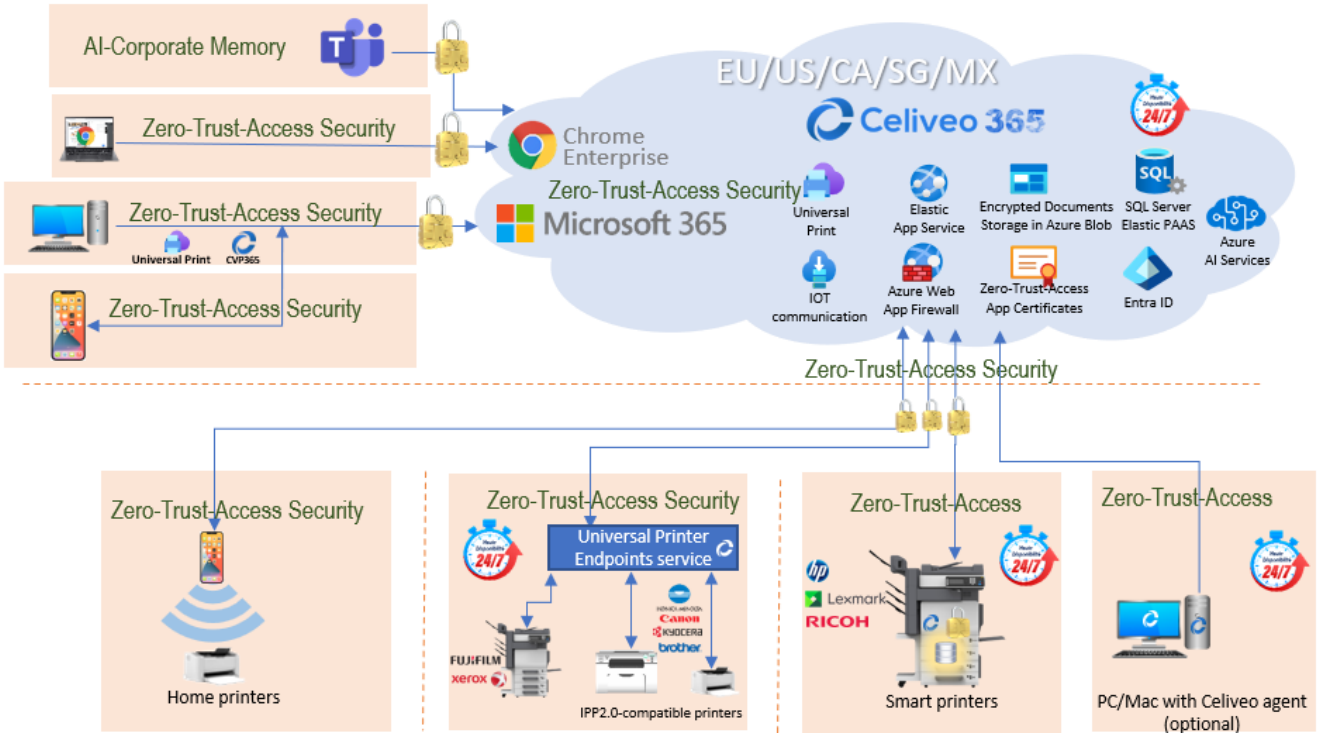
For mid-sized firms, this edition provides a low-entry barrier to cloud printing, with potential savings of millions annually through centralized management and analytics.

Technical Aspects

Technically, the Cloud Print Edition is a pure SaaS solution on Azure PaaS, extending Microsoft Universal Print with enterprise-grade features. It requires no VMs, OS, or gateways, no inbound endpoints, relying on direct client PC or mobile to Cloud and direct Smart printer-to-Azure connectivity.

Architecture

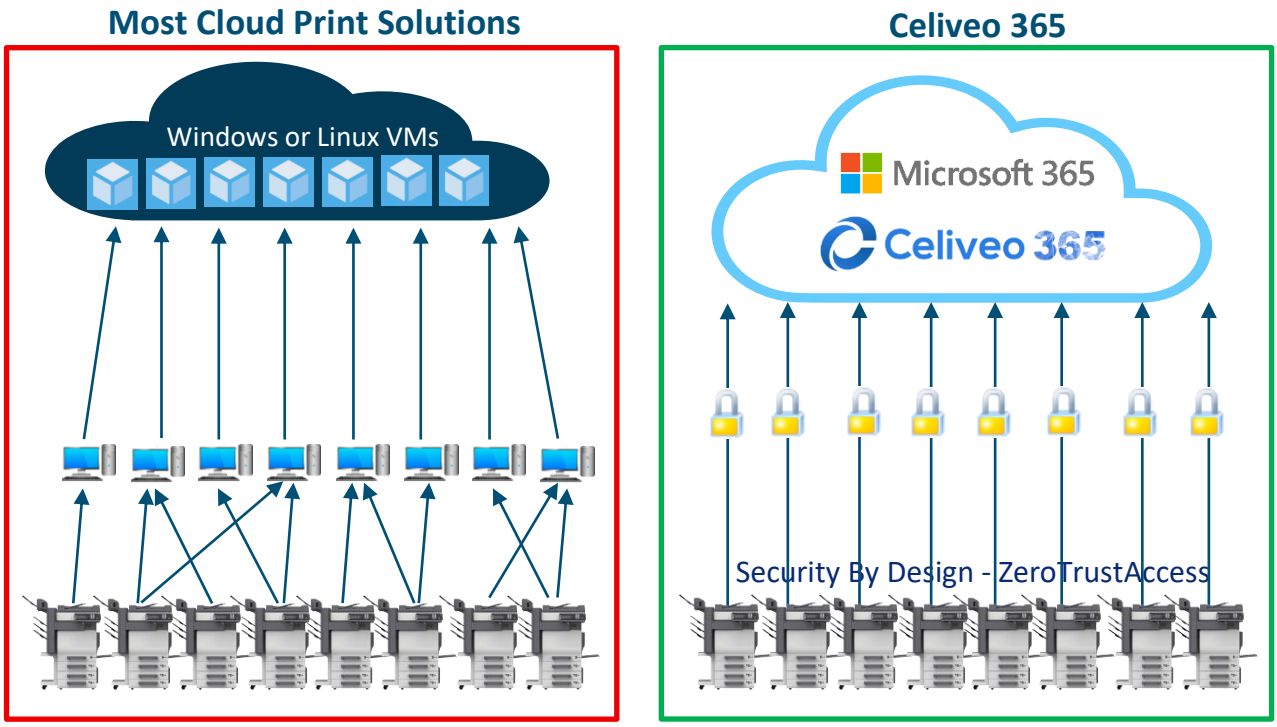
Serverless and agentless core, with optional printer-embedded agents for advanced resilience. Data flows securely from devices to Azure, with auto-discovery of printers and unified portal management. It inherits Azure's 99.75% SLA, geo-redundancy, High Availability, and elastic horizontal scaling to adapt dynamically to the workload.



Unlike other solutions, Celiveo 365 Cloud Print is not a print management solution in a VM running in the Cloud.

It is a true SaaS on PaaS, using APIs and elastic resources to adapt to volume, not require any OS update or reboot, not rely on a particular computer, and be automatically updated.
With no VM there is no black box representing a serious risk for clients.

Cloud Pull Print architecture, from the smart printers' view:



Smart printers accept the Celiveo 365 embedded agent, running security, Pull Print, data decryption and many other tasks from inside the printer. Not all printers allow that level of security and simplicity. Printers with embedded Celiveo agent connect directly and safely to Internet.

Directly: the Celiveo 365 agent installed on the smart printer communicates directly with the SaaS.

Safely: all connections to the Cloud are performed using true certificate-based Zero-Trust-Access.

- Celiveo 365 is immune to servers Operating System and solution updates
  - Most other solutions are affected by application server reboots/updates in the Cloud
- Celiveo 365 does not require any local print server or client on PC to print
- No Master-Slave server system, no complex architecture prone to downtime
- No more SQL Server to license, manage, maintain, cluster, backup, upgrade

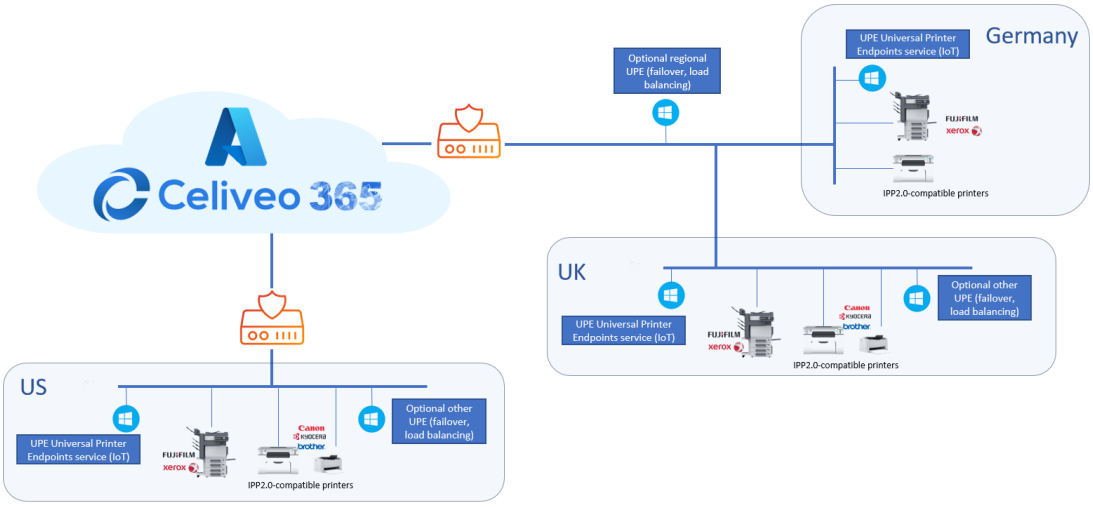
Support for printers not supporting the Celiveo 365 Embedded Agent

The Celiveo 365 UPE (Universal Printer Endpoint) is a lightweight, cyber-secure IoT service (an edge component) for Windows 11/Server and legacy Windows 10 that extends the capabilities of Celiveo 365 for printers that do not natively support embedded Celiveo 365 agents. It enables organizations to achieve enterprise-grade secure cloud Pull Print and management across mixed printer fleets—especially older or non-smart devices—while maintaining full integration with Microsoft Universal Print and the broader Celiveo 365 ecosystem (including Cloud Print and Enterprise Editions). This helps eliminate legacy infrastructure, reduce costs, and enforce Zero-Trust-Access security without limiting compatibility.

The UPE acts as an IoT agent pulling and decrypting documents from the cloud-based Celiveo 365 platform (which leverages Microsoft Universal Print), sending pages to legacy or agentless network printers/MFPs on the local network. It enables secure Pull Print (follow-me printing), documents release, tracking, and related features in environments where the printer itself cannot directly communicate with the cloud service, or does not provide the level or security expected from a printer facing the Internet.

Advanced features:

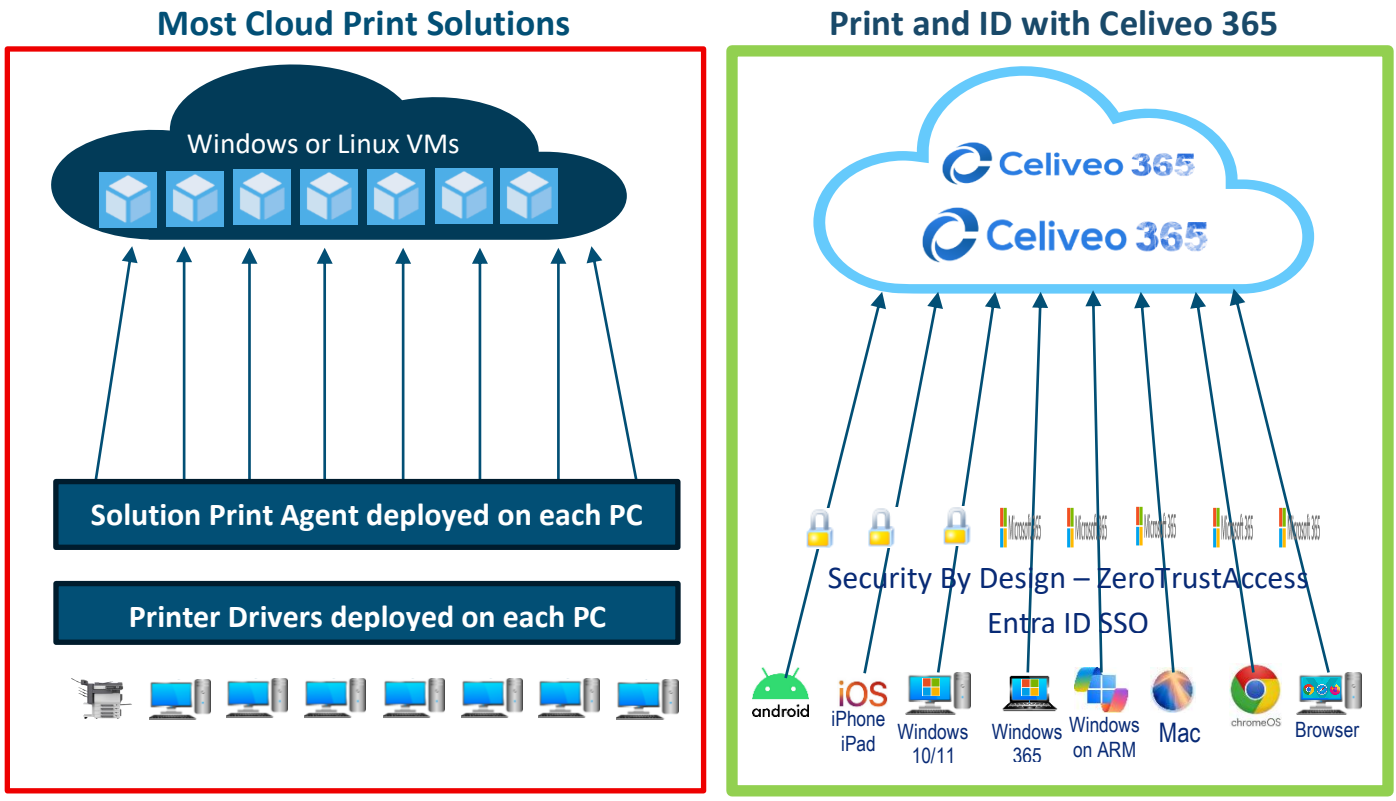
- Support of up to 500 printers being simultaneously served by one UPE
- No need to create/manage print queues, no print driver
- Monitors printer status: Checks reachability, availability, errors, and other telemetry, reflected in the Celiveo 365 portal for user and administrators
- Advanced IPPS/IPP/9100 print channels support
- Automatic Failover and Load Balancing
- Zero-Trust-Access communication with Certificate-chain and mutual TLS Auth



Example of UPE IoT service deployed for local load balancing and regional failover

Cloud Pull Print architecture, from the PC or mobile's view:

There is no need to install any driver or print agent on client Windows PC or mobile devices



2.1.1 Printing on Windows using Universal Print Queues or WinCVP 365

On Windows 11/365 and legacy Windows 10, Celiveo 365 utilizes native deep integration with Microsoft Universal Print to provide a seamless, agent-free printing experience. It is also possible to create a Celiveo 365 Virtual Printer agent for Windows (WinCVP 365) for extra security and native driver deployment and usage.

The process begins with queue deployment and proceeds through document submission to release.

1. **Cloud Print Queue creation**

    1. **Microsoft Universal Print Queue Setup and Deployment**: Administrators create one or more Universal Print queues directly in the Celiveo 365 Web Admin portal, no need to use the Azure portal. These shared queues are then produced inside Universal Print and can be deployed to client PCs manually or using tools like Microsoft Endpoint Manager (Intune). Users can manually add the cloud printer in Windows Settings by navigating to "Printers & scanners," selecting "Add device," and choosing the work or school-associated cloud printer (identified by a special icon with a cloud). Installation typically completes in 20-30 seconds, with no driver required.

2. **Celiveo WinCVP 365 Advanced Printer Agent Setup and Deployment**: Administrators can create one or more WinCVP 365 agents directly in the Celiveo 365 Web Admin portal. WinCVP 365 delivers the following services:

    1. Documents retention on the client PC, for sites with weak Internet connection
    2. Local printer driver usage, when special document output enhancement featured by the vendor printer driver is needed
    3. Automatic printer driver deployment and configuration
    4. Very fast spooling to Celiveo 365
    5. Direct IP printing where print job is sent instantly to a local network printer, no retention, as a failover to Cloud Pull Print during Internet outages.

    The agent includes a high security Certificates Chain authenticating the connection and linking it to the specific tenant and siloed APIs. It can be deployed to client PCs manually or using tools. The Cloud printer is installed automatically and activated as default printer. The WinCVP 365 self-updates and updates its drivers and settings when admins decide to deploy new versions.

2. **Document Submission**: it differs between the Universal Print and the WinCVP 365.

    1. **Universal Print**: From any Windows application, users select the Universal Print queue as the printer. The document is spooled locally and securely transmitted to Universal Print in the cloud, where Celiveo 365, invoked by Universal Print, encrypts and holds it. This driverless process ensures compatibility with Windows Protected Print (WPP) standards, and documents are visible in the Windows print spooler during transmission.
    2. **WinCVP 365**: From any Windows application, users select the default printer and can configure the driver setting if needed. Documents are spooled locally, securely encrypted and transmitted instantly to Celiveo 365 in the cloud, where they are stored, or encrypted and transmitted to the printer when direct IP printing is activated.

3. **Document Release**: At the printer, users authenticate using a PIN, ID code, contactless card, or NFC-enabled mobile device configured in Celiveo 365's authentication profiles. Once authenticated, they select and release the document from the printer's interface or via a mobile, with real time data decryption in the printer. This pull-print mechanism ensures documents are only printed when the user is physically present, enhancing security and reducing unauthorized access.

This workflow is ideal for enterprise environments, also supporting features like usage tracking and rules-based printing without local infrastructure.

Printing on macOS with Universal Print Queues

Celiveo 365 extends Universal Print support to macOS through the Microsoft Universal Print agent or the macOS Celiveo Virtual Printer 365 (macCVP 365), enabling vendor-specific printing with secure cloud integration. The process emphasizes compatibility and security via Microsoft Entra ID SSO.

1. **Print Queue Setup and Installation**:
   It is possible to use either the Microsoft Universal Print App or the macCVP 365 on the Mac, each has its own benefits.

   - **Microsoft Universal Print App**: Administrators install the Universal Print App for MacOS on the Mac. Users open the App and then need to sign in using a Microsoft Entra ID account. No driver is required to print, the user selects a Universal Print Cloud printer in the printer list and is ready to print. The drawback is the limited number of printer features that are supported during printing.

   - **Celiveo macCVP 365 App**: Administrators create a MacOS print queue in the Celiveo 365 portal, and download the macCVP 365 App package that includes the Zero-Trust-Access certificate chain (used for mutual TLS connection to endpoints) and displays briefly the Certificate security pass key needed for the package installation. On the Mac, users install that macCVP 365 App, which automatically creates a print queue that uses the default macOS PostScript (PS) driver or a manufacturer-specific driver for advanced features (e.g., stapling, or duplex printing). Microsoft Enterprise SSO is configured for Entra ID login, allowing single sign-on without repeated credentials entry. No additional agents are needed beyond the virtual printer setup. The App features automatic updates so that the latest App is always used, and very fast spooling. Spooled documents have a 50MB size limit.

2. **Document Submission**: From macOS applications, users print to the Microsoft Universal Print App or to the macCVP 365 print queue based on what App was installed. Documents are spooled securely to Celiveo 365 in the cloud. The system supports complex documents and ensures no local servers are involved.

3. **Document Release**: Authentication at the printer uses PIN, card, or mobile NFC. Users release documents via the printer's screen or a NFC mobile, pulling them from the secure cloud document retention and decrypting them in the printer after downloading with dual encryption and mutual TLS communication between secure endpoints. This ensures secure, on-demand printing compatible with the highest security requirements.

With both agents, Microsoft Universal Print App for Mac and the Celiveo macCVP 365 for Mac, macOS users benefit from full cloud queue support, making it suitable for distributed teams requiring vendor-agnostic printing.

Printing on Mobile Devices with Universal Print Queues

For iOS and Android, Celiveo 365 facilitates mobile printing through its WebApp, native App and web portal, for secure, location-agnostic printing. This supports bring-your-own-device (BYOD) scenarios without requiring device enrollment in Intune.

1. **Using the Celiveo 365 WebApp for Edge, Chrome browser**: Users connect to my.cvo365.com from their iOS or Android mobile. The WebApp works exactly like an app, without requiring any local installation and authenticates via Entra ID SSO, restricting access to authorized groups.

2. **Using the Celiveo 365 App for iOS and Android**: Users download the Celiveo Mobile Print app from the App Store (iOS) or Google Play (Android). The app authenticates via Entra ID SSO, restricting access to authorized groups. The main difference with the WebApp is the ability to print documents using the "Share With" function of iOS and Android.

3. **Using a web browser**: Alternatively, printing can occur via a web browser on any mobile or computer, accessing the Celiveo 365 Print Portal with Entra ID SSO

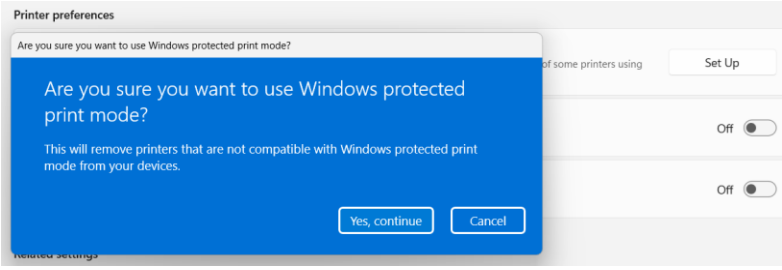
4. **Document Submission**: From the mobile device, users can select documents to push for printing (Microsoft 365, OpenOffice and PDF files), upload happens in a few seconds. Documents are sent to the Celiveo 365 who handles encryption and secure storage. No local print drivers or agents are needed, enabling printing from anywhere over public internet with Zero-Trust-Access security.

5. **Documents review and push print**: Users can review pending documents on their mobile, display them, delete them.

6. **Document Release**: At the printer, users authenticate using NFC tap, PIN, or card. The app lists available documents, allowing release on any Celiveo 365-controlled printer within the tenant. This pull-print functionality ensures documents remain secure until the user is present. Users can even push documents to a remote printer, i.e. for a colleague, from their mobile.
   Mobile printing with Celiveo 365 is particularly advantageous for remote workers, offering flexibility without compromising security or requiring complex VPN setups.

Microsoft Windows Protected Print (WPP): A New Standard for Secure Printing

Microsoft's new **Windows Protected Print (WPP)** architecture represents a fundamental shift in how printing is secured and managed in Windows environments. As WPP becomes mandatory in modern Windows versions, traditional printer drivers and legacy print components—including third-party port monitors—are increasingly restricted because they operate with elevated (SYSTEM/root) privileges and introduce significant security risk. This change effectively eliminates the long-standing model where print solution agents, custom port monitors, and locally installed drivers interact deeply with the Windows print spooler. Under WPP, only secure, standards-based, driverless printing models aligned with Microsoft's architecture are supported.



The impact for organizations is substantial: legacy print agents and server-based print infrastructures are no longer aligned with Microsoft's security direction. Solutions that depend on locally installed drivers, custom spooler extensions, or print server middleware face increasing compatibility and compliance challenges.

Celiveo 365 is fully aligned with the Windows Protected Print model because it relies entirely on **Microsoft Azure Universal Print architecture**. It does not require proprietary print drivers, local print agents, custom port monitors, or on premises print servers. Printing occurs through secure, cloud-native Universal Print queues integrated with Entra ID and Azure services, fully respecting Microsoft's protected printing framework.

This architectural alignment delivers multiple benefits: improved print reliability and quality through standardized rendering, elimination of driver packaging and compatibility testing, removal of print server deployment and maintenance, and the end of client-side print agent management. IT teams no longer need to test, deploy, patch, or support printer drivers or print server applications.
The result is dramatically simplified IT operations, reduced infrastructure costs, and a significantly strengthened security posture—fully consistent with Microsoft's Zero-Trust and modern Windows security strategy.

Printers and MFP support

The features available on a printer or MFP depend on the device brand, model and firmware. On most models all the features are available: User authentication, Pull Print, rules-based printing and tracking with full integration on the printer screen. On models where integration on the printer screen isn't possible, the user authentication with instant Pull Print and tracking are always available through the IoT Universal Printer Endpoint service running on a Windows Server/VM.

Celiveo 365 supports printers in **two distinct ways**, providing different levels of integration, user experience, and security.



Printers Supported by Celiveo 365 Embedded Agent

These printers run the **Celiveo 365 Embedded Agent** directly inside the device. This is the **best and most secure** mode because:

- The embedded agent speaks **directly** to Celiveo 365 in Azure (outbound only on port 443).
- Full **on-screen integration** (documents list, release, delete, color/B&W/duplex selection/rules).
- Full **MFP walk-up control** (copy, scan, email, fax) via Entra ID / card / PIN / NFC mobile.
- **Direct scan** to OneDrive/Sharepoint, no service in between, on selected printer models.
- Native card reader support + NFC.
- Full **usage tracking** (print, copy, scan, email, fax…)
- True **Zero-Trust-Access** (no intermediary servers, ECC-P256 certificates, no credentials).

Supported Brands & Series (Celiveo Embedded Agent alone and Agent + UPE IoT service):

- **Fujifilm** → Selected models (primarily production and high-end office MFPs), at least one UPE IoT service on the network, addressing the printer, is needed
- **HP** → FutureSmart 4, FutureSmart 5
- **Xerox-Lexmark** → eSF Framework 5, 6, and 7 (most modern Xerox-Lexmark MFPs and printers)
- **Ricoh** → SOP 2.5 and SOP 3.x
- **Xerox VersaLink and AltaLink** → ConnectKey platform, at least one UPE IoT service on the network is needed, addressing the printer from the Cloud in full security

These represent the "premium" integration tier.

Printers WITHOUT Embedded Agent → Supported via Celiveo UPE IoT Agent

These printers **cannot** run the embedded agent but are still fully supported for **secure cloud Pull Print** using the **Celiveo Universal Printer Endpoint (UPE)** without user interface on the printer screen or card reader.

How it works:

- The UPE is a very lightweight Windows service (IoT-based) installed on a Windows 10/11 PC, VM, or server on a network that can access printers using TCP-IP on ports 9100 (raw print) and/or 631 (IPP) and UDP port 161 and UDP port 162 (SNMP).
- It acts as a secure IoT agent that:
    - Only uses outgoing connection to Azure IoT servers
    - Uses Zero-Trust-Access with Certificate chain-based mutual TLS authentication
    - Pulls encrypted documents from Celiveo 365 Azure via outbound-only port 443
    - Decrypts and delivers the documents locally to the printer
    - Controls the print and printer status, report them to Celiveo 365 for PowerBI reports
    - Sanitizes all internet access for the printer.
- User authentication/release is done via mobile NFC tap on the printer (no app needed, works with any Entra ID + NFC-enabled phone). Documents list appears on the phone screen for selection and can be previewed before release.

- No card reader or on-screen documents list on the printer itself, to work seamlessly with any printer.
- Full Zero-Trust-Access security is maintained (printer itself never talks to the internet, mutual TLS authentication using positive certificate chains).

Supported Printers in this mode:

- Any network printer that fully supports IPP 2.0 (including IPP Everywhere).
- This covers ~98–99.8% of all modern network office printers.
- Works with virtually all brands: Brother, Canon, Epson, Konica Minolta, Kyocera, Sharp, Samsung, older or entry-level HP/Xerox-Lexmark/Ricoh/Xerox, Ricoh, OKI, Dell, etc.

One UPE instance can typically handle up to 500 simultaneous print requests. Multiple UPEs can be deployed for scale, load balancing, or geographic isolation using tags.

Wi-Fi printers, AirPrint, Mopria → Supported via mobile

These printers are typically found when users work from home or very small offices. Those printers cannot run the embedded agent but are still fully supported for secure cloud push print using the user mobile.

Release is easy and secure:

- On their mobile (iOS or Android), users browse to my.cvo365.com
- This portal requires Entra ID SSO strong authentication, usually with MFA
- Users can list and preview pending documents, post extra documents to print
- Documents can be selected and pushed to Wifi printing
- Selected documents are decrypted, previewed
- A print icon allows to call the OS-native print feature (AirPrint, Mopria, Android)
- Celiveo 365 tracks the Wi-Fi print request of those documents, for traceability/accountability
- There is no need for any local IT infrastructure, just an accessible printer that supports AirPrint or Mopria print protocols (99.9% of printers sold today)

Quick Recommendation Guide

- **Use Embedded Agent** (preferred) → HP FutureSmart, Xerox-Lexmark eSF, Ricoh SOP 2.5/3.x, Xerox VersaLink/AltaLink, Fujifilm.
- **Use UPE IoT Agent** → Everything else (Brother, Canon, Kyocera, Sharp, older models, entry-level devices not accepting embedded agents, etc.).
- **Use Mobile Wi-Fi Print** → for all Wi-Fi home and home office printers that are AirPrint and Mopria/Android compatible.

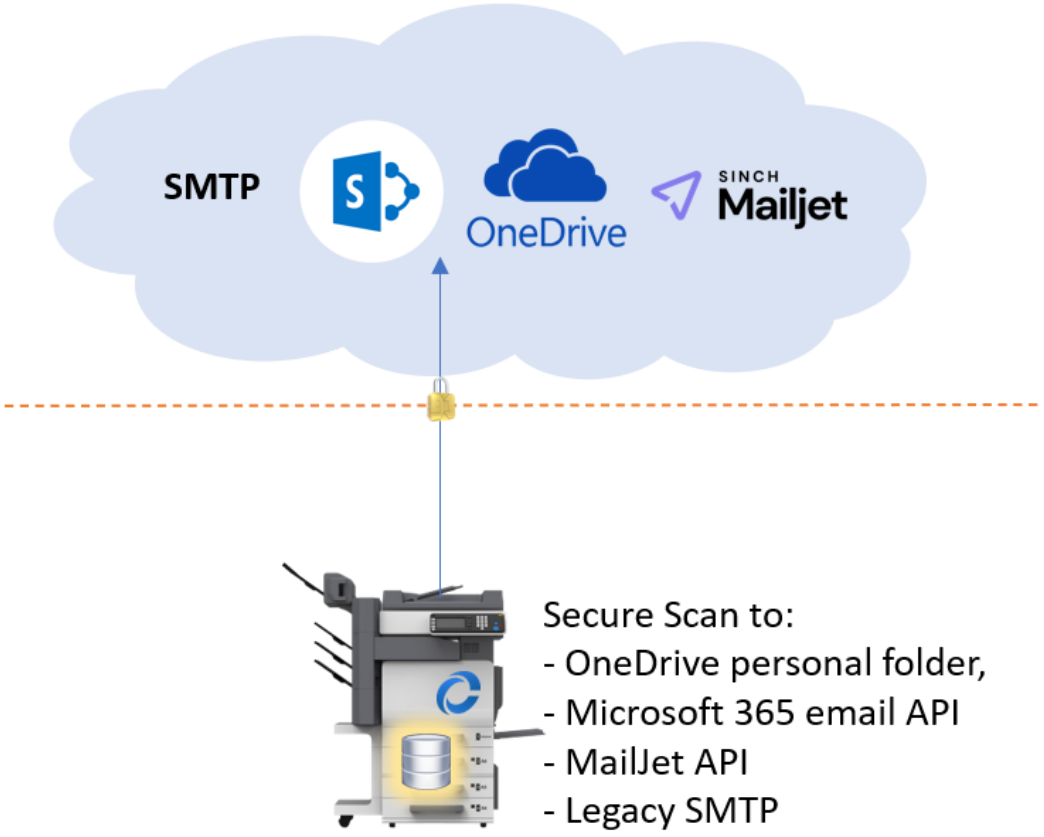
Printer type	User authentication	Pull Print	Secure Scan	Rules based	Copy/Scan control	Print tracking	Copy/Scan tracking	Integration on printer	Embedded/ UPE/Mobile
Canon	NFC, QRCode	Yes	No	Yes	No	Yes	No	No	UPE Service
Epson	NFC, QRCode	Yes	No	Yes	No	Yes	No	No	UPE Service
FujiFilm	Card, PIN, NFC	Yes	No	Yes	Yes	Yes	Yes	Yes	Embedded
HP LaserJet	Card, PIN, NFC	Yes	Yes*	Yes	Yes	Yes	Yes	Yes	Embedded
Konica Minolta	NFC, QRCode	Yes	No	Yes	No	Yes	No	No	UPE Service
Kyocera	NFC, QRCode	Yes	No	Yes	No	Yes	No	No	UPE Service
Xerox-Lexmark (eSDK)	Card, PIN, NFC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Embedded
Ricoh (SOP 2.5, 3.x)	Card, PIN, NFC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Embedded
Sharp	NFC, QRCode	Yes	No	Yes	No	Yes	No	No	UPE Service
Toshiba	NFC, QRCode	Yes	No	Yes	No	Yes	No	No	UPE Service
Xerox (EIP)	Card, PIN, NFC	Yes	No	Yes	Yes	Yes	Yes	Yes	UPE Service
Other network	NFC, QRCode	Yes	No	Yes	No	Yes	No	No	UPE Service
AirPrint / Mopria	Entra ID SSO	Push	No	No	No	Yes	No	No	Mobile

*: requires the activation of the hp WorkPath functionality on the printer

Please refer to the www.celiveo.com web site for the exact list of supported printers/MFPs, the table above is a simplified table, and exceptions may exist for some brands or models.

6. Secure Scan to email, OneDrive

Celiveo 365 introduces a transformative approach to secure document scanning from multifunction printers (MFPs) directly into the Microsoft 365 ecosystem, prioritizing **Zero-Trust-Access** principles, end-to-end encryption, and elimination of intermediary services to minimize data exposure risks. Unlike traditional or competing solutions that often route scanned documents through third-party servers, portals, or relays—where read/write access tokens may be stored and potentially accessible to external administrators—Celiveo 365 is engineered **secure by design**, ensuring security tokens never leave the authenticated user's control and documents flow peer-to-peer from the MFP to the destination without middlemen.



Key scan-to-cloud capabilities include:

- **Direct Scan to OneDrive**: Scanned documents are uploaded straight to the user's OneDrive for Business within their own Microsoft 365 tenant, leveraging **Entra ID SSO** for authentication via badge, PIN, or other supported methods. No intermediary service handles the file, preventing any opportunity for data leaks or unauthorized interception. This feature is available on Xerox-Lexmark eSF MFPs, Ricoh SOP 2.5 and 3.0 MFPs, and HP FutureSmart 4 and 5 MFPs with Workpath license.

- **Direct Scan to Email via Microsoft 365**: Utilizing modern authentication and Entra ID SSO—no reliance on legacy SMTP protocols—documents are sent securely as email attachments directly through Microsoft 365 infrastructure. This eliminates vulnerabilities associated with SMTP relays while maintaining seamless integration. Availability mirrors the above: Xerox-Lexmark eSF MFPs, Ricoh SOP 2.5 and 3.0 MFPs, and HP FutureSmart 4 and 5 MFPs with Workpath license.
- **Legacy SMTP Support**: As a backward-compatible fallback, direct scan-to-email via traditional SMTP is provided for environments not yet fully modernized, with the same rollout timeline as the advanced options. Availability mirrors the above: Xerox-Lexmark eSF MFPs, Ricoh SOP 2.5 and 3.0 MFPs, and HP FutureSmart 4 and 5 MFPs with Workpath license.

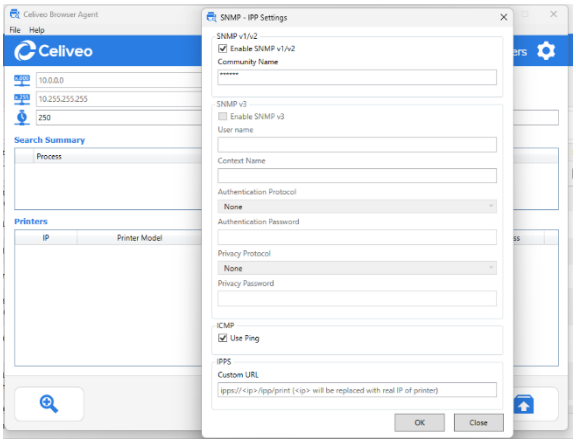
All scan workflows benefit from intuitive, user-centric enhancements: a document preview and validation step prior to transmission ensures accuracy and compliance, while a unified, friendly interface consolidates options—allowing effortless switching between email and OneDrive destinations on a single screen. Optional integrated **AI-Driven Data Loss Prevention (AI-DLP)** further scans content in real time for sensitive information (PII, PHI, financial data), blocking or alerting on potential leaks before sending.

By avoiding SAML-based web portals or token-relay mechanisms common in other solutions—which introduce risks through stored access tokens on cloud VMs—Celiveo 365 upholds strict least-privilege access and true peer-to-peer flows. This architecture dramatically reduces the attack surface, aligns with ISO 27001:2022, GDPR, HIPAA, and other standards, and empowers organizations to digitize paper workflows with confidence in high-security, compliance-driven environments. As adoption grows across Xerox-Lexmark, Ricoh, and HP platforms throughout 2026, Celiveo 365 sets a new benchmark for secure, cloud-native scanning in the modern workplace.

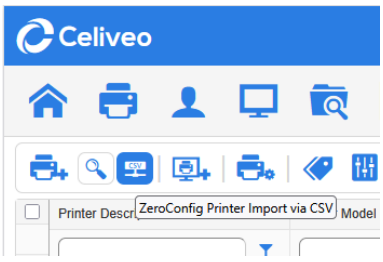
7. Easy and fast printer onboarding

Celiveo 365 revolutionizes printer onboarding by enabling organizations to integrate large printer fleets into a secure, cloud-native Universal Print environment in minutes rather than days or weeks—delivering a process that is secure, simple, slick, and exceptionally fast, with the capability to onboard up to 5,000 printers in as little as 30 minutes.

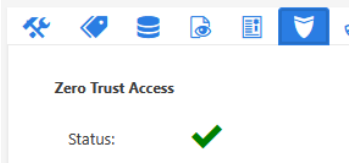
Unlike traditional solutions that require enrolling printers directly in Microsoft Universal Print, registering them in Intune or any MDM system, or installing manually embedded agents/software, Celiveo 365 handles discovery and configuration entirely through its intuitive Azure Web Admin console, bypassing these steps for true agentless simplicity on the administrative side.



Onboarding begins with powerful automated discovery using SNMP (v1/v2/v3) queries combined with ICMP ping and IPP/IPPS checks, performed via the lightweight Celiveo 365 Admin Browser Agent (a browser-based tool). Administrators initiate a network scan to automatically detect supported printers (such as HP FutureSmart, Xerox-Lexmark eSF, Ricoh SOP, Xerox ConnectKey, and many IPP 2.0-capable models), pulling key details like model, serial number, and capabilities in bulk. No need to register printers in InTune or any MDM.



For even faster or targeted deployments—especially with known IP lists— Celiveo 365 enables administrators to import hundreds or thousands of printers at once via CSV files through the Web Admin portal, streamlining large-scale fleet onboarding. Once imported, a powerful ZeroConfig Printer cloning feature accelerates configuration: define a master printer with all desired settings (authentication profiles, print rules, geotags, access controls, embedded agent parameters, floor map placement, etc.), then apply these settings identically to the entire batch or selected devices in a single operation, ensuring consistency across the fleet without manual repetition.



Security remains paramount throughout this rapid process. For printers that support the Celiveo 365 Embedded Agent (on compatible models), the system automatically generates and deploys a certificate chain based on ECC-P256 cryptography during synchronization. This establishes mutual TLS authentication (mTLS) between each printer, the cloud

services, and other nodes, enforcing true Zero-Trust-Access—no passwords, no shared secrets, and verification of identity before any communication occurs.

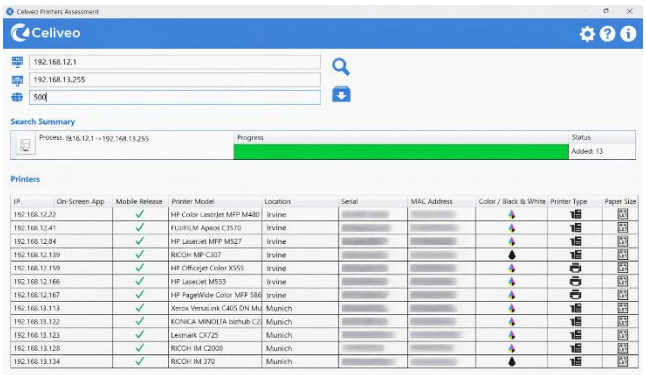
All outbound connections use TLS 1.3 over port 443, with no inbound ports required, further minimizing exposure. For non-embedded printers, the lightweight Universal Printer Endpoint (UPE) IoT service provides equivalent secure bridging without compromising the Zero-Trust-Access model.

This combination of SNMP auto-discovery, CSV batch import with master cloning, and automated certificate-based mTLS delivers unmatched onboarding speed and scale while eliminating dependencies on Intune, MDM enrollment, or direct Universal Print printer registration.

Organizations achieve enterprise-grade secure Pull Print deployment rapidly, with full fleet visibility, consistent policies, and robust security from the first printer onward—making Celiveo 365 the ideal choice for modern, agile print management in Microsoft-centric environments.

Printer Discovery & Assessment Utility: Enabling Risk-Free Cloud Migration

A successful transition to secure cloud printing begins with full visibility of the existing printer fleet. In many organizations, printer inventories are outdated, incomplete, or lack critical information about device capabilities and security posture. The Celiveo 365 Printer Assessment Utility eliminates this uncertainty by providing automated network discovery and detailed compatibility analysis. By scanning defined IP ranges, the tool identifies all printers on the network, evaluates their ability to securely connect to the cloud, and determines whether they support embedded Celiveo applications or require alternative deployment methods such as the Universal Printer Endpoint (UPE).



This assessment delivers immediate business value: it reduces migration risk, prevents unexpected hardware limitations, accelerates project planning, and enables accurate budgeting for upgrades or replacements. IT teams gain a clear, data-driven roadmap for cloud print adoption—knowing exactly which devices can support secure pull printing, advanced authentication, and Zero-Trust connectivity. For partners and enterprises alike, the utility transforms what is often a complex and uncertain discovery phase into a fast, structured, and reliable foundation for a successful Celiveo 365 deployment.

8. Flexible and Secure User Authentication

Celiveo 365 offers a versatile array of authentication methods to ensure secure, Zero-Trust-Access-compliant release of documents at printers and through mobile devices, all tightly integrated with Microsoft Entra ID for seamless single sign-on and granular access control.

At the physical printer or multifunction printer (MFP), users can authenticate using PIN codes (automatically generated and self-managed via a secure portal, with 4-12 character ID codes emailed upon first use), contactless cards or badges (via supported card readers on compatible models like Xerox-Lexmark, Xerox AltaLink/VersaLink, Fujifilm, Ricoh or HP). Supported card readers include Elatec TWN4, most RFIdeas and HID Omnikey with keyboard emulation. Celiveo 365 dual factor technology allows users to define a PIN that will be required during card authentication, for a higher security.

For printers without embedded agents, users can also use their NFC-enabled mobile/tablet (iOS or Android—no app required) providing contactless authentication and automatic documents list popup. The user's NFC phone acts as a secure remote interface displaying documents and confirming release after Entra ID SSO authentication.

For mobile-specific release, Celiveo 365 provides dedicated options via the Celiveo Mobile Print app (available on iOS and Android) or the secure web-based Print Portal. Users authenticate once with Entra ID SSO (optionally restricted to specific groups), then access pending documents from anywhere.

Release can occur through the app's push print menu (triggering documents printing on a selected or nearest printer), NFC tap at the printer (for seamless proximity release without manual entry), or in some configurations, QR code scanning linked to the mobile device although NFC is strongly recommended for its security and anti-forgery.

These methods ensure documents remain encrypted in the cloud until the authenticated user—verified via multi-factor-capable Entra ID—initiates release, preventing unauthorized access while supporting BYOD flexibility, high availability (to make copies and send faxes during connectivity interruptions on supported devices), and compliance with enterprise security standards. This multi-modal approach empowers organizations to balance convenience, security, and user choice across diverse printer fleets and work environments.

Secure Guest Printing with Customer-Controlled Identity

Enterprise-Grade Guest Printing Without Guest Identity Data in Celiveo 365

Welcoming external visitors, contractors, consultants and business partners should not mean weakening enterprise print security or creating another repository of personal information. Celiveo 365 extends secure cloud printing to authorized guests with guest identity management remaining under the customer's control using the enterprise identity governance.

Customer-Owned Guest Identity and Privacy by Design

A fundamental architectural difference from many guest-printing solutions is the separation of identity ownership from print management. Guest invitations, identity information, authentication and lifecycle management reside under the customer's guest identity management, not in a guest-identity directory maintained by Celiveo. Celiveo has no access to the guest's identity details and does not hold guest personally identifiable information (PII). The customer retains control of the guest identity, including its security policies and access lifecycle.

This reduces the spread of personal information into third-party print systems and helps organizations apply their existing privacy, identity and compliance governance to visitors as well as employees. Guest access is not an anonymous, unmanaged exception: it is an explicitly authorized identity-based workflow controlled by the customer.

Delegated Invitations: Entra ID-Backed Celiveo RBAC

The authority to invite a guest is defined through Celiveo 365 role-based access control (RBAC), backed by Microsoft Entra ID. Organizations decide which employees or administrators receive guest-invitation privileges, rather than allowing unrestricted invitation creation. This enables least-privilege delegation: an authorized host can invite a visitor while the organization retains centralized governance of who is permitted to extend guest printing access.

Guests Invited Directly from myCeliveo in Microsoft Teams

Authorized inviters use the myCeliveo application inside Microsoft Teams to invite guests. The invitation experience is therefore available within the collaboration workspace employees already use, benefiting from Teams' centralized application management and security controls. There is no need to introduce a separate public guest-registration system or to give every employee administrative access to Celiveo 365.

Guest Printing Experience

Once invited and authorized through the customer's guest access process, the visitor can print through Celiveo 365 mobile webapp and web portal as described in the user documentation. Guest printing is provided as an enterprise-controlled service, rather than bypassing authentication or relying on a shared visitor account. The organization's Microsoft identity policies remain the foundation for access decisions, while Celiveo 365 supplies the secure printing experience.

Security and Governance Benefits

- No Celiveo guest-identity directory: guest identities and their PII are managed under the customer's control.
- No Celiveo access to guest identity details: the customer retains identity ownership and governance.
- Controlled delegation: only users granted the appropriate Celiveo RBAC permissions, backed by Entra ID, can invite guests.
- Managed invitation channel: invitations are issued using myCeliveo in Microsoft Teams, under the organization's Teams administration and security framework.
- One enterprise identity policy: guest access can be governed through the customer's Microsoft identity and access controls rather than parallel, less-governed visitor accounts.

In short, Celiveo 365 makes secure printing available to visitors without making Celiveo the custodian of their identity. The customer manages guest identities; Celiveo RBAC determines who may invite them; and myCeliveo in Microsoft Teams provides an easy, centrally managed invitation experience.

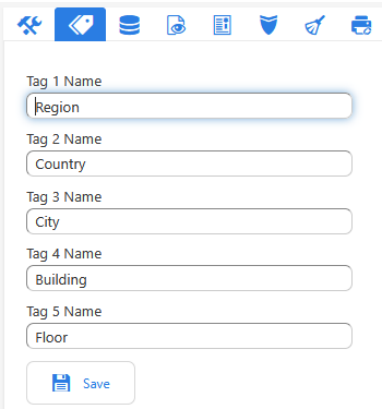
Further Information

End-user instructions: https://manual.celiveo365.com/currentrelease/en/topic/printing-as-a-guest-user

Administrator instructions: https://manual.celiveo365.com/currentrelease/en/topic/guest-users-management

9. Empowering Location-Based Print Management and Security with Geotagging

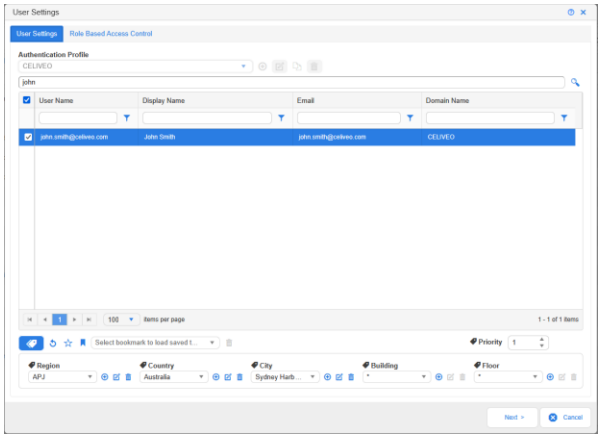
In an era of distributed workforces and global operations, effective print management requires more than just basic access controls—it demands intelligent, location-aware governance to ensure security, efficiency, and user productivity.



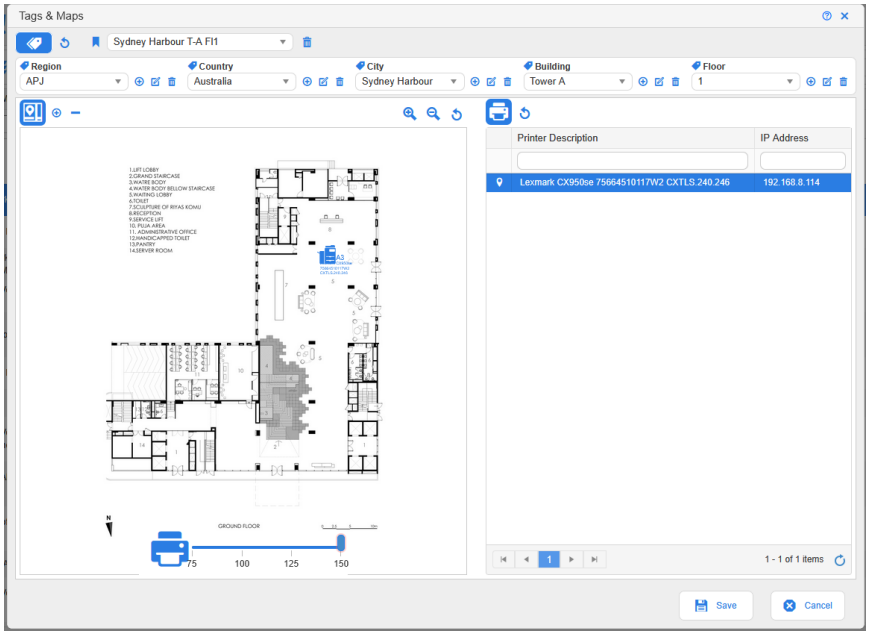
Celiveo 365 features a sophisticated geotagging system that assigns hierarchical location-based tags to printers, administrators, and users. This feature leverages up to five customizable tag categories (e.g., Country, Region, City, Building, Floor) to create "communities" or scoped groups, enabling granular control over print resources without on-premises infrastructure.

By integrating seamlessly with Microsoft Entra ID for automatic allocation to groups and users, these tags facilitate Zero-Trust-Access principles, where access and visibility are dynamically restricted based on contextual attributes like user location or organizational role. This not only streamlines

administration but also enhances compliance by preventing unauthorized interactions with printers outside designated scopes.

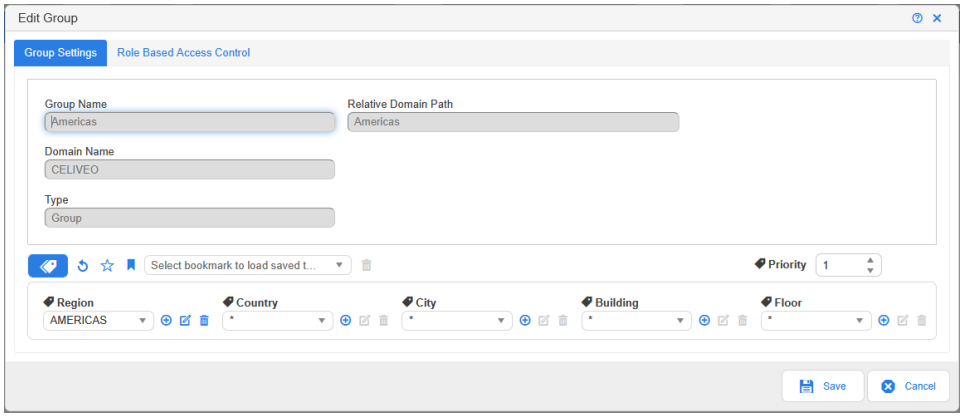


For local administrators, geotags provide a powerful mechanism to limit the scope of manageable printers and rules, promoting delegated administration while maintaining central oversight. Administrators are tagged similarly to users and printers, restricting their view in the Celiveo 365 Web Admin portal to only those devices and policies within their assigned communities.

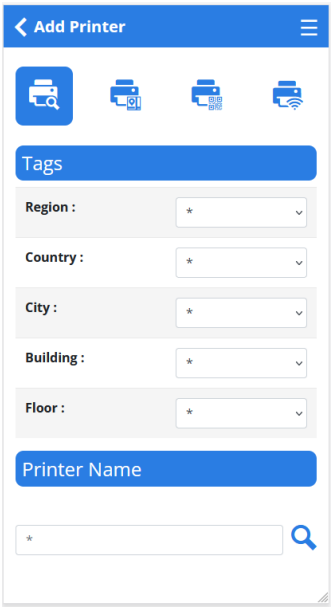


For instance, a regional admin tagged with "USA, California, San Francisco" can only configure queues, rules, and settings for printers in that city, preventing accidental or malicious changes to resources in other locations like "USA, New York." This hierarchical structure supports supersets—e.g., a state-level admin tagged "USA, California, *, *, *" oversees all California sites—ensuring scalability for large enterprises. The benefits are manifold: reduced administrative errors, enhanced security through least-privilege access, and simplified compliance audits, as actions are inherently logged and confined to geotagged boundaries.

End-users also benefit from geotag-driven restrictions, which limit the scope of accessible printers to those matching their location profile, thereby enforcing secure and relevant printing options.



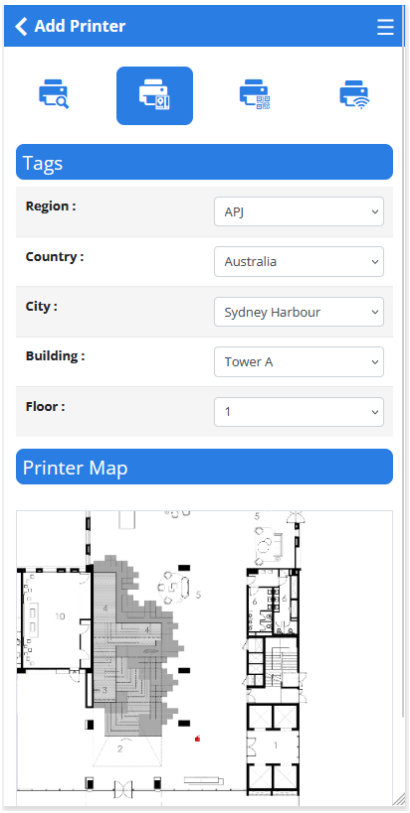
One of the most innovative applications of geotags is enabling users to automatically discover printers matching specific specifications within their building or site. Through the Celiveo 365 portal or mobile app, users can query for printers based on tag-filtered criteria, such as color capability, duplex support, or high-volume handling, confined to their geotagged community.



For example, a user in "Asia, Singapore, Headquarters, Floor 5" can search for "color MFPs" and receive a list of nearby devices that meet the specs, with real-time status updates on availability or toner levels.

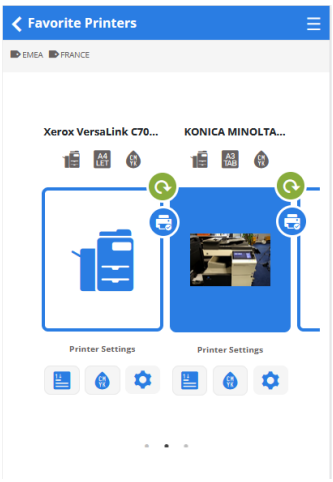
This dynamic discovery leverages SNMP for printer detection and Azure's cloud scalability, ensuring rapid responses even in large fleets. The benefits include boosted productivity, reduced downtime from mismatched printers, and environmental gains by directing documents to optimal devices, ultimately cutting waste and energy consumption in distributed offices.

Geotags further enhance usability by allowing printers to be positioned on interactive floor maps, making it effortless for users to locate available printers and multifunction printers (MFPs). Administrators upload floor plans to the Web Admin portal and place printer icons on floors, tagged with location details for accurate rendering.



Users access these maps via the Celiveo 365 web interface, desktop tools, or mobile/tablet app, where they can zoom, search, and navigate to find the nearest device. This visual aid is particularly valuable in large buildings or campuses, reducing time spent wandering and improving the overall user experience. Integrated with real-time data, maps display printer status (e.g., online, jammed), properties, and even walking directions, fostering a more intuitive and efficient print ecosystem.

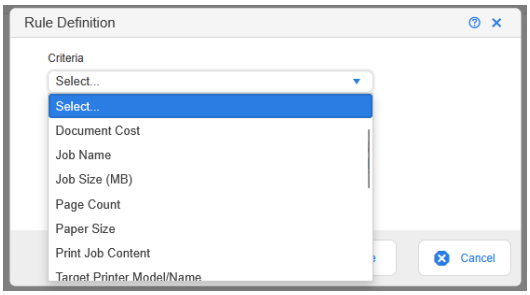
Finally, Celiveo 365's geotagging extends to visual identification by associating on-site photos with printers, available to all users for quick recognition. Administrators can upload photos of the physical printer during setup, which are then displayed alongside map positions, queue details, or search results. This feature helps users confirm the correct device—especially in environments with similar models—by showing real-world images, including surrounding landmarks or room numbers. Tied to geotags, these photos ensure context-specific visibility, enhancing accessibility for new employees or visitors. The overarching advantage is a more human-centered approach to print management, where security and convenience converge to support modern workplaces, all powered by Celiveo's seamless Azure integration.



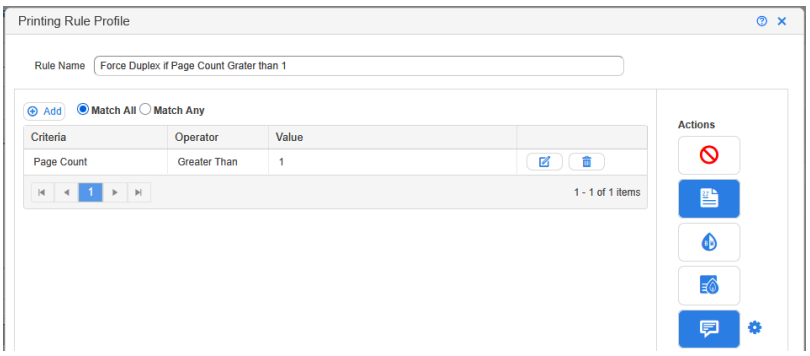
10. Print rules

Print rules in Celiveo 365 are centralized within the intuitive Web-Admin portal, allowing for easy configuration and management of Universal Print queues.

Administrators can create rules based on various criteria, such as document size (e.g., preventing the printing of documents exceeding 300 pages on smaller printers), color versus black-and-white output, duplex requirements, time, day, Entra ID group, printer characteristics, or even user-specific quotas to curb waste and control costs.



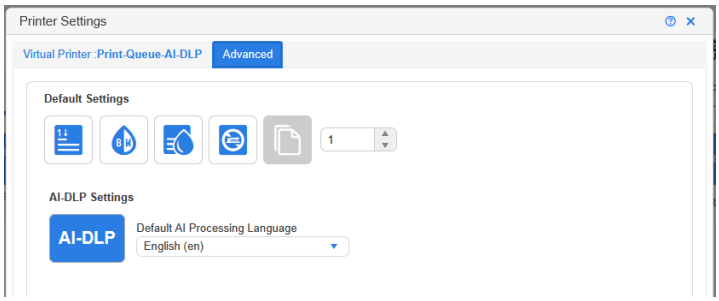
The benefits of Celiveo 365's print rules extend far beyond basic access control, offering organizations a powerful toolset to enforce print policies with minimal effort. By controlling who can print what—such as restricting color printing to marketing teams or blocking sensitive financial documents for non-finance users—administrators reduce printing volumes by up to 50%, lowering costs and environmental impact. AI-DLP enhances compliance by preventing data leaks at the source, minimizing risks of breaches and regulatory fines while maintaining transparency through detailed notifications and Power BI reporting (read below).



This granular enforcement fosters a culture of accountability, where policies are automatically applied based on user roles, document content, and context, all within a Zero-Trust-Access framework that encrypts workflows and limits access to need-to-know basis. Ultimately, these capabilities simplify policy management, eliminate manual oversight, and integrate printing into broader enterprise security strategies, making Celiveo 365 an essential solution for modern, secure print governance.

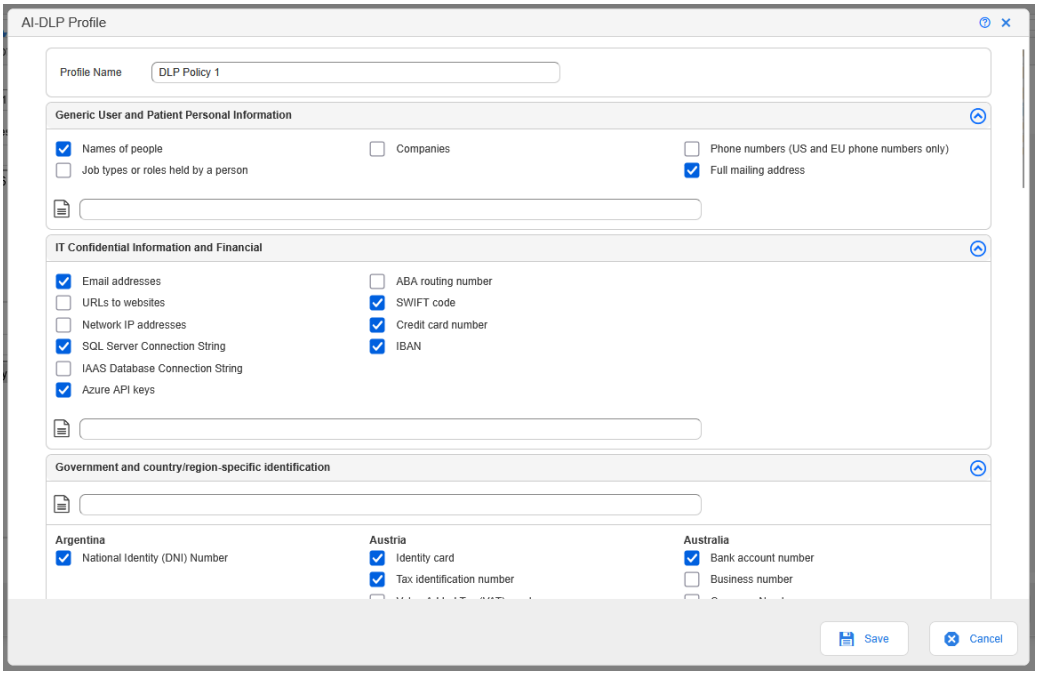
11. AI-DLP

In today's hybrid work environments, where data security and operational efficiency are paramount, organizations face increasing challenges in managing print workflows. Uncontrolled printing can lead to data breaches, excessive costs, and non-compliance with regulations such as GDPR and HIPAA.

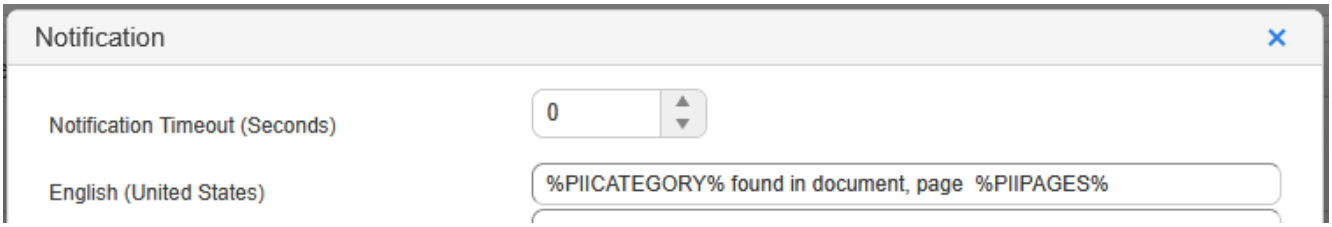


Celiveo 365 addresses these issues through its robust print rules capabilities. These features enable administrators to define granular policies that dictate who can print what, under what conditions, and with what restrictions, all without the need for on-premises infrastructure. By integrating seamlessly with Microsoft Entra ID and leveraging Azure's scalability and security, Celiveo 365 transforms printing from a potential vulnerability into a controlled, secure process that Zero-Trust-Access principles.

A standout feature is the integration of AI-Driven Data Loss Prevention (AI-DLP), which employs natural language processing (NLP) and machine learning to scan documents in real-time for sensitive content. Categories for detection include Personal Identifiable Information (PII) like names, addresses, and phone numbers; financial data such as credit card numbers and IBAN codes; government IDs including social security numbers and passports; and health-related information (PHI). Rules can be set to flag, block, or notify users about documents containing such data, with customizable whitelists to minimize false positives. This setup ensures that print policies are not only reactive but proactive, embedding security directly into the workflow.



The implementation of print rules is streamlined and user-friendly, requiring no additional hardware or software agents. To set up a rule, administrators select a Universal Print queue in the portal, navigate to the Access & Rules section, and define printing rules by adding criteria such as AI-DLP profiles. For instance, a profile might specify detection, with actions like blocking documents that trigger PII alerts or notifying the user via the printer panel or mobile with details on the flagged content (e.g., "%PIICATEGORY% on pages %PIIPAGES%").



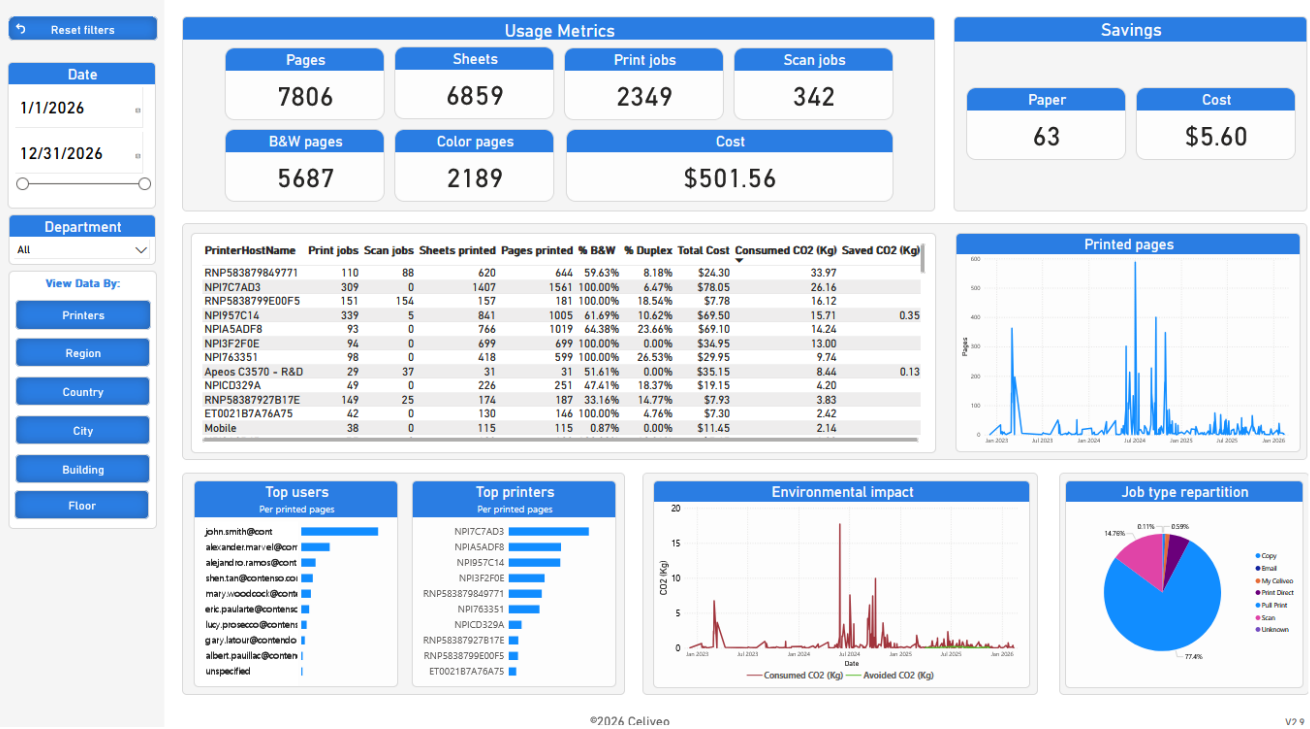
Integration with Microsoft Entra ID allows rules to be tied to user groups or organizational units, ensuring that policies align with existing identity management.

This cloud-based approach supports high availability, with rules enforced even during outages through edge computing on supported printers, and scales effortlessly across global fleets without performance degradation.

12. Advanced Printer Tracking and Reporting by Power BI

Celiveo 365 delivers enterprise-grade tracking and reporting that provides complete, real-time visibility into every aspect of printing activity across the organization. The platform automatically logs all key events, including document submissions and releases, printer panel interactions, print usage, MFP walk-up usage (copy, scan, fax) on printers with embedded Celiveo 365 agent.

Going beyond basic logs, Celiveo 365 integrates natively with Microsoft Power BI to transform raw tracking data into powerful, customizable dashboards and reports.



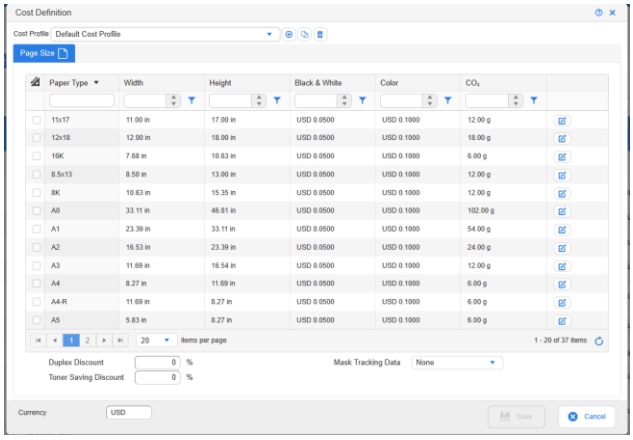
Organizations benefit from an interactive dashboard showing:

- Top users and printers
- Color vs. black-and-white usage trends
- Cost allocation by department, user, or project
- Green IT metrics (pages saved, CO^2 reduction through duplex/default rules)
- Compliance and audit trails with privacy-masked user identities for GDPR/HIPAA compliance
- Printer utilization and documents volume heatmaps

Cost is defined per printer, for each paper format and supports discount for duplex and B&W print.

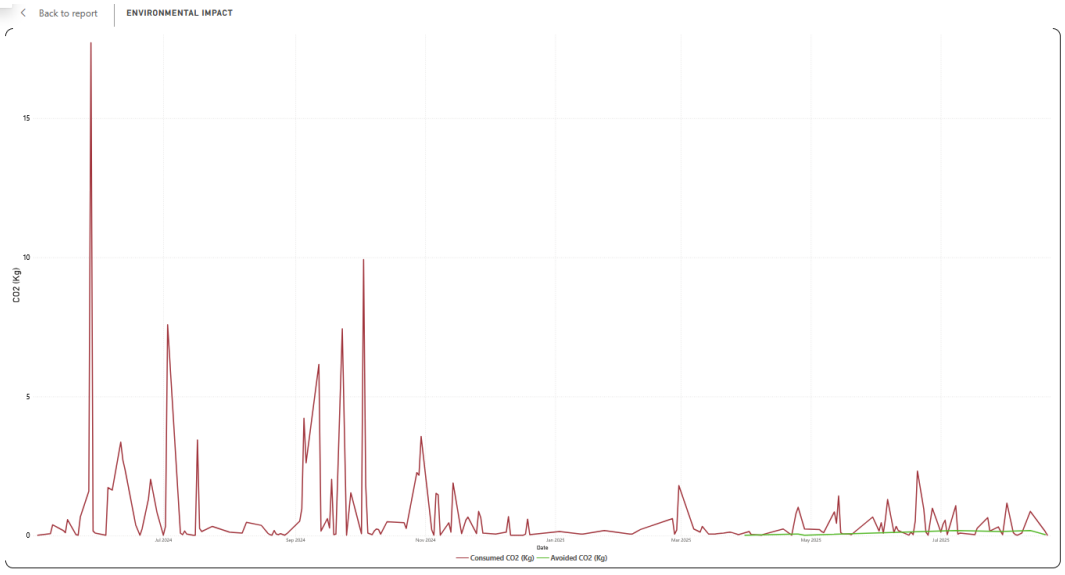
It is also possible de define a CO^2 impact for each paper format.

A currency can be applied to a cost profile, when managing a multi-country fleet where print usage is billed in the local currency.

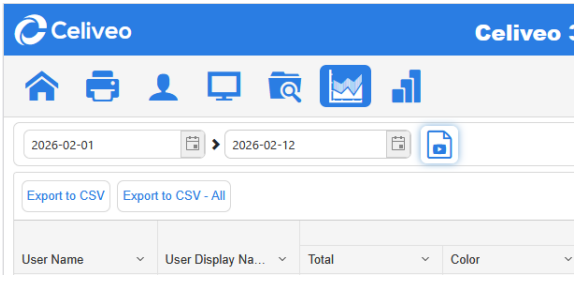


Power BI reports can be shared securely across the organization, embedded in internal portals, or scheduled for automated distribution.

This combination of granular tracking and Power BI analytics enables organizations to optimize print costs, enforce policies, demonstrate regulatory compliance, and support sustainability initiatives—all from a single cloud-native platform with no additional infrastructure required. The result is actionable intelligence that drives efficiency, accountability, and continuous improvement in modern Microsoft-centric print environments.



Data can be exported in standard formats (CSV, PDF, Excel) while maintaining full auditability.



13. Subscription

Subscribing to Celiveo 365 through the Microsoft Azure Marketplace provides organizations with a seamless, streamlined procurement process that integrates directly with existing Microsoft 365 and Azure ecosystems.

To begin:

1. Navigate to the Celiveo 365 listing on the Azure Marketplace (search for "Celiveo 365" or access it via the direct link at marketplace.microsoft.com).
2. Authenticate using a Microsoft Entra ID account with the necessary administrative privileges, such as the ability to consent to app permissions and manage subscriptions within the tenant.
3. Review and accept the required permissions for Celiveo 365 to link securely to your Microsoft 365 tenant, then select the preferred datacenter region (e.g., Europe/France, United States, Mexico, Canada or Singapore) for data residency compliance.
4. Choose the appropriate plan—such as the Evaluation Edition for a 30-day free trial or a paid tier like the Cloud Print or Enterprise edition, priced per monthly active user with flexible, scalable floating licenses.
5. Complete the subscription by confirming billing details (via Azure consumption billing, or through a Microsoft Cloud Solution Provider for invoicing alignment), after which the service provisions automatically.
6. Post-subscription, you receive and email indicating how to access your dedicated Celiveo 365 administration portal to manage users, configure Universal Print queues, and deploy features.

This Azure-native SaaS model ensures rapid onboarding—often within minutes—eliminates infrastructure overhead, and aligns billing with Microsoft's predictable per-user pricing, enabling enterprises to extend Universal Print with advanced secure Pull Print, authentication, and AI-driven document management while maintaining full governance and compliance within the Microsoft cloud.

14. Celiveo 365 Web Admin Console

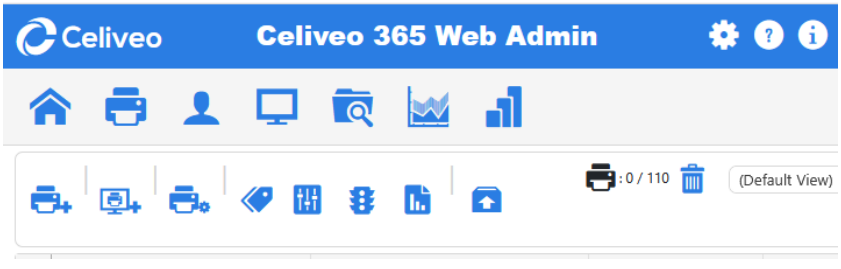
The Azure-based Celiveo 365 Web Admin Console serves as a unified, intuitive single-pane-of-glass interface that consolidates every aspect of print management, eliminating the need for multiple tools, on-premises servers, or fragmented dashboards.

Accessible via secure browser login with Microsoft Entra ID single sign-on, the console centralizes administration for Universal Print queues, printer fleets, security policies, mobile workflows, and comprehensive reporting—delivering simplicity, efficiency, and full visibility in a Zero-Trust-Access environment.

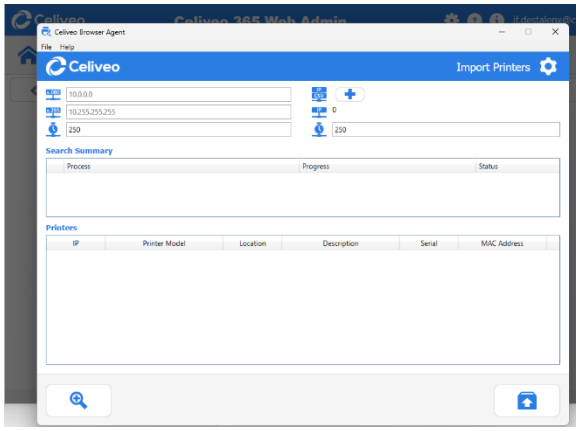


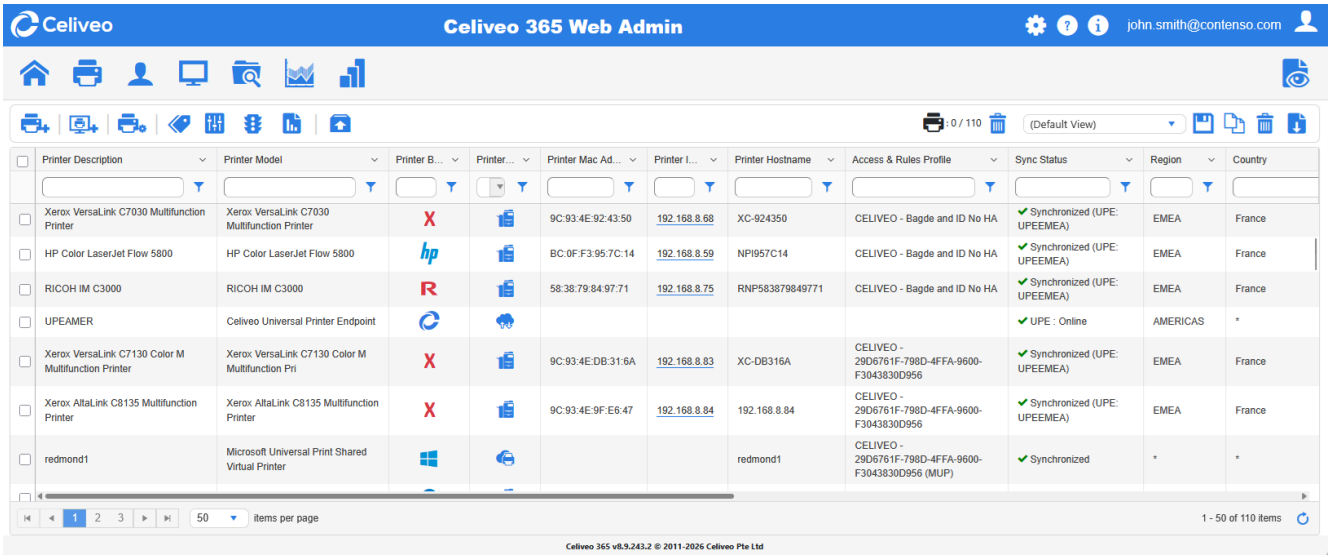


Administrators can rapidly create and configure Universal Print queues directly within the portal. By selecting printers, defining queue names, applying authentication profiles, and deploying via Microsoft Universal Print, queues are shared tenant-wide in minutes. Geotagging and access rules ensure scoped visibility and control from day one.



Printer fleet management is equally streamlined. The console supports quick bulk import via SNMP auto-discovery, CSV upload, or manual addition, automatically detecting supported models (HP FutureSmart, Xerox-Lexmark eSF, Ricoh SOP, Xerox ConnectKey, etc.) and assigning the appropriate Celiveo 365 Embedded Agent or Universal Printer Endpoint (UPE IoT). Fleet-wide operations—such as firmware status monitoring, geotag assignment (Country/Region/Building/Floor), floor map positioning, photo uploads, and agent configuration—are handled centrally, with real-time health indicators and bulk actions for thousands of devices.

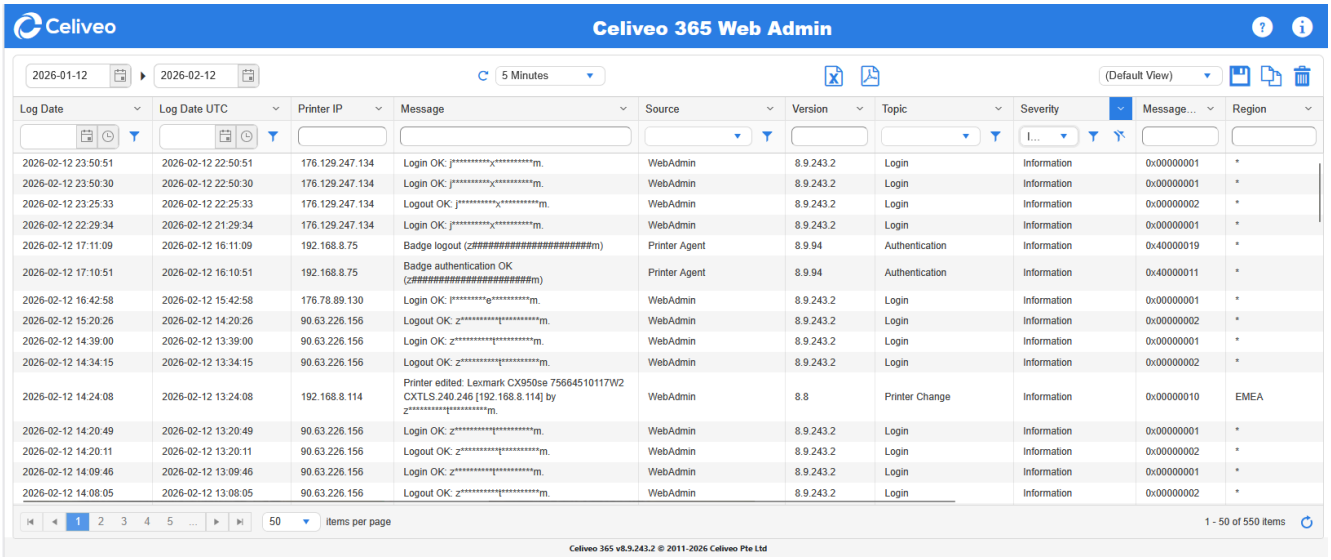




Security and policy configuration are fully integrated. Administrators define print rules (color/B&W restrictions, page limits, quotas, duplex enforcement) and AI-Driven Data Loss Prevention (AI-DLP) profiles that scan documents for PII, PHI, or financial data, with block/notify actions.

Authentication methods (PIN, contactless card, NFC mobile/tablet, Entra ID) are configured per queue or globally, while mobile print settings enable the Celiveo Mobile Print app, web portal, and push/NFC release workflows.

Finally, the console provides powerful tracking and reporting capabilities. Detailed logs capture every event—document submissions, releases, authentications, admin actions, and MFP walk-up usage—displayed in searchable grids or exported for compliance. Integrated Power BI dashboards offer customizable usage reports, cost analysis, Green IT metrics, and audit trails, with privacy masking for GDPR/HIPAA compliance.



By bringing queue creation, fleet management, agent configuration, print rules, mobile print, and advanced analytics under one roof, the Celiveo 365 Web Admin Console simplifies operations, accelerates deployment, strengthens governance, and scales effortlessly—making it the ideal control center for organizations leveraging Microsoft Universal Print in modern, secure, cloud-first environments.

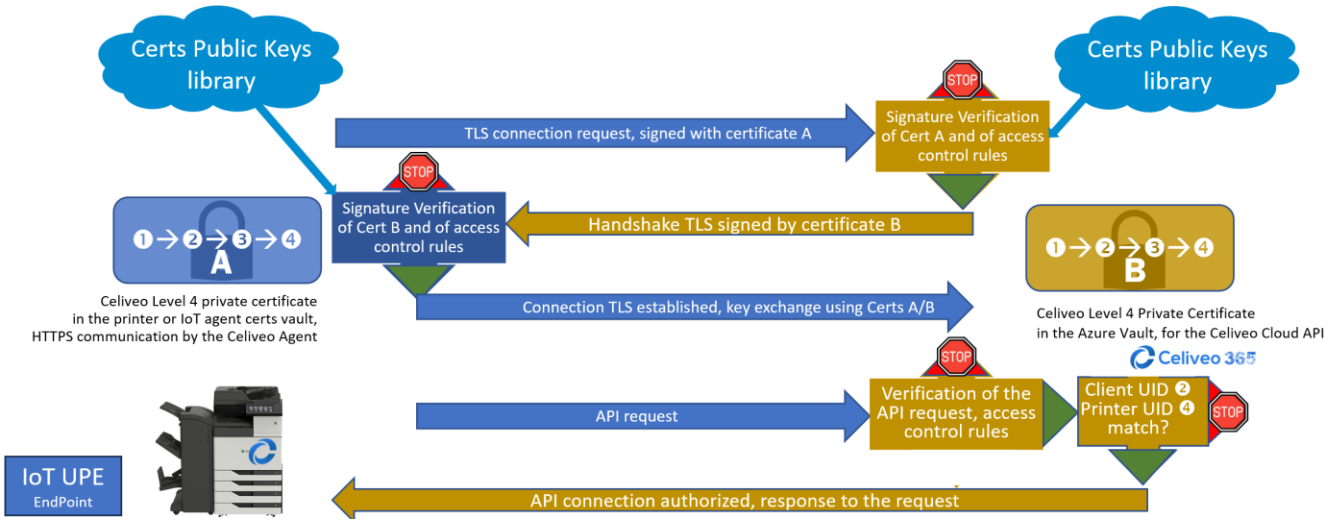
15. Ports, protocols and flows

Celiveo 365, as a fully cloud-native SaaS extension to Microsoft Universal Print hosted on Azure, is engineered with a strong emphasis on security, simplicity, and Zero-Trust-Access principles.

One of its standout architectural advantages is an exceptionally lean network profile: all communications rely exclusively on outbound HTTPS traffic over port 443, with no inbound ports required to be opened on corporate firewalls. This design eliminates the need for inbound rules, VPN tunnels, or exposed endpoints, significantly reducing the attack surface compared to traditional print management solutions that often demand multiple open ports or local servers.

Whether for embedded agents running directly on supported printers (such as Fujifilm, HP FutureSmart, Xerox-Lexmark eSF, Ricoh SOP, or Xerox ConnectKey models), the lightweight Universal Printer Endpoint (UPE) IoT service on Windows, administrator web access, or client document submissions via WinCVP 365, every connection initiates outbound-only from the on-premises environment to Celiveo 365 cloud services.

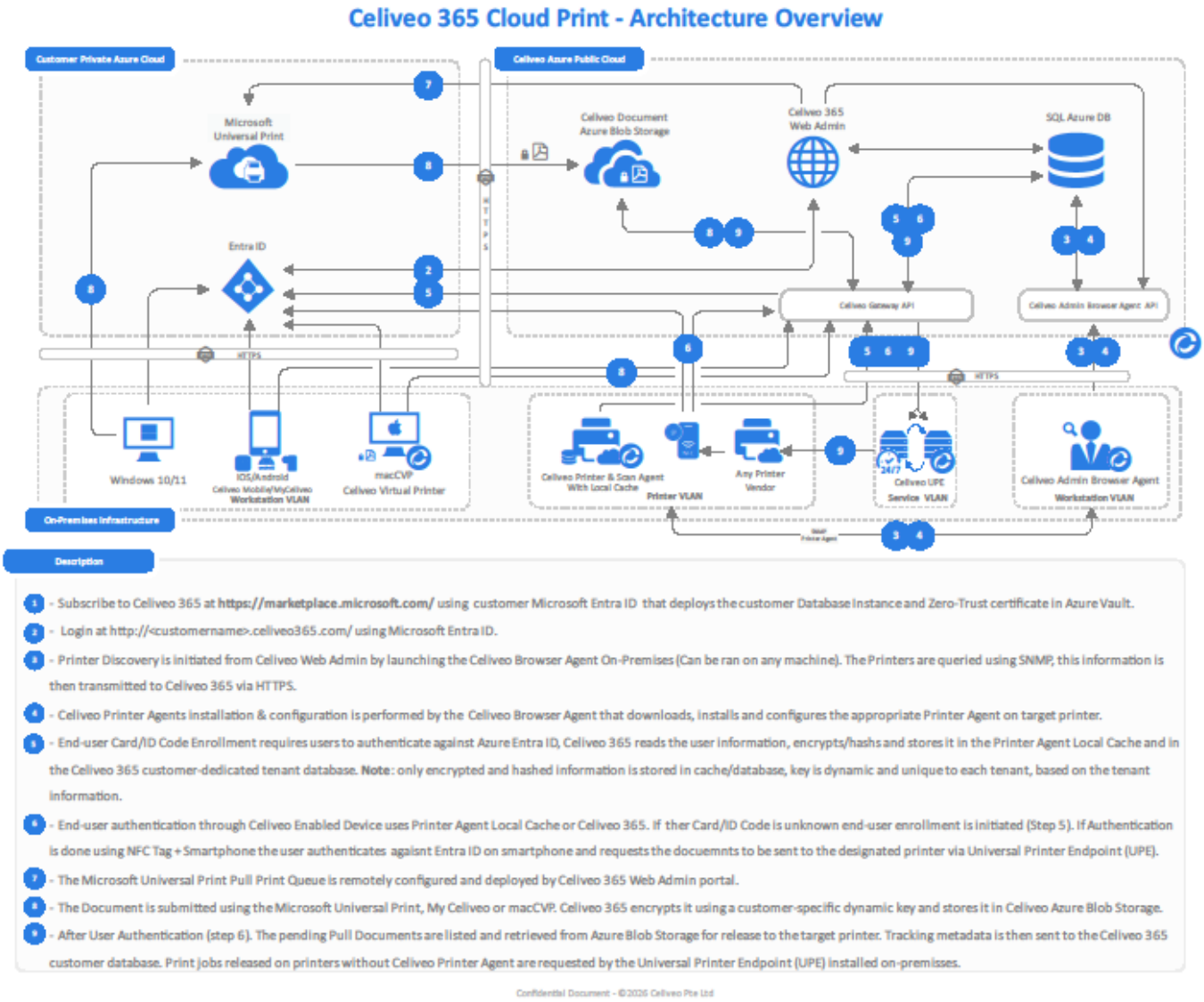
The protocol is modern HTTPS (TLS 1.2 or higher), further fortified by mutual TLS authentication using ECC-P256 certificate chains. This mutual authentication ensures that both the client (printer agent, UPE, or browser) and the cloud service verify each other's identity before any data exchange, preventing man-in-the-middle attacks and unauthorized access even on compromised networks. Not a single bit of data is exchanged before both sides verify who they will communicate with.



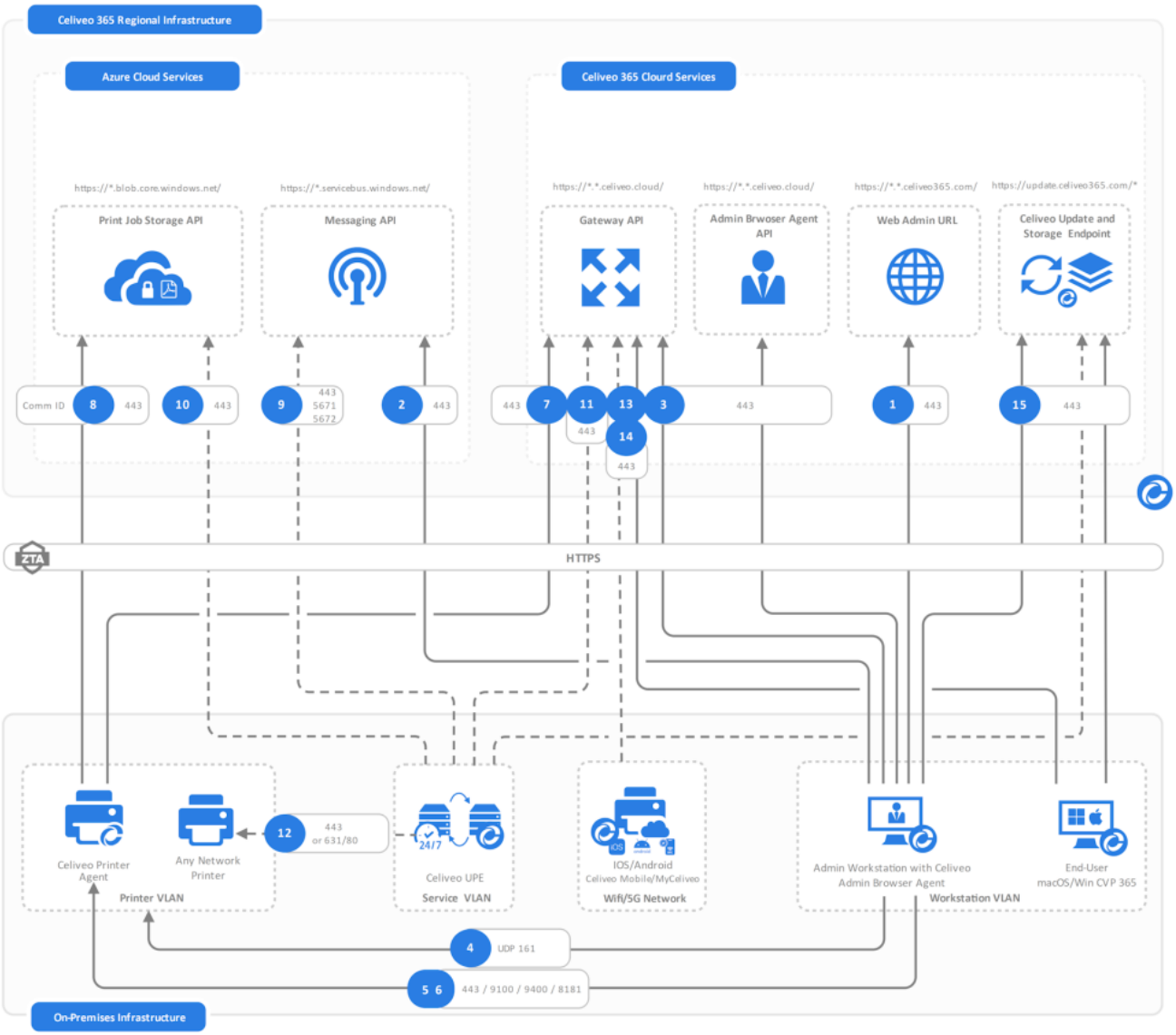
For the UPE—used to support any IPP 2.0-capable printer not supporting the Celiveo 365 embedded agent—the service leverages Microsoft Azure IoT for secure, outbound-only communication over port 443. No firewall ports need to be opened inbound; Azure pushes instructions to the UPE via this persistent, encrypted outbound channel, after which the UPE decrypts and delivers documents locally to the printer (using standard local ports like 631/IPP or 80/443 depending on the device model). Printer agents embedded in compatible MFPs similarly establish outbound connections to pull documents metadata, authentication events, and tracking information, all encrypted and authenticated mutually.

This outbound-only, port-443-exclusive model delivers several high-security benefits:

1. Zero inbound exposure — No risk of external attacks targeting on-premises devices or services.
2. Simplified firewall management — Organizations simply allow outbound HTTPS to known Celiveo and Azure endpoints, aligning with standard Microsoft 365/Universal Print allowlisting practices.
3. Compliance-friendly — Supports stringent security policies (e.g., ISO 27001:2022, SOC 2, HIPAA) by avoiding legacy ports, reducing complexity, and enforcing encryption and mutual authentication at every hop.
4. Resilience in restricted networks — Works reliably behind strict proxies or firewalls that permit only standard web traffic.



In summary, Celiveo 365 achieves enterprise-grade secure Pull Print with the lightest possible network footprint: purely outbound port 443 traffic secured by mutual TLS authentication. This approach not only minimizes administrative overhead and potential vulnerabilities but also enables rapid, low-risk deployment in even the most security-conscious environments, making it an ideal choice for modern, cloud-first organizations leveraging Microsoft Universal Print.



- Outbound port: 443
- Inbound port: none
- Horizontal traffic for Admin purpose
    - SNMP (status, setup)
    - 631 (IPPS) or 9100 (raw)
    - 80/443 (app loading)

Endpoints to whitelist:

- Celiveo 365 Azure App endpoints
- https://*.blob.core.windows.net/
- https://*.servicebus.windows.net/
- https://*.*.celiveo.cloud/ (Azure App Service)
- https://update.celiveo365.cc/file/celiveoupdates/*
  (Azure App Service for Edge browser agent update)

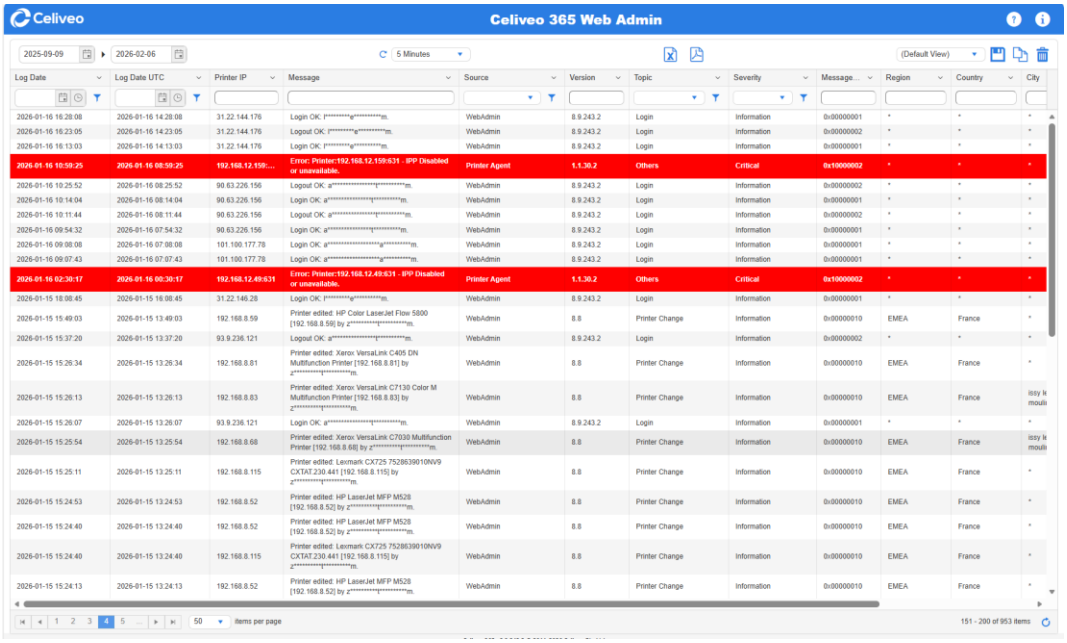
16. Logs and Audit

Comprehensive Logging and Auditing in Celiveo 365: Balancing Transparency with Privacy Compliance

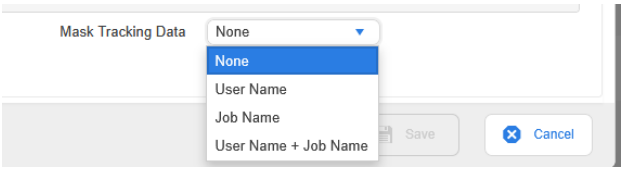
Celiveo 365 delivers robust, enterprise-grade logging and auditing capabilities that capture a complete audit trail of all activities across the platform, ensuring full traceability while upholding stringent privacy standards.

The system logs every significant event in real time, including actions performed in the Celiveo 365 Web Admin portal (such as queue creation, rule modifications, user/group assignments, and administrative changes), printer-specific operations (document releases, authentication attempts, copy/scan/fax usage on MFPs, failures, incidents, or hardware events like card reader removal on some printer models), and user interactions (successful and failed authentications via PIN, contactless card, NFC mobile/tablet, or Entra ID login, along with document releases, and deletions).

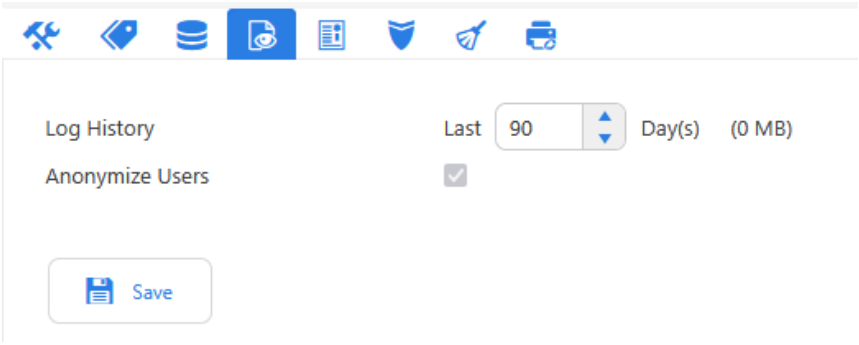
Extensive logs and alerts are displayed in dedicated browser views within the Web Admin portal, with advanced big-data reporting for detailed insights into who accessed what, when, and on which device.



This end-to-end traceability supports security investigations, cost allocation, Green IT analysis, and regulatory compliance audits.



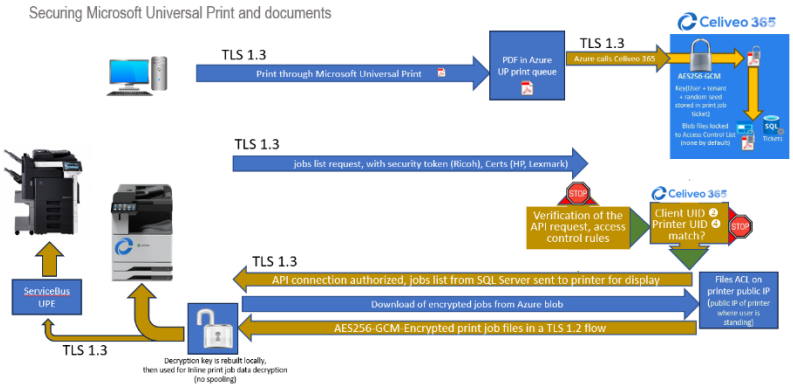
To remain fully compatible with GDPR, HIPAA, CCPA, and other privacy laws, Celiveo 365 incorporates intelligent privacy safeguards: sensitive user identities and personal data are masked, pseudonymized, or hashed where appropriate (e.g., in exported reports or shared dashboards), ensuring that only authorized personnel access identifiable information while still providing immutable, tamper-proof compliance trails through Azure's daily audits and encryption.



This privacy-by-design approach minimizes data exposure risks, fosters user trust, and simplifies demonstration of accountability during audits or data subject requests—all without compromising the platform's Zero-Trust-Access security model or operational transparency.

17. Documents encryption

In an increasingly hostile cyber landscape, where threats range from external hackers intercepting data in transit to malicious insiders or rogue administrators attempting unauthorized access, Celiveo 365 delivers uncompromising document confidentiality through its advanced, defense-in-depth encryption strategy. Built natively on Microsoft Azure PaaS and extending Microsoft Universal Print, Celiveo 365 ensures that documents are protected from submission to release with double encryption that surpasses standard protections.



As soon as a document reaches Azure via Universal Print—whether from Windows, macOS, mobile devices, or the secure portal—it undergoes immediate encryption using AES-256-GCM, a military-grade symmetric algorithm renowned for its speed, integrity, and resistance to cryptanalysis. Each document receives a unique, dynamic AES-256-GCM key, often derived from or tied to the requesting user's certificate in the Zero-Trust-Access PKI chain (based on ECC-P256), making keys multi-factor and non-reusable across documents or users. This per-document encryption renders stored content unreadable even if an attacker gains access to Azure blobs or databases—no user credentials are stored in Celiveo 365, and keys remain bound to authenticated identities.

This data-at-rest protection layers on top of TLS 1.3 (with mutual authentication via ECC certificates) securing all communication pipes, providing end-to-end encryption in transit that prevents interception by outsiders, man-in-the-middle attacks, or network eavesdroppers. For release, decryption occurs only inside the printer (via embedded agent on supported models or the secure Universal Printer Endpoint for others) after successful user authentication—such as PIN, contactless card, NFC mobile/tablet, or Entra ID—ensuring documents remain ciphertext until the authorized user is physically present.

This architecture neutralizes a broad spectrum of threats:

- Outsiders cannot decrypt intercepted or stolen data without the unique dynamic key.
- Insiders or rogue admins lack access to plaintext documents or decryption keys, as encryption is enforced at the cloud ingress and tied to user-specific PKI elements.

Even compromised infrastructure yields no usable data, thanks to the separation of keys from storage and the absence of persistent credentials.

By combining AES-256-GCM with dynamic, certificate-linked keys, per-document uniqueness, and TLS mutual authentication—all within a serverless, Zero-Trust-Access framework—Celiveo 365 provides robust protection that aligns with ISO 27001:2022, SOC 2, HIPAA, and GDPR requirements, empowering organizations to confidently adopt cloud Pull Print without compromising sensitive information against any class of adversary.

18. Security

Celiveo 365 delivers unbreakable, enterprise-grade security for Microsoft 365 and Universal Print environments through a purpose-built, serverless Azure-native SaaS architecture founded on true Zero-Trust-Access principles.

Every communication—between clients, printers, MFPs, and the cloud—is treated as hostile until authenticated via multi-level ECC-P256 elliptic curve certificate chains unique to each tenant, eliminating passwords, secret keys, and VPN dependencies while enabling instant revocation of compromised endpoints.



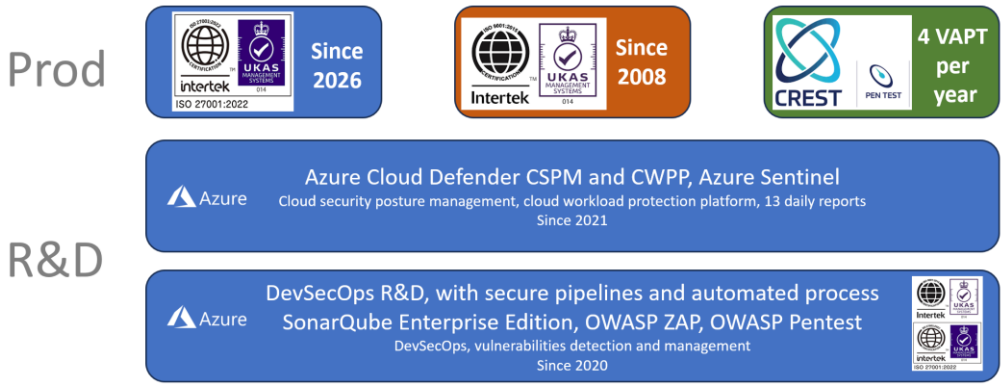
Tested with the following compliances requirements

- ISO 27001:2022 and ISO 27001:2013
- NIST SP 800 171 R2
- FedRAMP M
- NIST SP 800 53 R5
- FedRAMP H
- HIPAA HITRUST
- CIS Azure Foundations v1.4.0
- SOC TSP
- SOC 2
- New Zealand ISM Restricted
- Microsoft cloud security benchmark
- Canada Federal PBMM
- UKO and UK NHS
- Australian Government ISM PROTECTED
- New Zealand ISM Restricted v3.5

Daily audit by Microsoft Cloud Defender CSPM on the full SaaS infrastructure

Documents remain under customer control within their own Microsoft 365 tenant, undergoing military-grade double encryption (AES-256-GCM with dynamic, certificate-tied keys at rest, plus TLS 1.3 in transit), with metadata and authentication elements (PINs, card IDs) stored exclusively as irreversible SHA-256 hashes. Dedicated per-tenant SQL databases and IP-locked Azure Blob storage ensure complete data isolation, rendering even a full database breach useless to attackers, while Celiveo support and R&D teams have zero visibility into customer documents or PII. Integrated AI-Driven Data Loss Prevention (AI-DLP) scans documents in real time for sensitive content (PII, PHI, financial data) before release, and secure pull-printing with Entra ID SSO, card/NFC/mobile, or PIN authentication guarantees documents are only accessible by authorized users at the device.

Fully compliant with ISO 27001:2022 (covering SaaS and Cloud), GDPR, HIPAA, SOC 2, CCPA, and 11+ global standards—with daily automated compliance audits and on-demand reports— Celiveo 365 adheres to SecDevOps principles—prioritizing security as the foundational element throughout the entire software development lifecycle—by implementing rigorous, high-security R&D pipelines that embed security practices from design through deployment.



The platform's development process follows a structured, multi-environment progression featuring dedicated R1D (research and initial development), test, staging, and production instances of its fully Azure-native SaaS architecture. This segregated approach enables comprehensive security validation at every stage: SAST, DAST & Cloud Security pipeline with peer review of code change, early threat modeling and secure-by-design prototyping in R&D, automated vulnerability scanning, static/dynamic analysis, and penetration testing in the test environment, controlled integration and pre-production security hardening in staging, and finally hardened, monitored deployment to production with continuous monitoring and automated rollback capabilities in Azure.

By enforcing least-privilege access, code reviews incorporating security champions, infrastructure-as-code with immutable configurations, and integrated secrets management across all pipeline stages, Celiveo ensures that potential vulnerabilities are identified and mitigated proactively—often referred to as "shifting security left"—while maintaining rapid iteration without compromising the enterprise-grade Zero-Trust-Access foundation that protects customer data end-to-end. This disciplined SecDevOps methodology, combined with ISO 27001:2022-certified processes, delivers unmatched security assurance and software quality for organizations relying on Celiveo 365 in sensitive, compliance-driven environments.

19. GDPR, CCPA and Privacy Law Compliance by Design

Modern privacy regulations such as **GDPR (EU)**, **CCPA/CPRA (California), PIPEDA/CPPA (Canada) APPI (Japan), PDPA (Singapore, Thailand), PIPA (South Korea), DPDPA (India)** and other global data protection frameworks impose strict requirements on how personal data is processed, stored, secured, and audited. Celiveo 365 has been architected from the ground up with **privacy-by-design and privacy-by-default principles**, ensuring that customer data exposure is minimized and regulatory compliance is structurally embedded in the platform.

- **No User Data Stored in Celiveo Databases**

Celiveo 365 does **not store personal user information** (such as names, emails, or identity attributes) inside its SQL databases, even for users authenticating on printers.
Instead:

- Only **hashed identifiers** and secure pointers referencing Microsoft Entra ID (Azure AD) objects are stored.
- User identity validation is performed exclusively through **Entra ID authentication and authorization mechanisms**.
- All identity data remains under the customer's Microsoft tenant governance.

This architecture significantly reduces the risk surface and aligns with GDPR principles of **data minimization (Art. 5)** and **privacy by design (Art. 25)**. Because Celiveo does not maintain independent user identity records, it also simplifies compliance with **data subject access requests (DSAR)** and right-to-erasure obligations.

Strict Tenant Isolation – Dedicated SQL Database Per Customer

Each Celiveo 365 customer operates on a **dedicated SQL database instance**, eliminating shared data layers between tenants.
This design prevents:

- Horizontal privilege escalation
- Cross-tenant data exposure
- Accidental data leakage between organizations

Such segregation aligns with GDPR's requirements for **integrity and confidentiality (Art. 5(1)(f))** and supports CCPA's mandate to implement reasonable security procedures to protect consumer data.

ISO 27001:2022 Certification and Independent Audit

Celiveo is **ISO/IEC 27001:2022 certified**, with its Information Security Management System (ISMS) audited by **Intertek**, an internationally recognized certification body.

ISO 27001:2022 directly supports GDPR and privacy law compliance through:

- Formal **risk assessment and risk treatment processes**
- Defined **access control policies**
- Encryption and cryptographic controls
- Secure development lifecycle procedures
- Incident response and breach notification governance
- Vendor and third-party risk management
- Continuous monitoring and internal audit processes
- Documented data retention and data classification policies

ISO 27001 Annex A controls (especially those related to access control, cryptography, logging, and supplier relationships) provide a structured framework that aligns with GDPR Articles 24, 28, 32, and 33 concerning security of processing and breach management.

Annual external audits ensure these controls are not only documented but actively implemented and monitored.

Stealth Mode: Advanced User Anonymization

Celiveo 365 provides an optional **Stealth Mode** that enables deep anonymization of print-related metadata.

When activated:

- User identities can be anonymized in logs and reports.
- Print job names can be masked or replaced.
- Tracking data can be stripped of any content hints.
- Configuration can be applied globally or at granular levels (including per printer).

This ensures that even operational logging and usage tracking contain no directly identifiable personal information, supporting compliance with strict data minimization and confidentiality requirements under GDPR and CCPA.

Privacy by Architecture

By eliminating local identity storage, enforcing strict tenant isolation, maintaining ISO 27001-certified governance, and enabling configurable anonymization, Celiveo 365 delivers a privacy-centric cloud printing platform aligned with global data protection laws.

Rather than relying solely on policy statements, Celiveo 365 embeds regulatory compliance directly into its technical architecture—reducing legal risk, simplifying audits, and strengthening customer trust.

20. Elasticity for Enterprise-Grade Performance

Celiveo 365 stands as a true cloud-native SaaS solution built directly on Microsoft Azure Platform-as-a-Service (PaaS), inheriting the platform's inherent elasticity, automatic horizontal scaling, and distributed architecture to deliver seamless performance regardless of workload demands.

Unlike traditional print management solutions that rely on virtual machines (VMs) tied to specific servers—or even hosted gateways in the cloud—Celiveo 365 operates as serverless, elastic resources deep within Azure. This means the service automatically scales out by provisioning additional instances across multiple servers and datacenters as documents volume, user counts, or printer fleet sizes increase, without manual intervention, reboots, or capacity planning.

Azure's auto-scaling handles peak loads—such as end-of-month reporting surges, seasonal printing spikes, or rapid enterprise growth—dynamically adjusting compute and throughput while maintaining low latency and high availability, often backed by Azure's 99.75% (combination of Azure PaaS services with 99.95% SLA) + SLA through optional geo-redundancy and multi-region deployment.

This PaaS foundation provides profound advantages over VM-based alternatives, which remain vulnerable to single points of failure, hardware degradation, memory exhaustion during usage peaks, OS patching windows that cause downtime, and inherent limits on vertical scaling. In contrast,

Celiveo 365 decouples from physical or virtual server constraints: there are no OS vulnerabilities to patch, no reboots or downtime required for updates, and no risk of a single VM bottleneck impacting the entire fleet.

Horizontal scaling at will ensures linear growth—supporting up to tens of thousands of printers, global sites, and massive concurrent documents—while edge computing on supported printers (via embedded agents) adds offline resilience for authentication and rules enforcement even during transient connectivity issues. For the largest deployments, optional dedicated elastic instances with geo-replication further enhance performance and compliance for multi-region enterprises.

The result is predictable, cost-efficient scalability aligned with actual usage: organizations pay only for active monthly users via floating licenses, avoiding over-provisioning common in VM-hosted systems. This architecture empowers hybrid and remote workforces to print securely from anywhere without performance degradation, eliminates infrastructure overhead, and future-proofs print management against growth and decrease. By fully embracing Azure's elastic PaaS model, Celiveo 365 transforms printing into a resilient, always-available service that scales effortlessly—delivering enterprise reliability without the traditional pain points of legacy or hybrid-cloud print solutions.

21. Service Level Agreement (SLA), RTO and RPO

Service reliability and operational continuity are critical factors for enterprise cloud services. For organizations relying on cloud print management and document security platforms, clearly defined availability and recovery targets ensure predictable service quality and business continuity. Celiveo 365 addresses these requirements through a structured **Service Level Agreement (SLA)** supported by defined operational procedures, monitoring systems, and incident response commitments.
The SLA establishes measurable targets for system availability, support response, and service recovery.
In combination with **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO)**, it forms the foundation of Celiveo's service continuity strategy and operational reliability framework. These metrics define how quickly services must be restored after disruptions and how much data loss is acceptable, ensuring alignment between infrastructure capabilities and business continuity expectations.

Celiveo Service Level Agreement (SLA)

SLA Scope
The Celiveo SLA defines the terms governing the delivery of Celiveo 365 SaaS services to customers, including service availability targets, customer responsibilities, monitoring mechanisms, and remedies in the event of service disruptions.
The agreement primarily covers the **Cloud Print Service and associated SaaS platform components**, ensuring that enterprise customers benefit from predictable uptime, responsive support, and transparent monitoring.

Service Availability Commitment
Celiveo guarantees a **minimum service uptime of 99.75%** for its cloud services.

- **Target uptime: 99.75% per month**
- **Maximum aggregated downtime: less than 111 minutes per month**

The availability commitment ensures that you can rely on the service for critical document workflows such as secure printing, document tracking, and access control in distributed enterprise environments.

Incident Response and Resolution Targets

To maintain operational continuity, Celiveo defines response and resolution targets for service incidents:

Resolution Time

For complete service disruption of Celiveo 365 (Severity 1), Celiveo aims to resolve the issue within:

- **1 hour**

This rapid recovery objective helps limit operational impact for organizations relying on cloud printing infrastructure.

Support Response Time

Celiveo commits to acknowledging non-severity 1 support requests within:

- **One business day**

Customers must report incidents through the official **Celiveo support portal**, ensuring traceability and proper escalation.

Monitoring and Performance Reporting

Service performance is continuously monitored using Celiveo's operational monitoring systems.
They collect availability and operational metrics used to validate SLA compliance.
Customers can view service status and uptime information via:

- Celiveo service status portal: https://status.celiveo365.com for standard deployment offers
- Azure Sentinel for clients

In case of disputes regarding uptime or downtime measurements, Microsoft Azure service logs are considered the authoritative reference for determining service availability.

Service Credits for SLA Breaches

If Celiveo fails to meet the agreed availability levels, customers may be eligible for service credits.
The SLA specifies the following remedies:

Monthly Uptime	Downtime	Service Credit
≥ 99.9%	≤ 216 min	No credit
< 99.9%	> 216 min	Up to **10% of monthly fees**
< 99%	> 432 min	**20% of monthly fees**

Service credit claims must be submitted within the calendar month following the incident and must include sufficient details about the reported downtime.
These credits constitute the exclusive contractual remedy for SLA breaches.

SLA Exclusions

The SLA explicitly excludes outages or service disruptions resulting from external dependencies or customer infrastructure.

Examples of excluded scenarios include:

- Customer network instability
- Internet connectivity problems
- Firewall or routing issues
- Client-side configuration errors
- Printer instability, misconfiguration and firmware defects
- Microsoft Azure services outages
- Microsoft Universal Print spooling and print job rendering defects/outages
- Customer workstation, server or mobile failures

By defining these exclusions, the SLA ensures that availability metrics accurately reflect the performance of the Celiveo service itself rather than external infrastructure components.

Recovery Time Objective (RTO)

The Recovery Time Objective (RTO) defines the maximum acceptable time required to restore service after a disruption. In cloud services, this metric reflects the organization's ability to detect incidents, initiate remediation procedures, and return systems to operational status.

Celiveo's operational objective for full service disruption resolution is:

RTO target:

1 hour

This aggressive recovery objective is supported by:

- cloud infrastructure redundancy
- automated monitoring
- incident response procedures
- scalable Azure platform services

The objective ensures minimal interruption to business operations relying on secure cloud printing and document access services.

Recovery Point Objective (RPO)

The Recovery Point Objective (RPO) defines the maximum amount of data loss that may occur in a disaster scenario, measured as the time between the most recent recoverable data state and the moment of failure.
In cloud-native architectures such as Celiveo 365, RPO targets are achieved through:

- cloud-native database resilience
- replicated storage services
- automated backups
- distributed cloud infrastructure

These mechanisms ensure that data related to:

- print jobs
- user access control
- audit and tracking logs
- configuration settings

remains protected and recoverable in the event of infrastructure incidents.

RPO: 1 hour
This means that, in a worst-case recovery scenario, up to one hour of data may need to be reconstructed or replayed following restoration of the service. The RPO therefore drives the platform's backup and replication strategies to ensure that recoverable data snapshots are maintained at intervals compatible with this objective.

Operational Governance and Customer Responsibilities

Ensuring SLA compliance requires cooperation between the service provider and customers.

Customers are responsible for:

- promptly reporting service issues through the https://support.celiveo.com portal
- verifying that issues are not caused by local infrastructure problems
- providing access or information necessary for troubleshooting

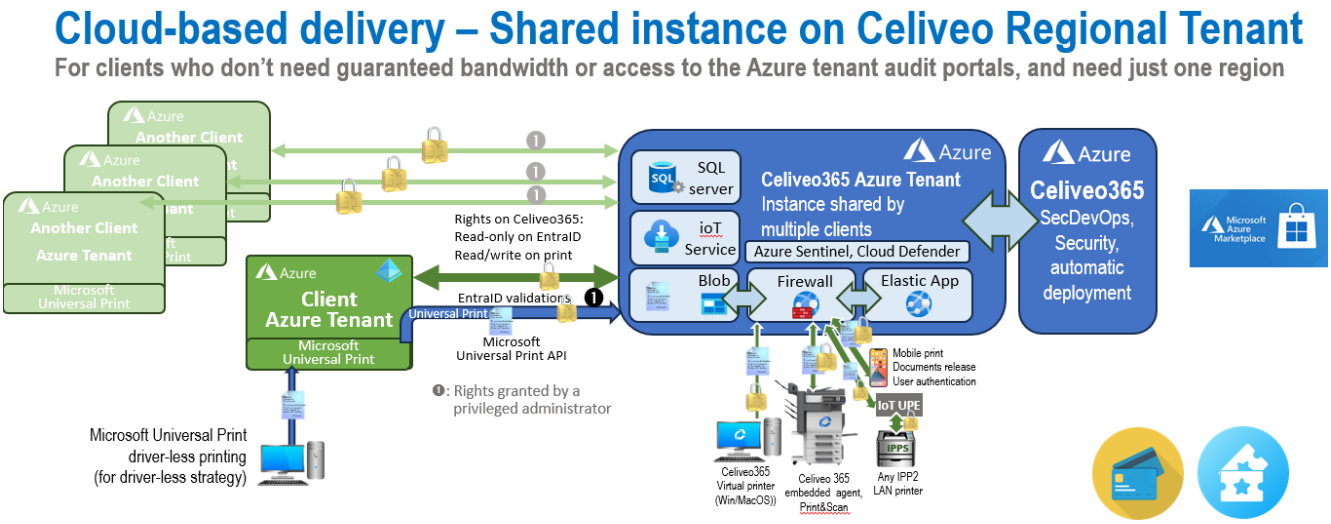
This collaborative approach allows Celiveo engineers to quickly identify root causes and restore service availability.

22. Your Deployment Options

Celiveo 365 is proposed in three deployment modes:

- Shared resources with dedicated SQL database, on Celiveo Azure tenant
- Dedicated resources and endpoints on Celiveo Azure tenant
- Dedicated resources and endpoints on your Azure tenant

Shared resources with dedicated SQL database, on Celiveo Azure tenant



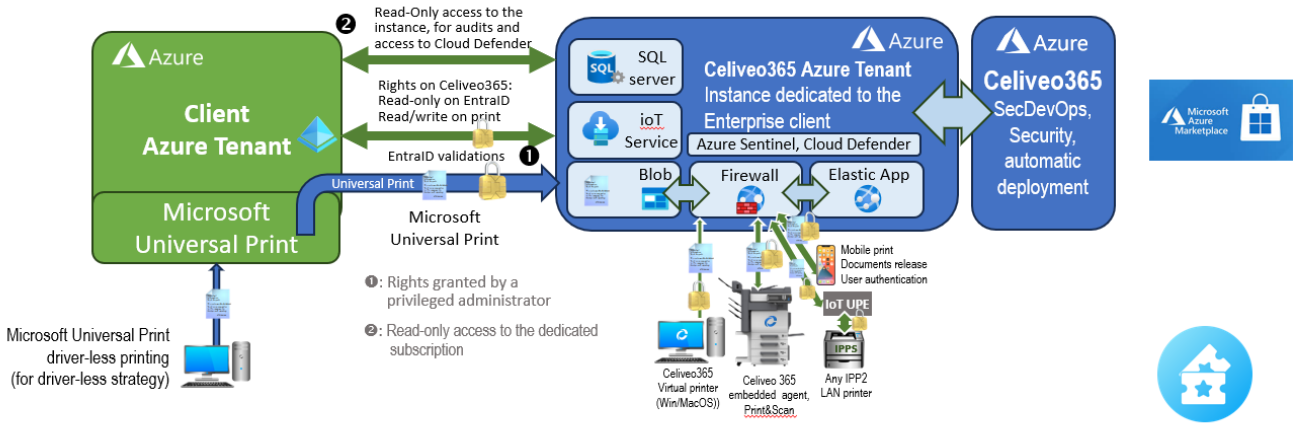
Celiveo 365 is running on the Celiveo Azure tenant, not on the client tenant, in the chosen regional Azure Datacenters for the client.
A trusted Entra-ID binding is created between the client and Celiveo tenant to access Entra-ID/AAD information and manage Universal Print Jobs (if applicable). The client has a dedicated SQL Server database, no client mix in databases. No VPN used/needed.

Client workflow: Azure Marketplace to subscribe and bind tenant - usage on https://<name>.celiveo365.com
Deployment/updates by Celiveo: Automated using Terraform templates, no manual process, test/staging/production instances

Dedicated resources and endpoints on Celiveo Azure tenant

Cloud-based delivery – Dedicated instance on Celiveo Tenant

For clients who want a guaranteed bandwidth, with 24x7 access to monitoring and security audits for Cloud IT & CSO



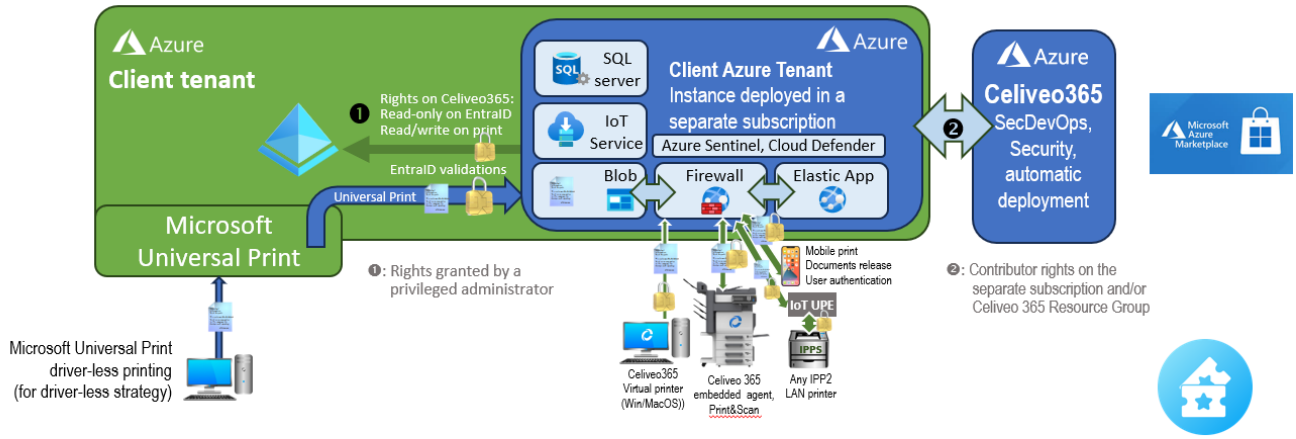
Celiveo 365 is running on the Celiveo Azure tenant, not on the client tenant, in one or more Azure Datacenters chosen by the client (Cloud sovereignty). A trusted Entra-ID binding is created between the client and Celiveo tenant to access Entra-ID/AAD information and manage Universal Print Jobs (if applicable). Client IT and CSO have read-only access to the infrastructure like if it is on their tenant. No VPN used.

Client workflow: Azure Marketplace to subscribe and bind tenant - usage on https://<name>.celiveo365.com
Deployment by Celiveo: Automated using Terraform templates, no manual process, test/staging/production instances

Dedicated resources and endpoints on your Azure tenant

Cloud-based delivery – Dedicated instance on Client Tenant

For clients who want all data on their own tenant, with 24x7 access to monitoring and security audits for Cloud IT & CSO



Celiveo 365 is running on the Client Azure tenant, not on the Celiveo tenant, in one or more Azure Datacenters chosen by the client. Client IT and CSO have read-only access to the infrastructure like if it is on their tenant. No VPN used.

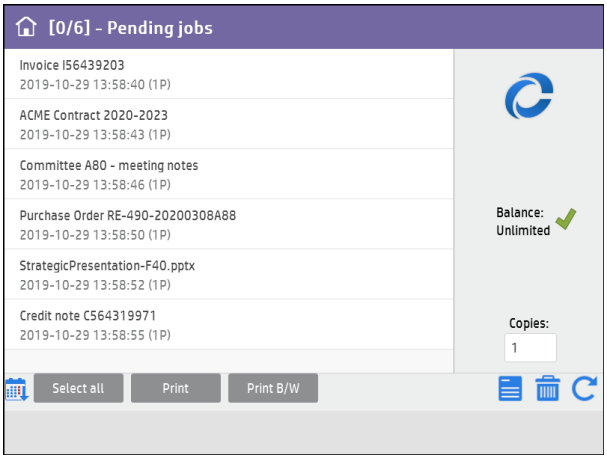
Client workflow: Azure Marketplace to subscribe and bind tenant - usage on https://<name>.celiveo365.com
Deployment by Celiveo: Automated using Terraform templates, no manual process, test/staging/production instances

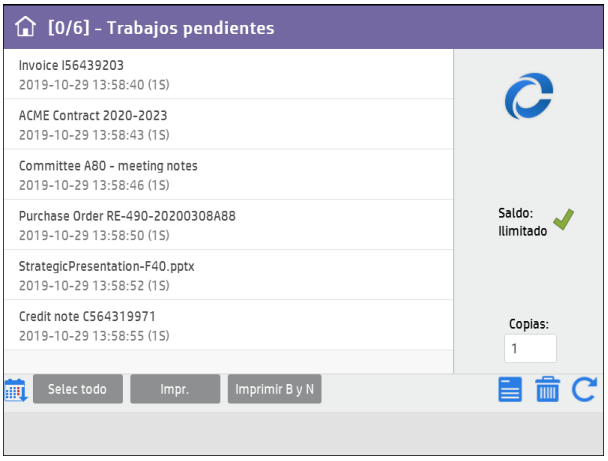
23. Supported Languages

Because Celiveo clients are located all over the world, Celiveo 365 Web Admin, Embedded Printer Agent and WinCVP 365 clients for Windows and MacOS are in the following languages:

Portuguese (BR)	Japanese
Czech	Korean
Dutch	Polish
English	Russian
Finnish	Slovakian
French	Spanish
German	Swedish
Hungarian	Turkish
Indonesian Bahasa	Chinese (simplified)
Italian	Chinese (traditional)

Example of Celiveo 365 Printer Agent screen in English and in Spanish, on a MFP screen:





24. Features list

	Celiveo 365 Cloud Print Edition	Celiveo 365 Enterprise Edition
■ standard □ optional		
CORE FUNCTIONS		
Full Cloud Secure Print & Scan Management	■	■
Eliminate Print Server, Print Driver/Agent/Software	■	■
Azure-based Follow-me Pull Print	■	■
Print Release with Card, NFC phone, PIN, ID Code	■	■
Print Rules for Cost Reduction, Compliance	■	■
Mobile Print, Print on Home Printers	■	■
Usage Tracking & Reporting (Power BI)	■	■
AI-DLP – Data Loss Prevention	■	■
AI-Powered Document Management creating a Corporate Memory	■	■
Elastic, High Availability SaaS on Azure PaaS	■	■
One hour onboarding remote session per tenant	■	■
ADMINISTRATION		
Central management console hosted on Azure portal, zero setup	■	■
Role Based Access Control (RBAC) with scope and geo restrictions	■	■
Printer discovery and bulk import from browser	■	■
Suppression of all Print Drivers, agent on PC	■	■
Ability to apply configurations at scale, bulk edits, fleet-wide policy	■	■
Deep integration with Microsoft Universal Print	■	■
Deep integration with Azure Entra ID SSO	■	■
Multi-level delegation of administration	■	■
Conditional access to printers by Entra ID group, geotags	■	■
Geo tags and floor maps with printers	■	■
SECURE PRINTING		
Remove all print servers, all print drivers, all print solutions	■	■
Secure Printing without any app/driver on PC	■	■
Print through standard Win 11 Cloud Print queues	■	■
Print from mac, with Entra ID SSO, directly to Azure	■[3]	■[3]
Print from mobile (iOS, Android) and browser, with Entra ID SSO	■	■
Release documents on any printer upon authentication	■	■

Release documents from mobile upon Entra ID SSO authentication	■[2]	■[2]
Printer locator with floor maps and printer specs	■	■
On printer screen , select documents to release (Pull Print)	■[1]	■[1]
On mobile screen and browsers, preview and release documents	■	■
Live printer status	■[2]	■[2]
Optional Print agent for Win10/11/365 and Azure Virtual Desktop	■	■
Optional Print agent for MacOS for advanced features	■	■
Automatic drivers, print queue deployment and installation	■[3]	■[3]
Automatic documents data encryption (AES265 dynamic keys)	■	■
Print rules on printer/MFP	■	■
Print rule to stop document	■	■
Print rule to force Black & White	■	■
Print rule to force toner saving	■[1]	■[1]
Print rule to force duplex	■	■
Soft quota for print & copy	■	■
Hard quota for Pull Print	■	■
Stealth mode masking sensitive documents metadata in tracking	■	■
Document name anonymizer	■	■
SECURE SCAN		
Scan to OneDrive, direct to OneDrive with Oauth2 authentication	■[4]	■[4]
Scan to email, direct to 365 with modern authentication (no SMTP)	■[4]	■[4]
Scan to email, direct to MailJet with Authentication Key (no SMTP)	■[4]	■[4]
Scan to email (SMTP)	■[4]	■[4]
Smart Scan with document preview	■[4]	■[4]
Smart Scan with single screen for OneDrive, Email	■[4]	■[4]
Enforcement of “Scan-to-Self”	■[1]	■[1]
USER AUTHENTICATION FOR SECURE PRINT AND SCAN		
User Authentication integrated with Entra ID	■	■
Enrollment compatible with password-less policy	■	■
Authentication on printer: PIN ID Code	■	■
Authentication on printer: AlphaPIN ID Code	■	■
Authentication on printer: Card	■	■
Card self-(un)enrollment on MFP	■	■
Authentication on printer: NFC with mobile	■	■
iOS and Android mobile/tablet	■	■

Authentication rules[1]	■	■
Multilevel authentication (i.e. card & login/pwd, or PIN & proximity)	■	■
Dual factor (card + password)	■	■
Authentication against offline users list in the printer/MFP[1]	■	■
Automatic sync of offline users list with Entra ID[1]	■	■
High Availability[1]	■	■
AI-DLP DATA LOSS PREVENTION		
Automatic AI-Analysis of documents sent to Azure Print Queues	■	■
Activable per print queue	■	■
Detects PII	■	■
Detects PHI	■	■
Custom actions upon DLP trigger	■	■
Stop document upon DLP detection	■	■
Warning upon DLP detection	■	■
Customizable and multi-lingual messages for DLP detection	■	■
Log message injected upon DLP detection	■	■
Poolable DLP detection page credits	■	■
AI-POWERED DOCUMENT MANAGEMENT SYSTEM		
Easy AI-DMS setup in one hour, creating a Corporate Memory		■
Save up to 2 hours of work per user/day, with information availability		■
Instant document Capture built in Win 11/365, Azure Virtual Desktop		■
Celiveo AI agent for Teams, to query the Corporate Memory		■
Multi-lingual Generative AI from natural language queries in Teams		■
Document capture from Mobile, tablet, BYOD compliant		■
Siloed AI Analysis and Indexing of Information		■
Automatic User Cohorts to Silo Information		■
Individual PKI Document Encryption using Azure Key Vault		■
Document & AI Knowledge Base stored inside your Azure Tenant		■
Your documents and queries are not used to train any public AI system		■
No markup on Azure resources usage cost for AI and storage		■
TRACKING & REPORTING, COST		
Reporting at cost-center or site level, including usage by site/device, monochrome vs color trends, and policy impact.	■	■
Tracking data from printer engine	■[1]	■[1]
Tracking data from document analyzer in Azure	■	■
Power BI dashboard and report	■	■
Table report	■	■
Graphical reports	■	■
Green IT reports, CO^2 and Saved Trees	■	■
Detailed cost definition, per printer model and paper format	■	■
Detailed documents and user metadata	■	■
Documents report per user	■	■
Documents report per printer	■	■

Reports per Entra ID group	■	■
Advanced filtering in reports	■	■
Complete data CSV export	■	■
AUDIT, LOGGING		
Audit logging for print, copy, scan, and admin activity/changes	■	■
Exportable logs	■	■
Customizable views to display alerts, warning, information	■	■
SECURITY		
SaaS on Azure PaaS, no VM, no OS to update	■	■
Zero downtime during SaaS update, maintenance	■	■
Dedicated SQL database for each client, access by certificate chain	■	■
Secure By Design, no passwords, no secret keys	■	■
Zero-Trust-Access architecture, based on ECC-P256 Cert chains forest	■	■
Mutual TLS Auth between endpoints using ECC-P256 Cert chains	■	■
Outgoing port opening only, no incoming port opening	■	■
Communication exclusively over port 443	■	■
Support for web proxy and ZCaler	■	■
Documented endpoints list	■	■
DevSecOps secure development pipelines	■	■
SAST, DAST & Cloud Security pipeline with peer review	■	■
24x7 CSPM protection (Cloud Security Posture Management)	■	■
24x7 CWPP protection (Cloud Workload Protection Platform)	■	■
Automatic failover and High Availability in Azure	■	■
Automatic encrypted backup in Azure of your records	■	■
Infrastructure with R&D, test, staging and production instances	■	■
Instant rollback to last stable version if needed, without downtime	■	■
ISO 27001:2022 certified company, UKAS and Intertek	■	■
HOSTING		
Shared tenant in Azure datacenter in client-selected region	■	■
Dedicated tenant in Azure datacenter in client-selected region	□	□
Deployment on client Azure tenant for fully siloed data	□	□
8x5 Support	■	■
24x7 Support	□	□
LICENCING MODEL		
Subscription on the Microsoft Azure Marketplace	■	■
Invoicing by Microsoft or Microsoft CSP	■	■
No billing of inactive users during a month	■	■
No cost per printer, PC or mobile	■	■
Subscription covers print storage and print egress traffic cost	■	■
Subscription per floating user/month, 12 months commitment	■	■

[1]: available on printers with Celiveo 365 embedded agent support

[2]: Azure IoT agent client required on the printer network, one instance minimum

[3]: On Windows 10/11/365 with the WinCVP 365 optional agent, on Mac with the optional macCVP 365 App

[4]: Available on Ricoh SOP 2.5/3.0, Xerox-Lexmark eSF, HP FutureSmart 4/5

Index

A

AI Document Management, 5
AI-DLP, 24, 33, 34, 35, 40, 49, 61, 63
AirPrint, 21, 22
Android, 10, 17, 21, 22, 27, 61, 62
Architecture, 11, 12, 14
Authentication, 19, 22, 63
  Alpha ID, 62
  ID Code, 62
  Self-enrollment, 62
Azure, 5, 6, 7, 10, 11, 14, 19, 20, 25, 31, 32, 34, 38, 39, 42, 43, 45, 47, 48, 49, 50, 53, 58, 59, 61, 62, 63, 64

B

Browser, 17, 25, 39, 42, 45, 46, 61

C

Card, 15, 16, 17, 19, 21, 27, 34, 40, 46, 48, 49, 63
CCPA, 7, 47, 49
CCPA/CPRA, 51
Celiveo Features, 61
Cloud Print, 6, 7, 10, 11, 12, 13, 14, 38, 61
CO^2, 10, 36, 37, 63

D

Deployment, 38, 62
Distributed architecture, 12
Document Release, 15
document submissions, 36, 40, 42
Documents, 10
DPDPA, 51

E

ECC-P256 certificate chains, 42
Embedded Agent, 13, 19, 20, 22, 25, 40
Encryption, 16, 17, 23, 43, 47, 48, 49, 62
Endpoints, 45
Entra ID, 5, 16, 17, 19, 20, 21, 22, 23, 24, 27, 29, 33, 34, 35, 38, 39, 40, 46, 48, 49, 61, 62, 64

F

Floor maps, 32, 61, 62
Fujifilm, 20, 22, 27, 42

G

GDPR, 5, 7, 8, 24, 34, 36, 40, 47, 48, 49, 51, 52
Geotags, 25, 30, 31, 32, 61
Green IT, 36, 40, 46, 63
Guest Printing, 3, 28
guests, 28, 29

H

High Availability, 10, 63
HIPAA, 5, 7, 24, 34, 36, 40, 43, 47, 48, 49
HP, 20, 21, 22, 23, 24, 25, 27, 40, 42, 64

I

Installation, 62
iOS, 10, 17, 21, 27, 61, 62
IoT Universal Printer Endpoint, 19
IPPS, 13, 25, 45
ISO 27001, 5, 7, 24, 43, 48, 49, 50, 64

L

LDAP, 63
Lexmark, 20, 21, 22, 23, 24, 25, 27, 40, 42, 64
logs, 36, 40, 46, 64

M

macCVP 365, 16
macOS, 10, 16, 48
MailJet, 62
MDM, 25, 26
Metadata, 62, 63, 64
Microsoft 365, 17, 23, 24, 38, 43, 49
mobile printing, 10, 17
Mopria, 21, 22
mTLS, 25, 26

N

NFC, 15, 16, 17, 19, 20, 22, 27, 40, 46, 48, 49, 61, 62

O

OneDrive, 19, 23, 24, 62
Operating System, 12

P

PDPA, 51

PIN, 15, 16, 17, 19, 22, 23, 27, 40, 46, 48, 49, 61, 62, 63
PIPA, 51
PIPEDA, 51
Ports, 42
Power BI, 10, 33, 36, 37, 40, 61, 63
Print rules, 33, 62
Printer Discovery, 26
Printer screen, 19, 22
Printers and MFPs
HP, 22
Konica Minolta, 22
Lexmark, 22
Other network printers, 22
Ricoh, 22
Xerox, 22
Privacy Law, 51
Protocols, 42
Pull Print, 10, 12, 13, 14, 20, 22, 26, 38, 44, 48, 62
Push Print, 17, 27

R

RBAC, 28, 29, 61
Ricoh, 20, 21, 22, 23, 24, 25, 27, 40, 42, 64
RPO, 54, 57
RTO, 54, 56
Rules-based printing, 19

S

Scan, 4, 19, 23, 24, 25, 34, 36, 40, 46, 64
SecDevOps, 49, 50
Security, 25, 29, 40, 49, 64
SLA, 11, 53, 54, 55, 56, 57
SMTP, 24, 62
SNMP, 20, 25, 26, 31, 40, 45
Stealth mode, 62
Subscription, 7, 38
Supported Printers, 21

T

Tracking, 10, 13, 15, 19, 22, 36, 37, 40, 43, 61, 62, 63
Cost definition, 63
Reporting, 61, 63

U

Universal Print, 5, 6, 10, 11, 13, 14, 15, 16, 17, 25, 26, 33, 35, 38, 39, 41, 42, 43, 44, 48, 49, 61
UPE, 13, 20, 21, 22, 26, 40, 42, 43
User authentication, 19

W

Web Admin, 14, 15, 25, 30, 32, 39, 41, 46, 60
Wifi, 21, 22
Wi-Fi printers, 21
WinCVP 365, 14, 15, 42, 60, 64

X

Xerox, 20, 21, 22, 25, 27, 40, 42

Z

Zero-Trust-Access, 4, 12, 13, 16, 17, 19, 20, 21, 23, 26, 27, 29, 33, 34, 39, 42, 47, 48, 49, 50, 64

Your Notes

Your Notes

Your Notes


Celiveo 365