Celiveo 8

Ver 2022-09-22E — Last update: 6 December 2022

Celiveo

Copyright © 2022 Celiveo

Table of Contents

1. Welcome to the Celiveo Technical Documentation! 5

2. Legal Information 7

2.1. EULA for Celiveo 8 8

2.2. Terms of Service for Celiveo SaaS Services 12

3. Architecture Overview 19

3.1. Print Job Retention 20

3.2. Server-based Pull Printing 21

3.3. Serverless Pull Printing 22

3.4. Print Job Encryption 23

4. Downloads Celiveo 8 – Current Release Installers 27

5. Quick Start Guide 29

6. Compatibility 30

6.1. System Requirements for Celiveo 8 31

6.2. Requirements for Hardware 35

6.3. Operating System, SQL and Active Directory rights to install and use Celiveo 36

6.4. Ports and Communication 40

6.5. SNMP Settings 44

6.6. Celiveo Versions Compatibility with Windows 10 46

7. Installation 47

7.1. How to install the Celiveo Hardware 48

7.2. Installing the Celiveo Web Admin 50

7.3. Installing TGS 10 56

7.4. After Installation 61

7.5. Web Admin First Run 62

8. Configuration 66

8.1. Add Printers and their settings to the Web Admin 67

8.2. Add Printers Manually 78

8.3. ZeroConfig 82

8.4. Celiveo Virtual Printer for Windows 87

8.4.1. Antivirus False Positive cases 88

8.4.2. Add a Celiveo Virtual Printer to Web Admin 89

8.4.3. Add a Celiveo Shared Virtual Printer to Web Admin 98

8.4.4. Add a Celiveo Virtual Printer for Print-Direct 105

8.4.5. Deploy a Celiveo Shared Virtual Printer Package on a Print Server 108

8.4.6. Deploy a Celiveo Virtual Printer on a User's Work Station (For Pull Printing) 113

8.4.7. Deploy a Celiveo Virtual Printer on a User's Work Station (For Direct IP Printing) 118

8.4.8. Upgrade Celiveo Server Services for Windows 122

8.5. Celiveo Virtual Printer for macOS 126

8.5.1. Install Celiveo Virtual Printer on multiple macOS workstations – Silent Install Procedure 127

8.5.2. Add a Celiveo Virtual Printer on macOS machine – Interactive Install Procedure 130
8.5.3. Connect to a Windows Celiveo Shared Virtual Printer from macOS machine 136
8.5.4. Upgrade Celiveo Secure Services for macOS 144
8.5.5. Configure Celiveo macOS NAS Job Transfer with Job Delegation 145
8.5.6. Configuring the Kerberos SSO Extension 151
8.6. Multi-SQL Configuration 153
8.7. Configuring SQL Database for AlwaysOn Availability feature 160
8.8. Set up Access 165
8.9. Synchronize Printers 172
8.10. Set the Session Timeout 173
8.11. Configuration to be done at the Printer 176
8.11.1. Konica Minolta 177
8.11.2. Lexmark 188
8.11.3. Embedded Agent for Ricoh Android SOP 2.x MFP 195
8.11.4. Xerox 203
8.11.5. HP 213
8.12. Viewing and Updating Your Celiveo License 221

9. SAP Connector Configuration 224

10. Using Celiveo 229
10.1. Enroll a Card on a Celiveo-Enabled Printer 230
10.2. Tag Printers and Users 231
10.3. Place or Locate Printers on a Floor Plan 237
10.4. Print from a Workstation 241
10.5. Print Using Print-Direct 248

11. Authentication 251
11.1. Access Control Rules 252
11.2. Authentication Profiles 270
11.3. High Availability 282
11.4. Enable ID Code Authentication for Printers 289
11.5. Save Card Number and ID code on Active Directory 297
11.6. Enable Smart card authentication for printers 302
11.7. Configure BLE RF IDEAS Readers for Smartphone Authentication with Orange Pack-ID Application 309
11.8. Configure ID Mask 313
11.9. Custom Access Control for HP FutureSmart Printers 315
11.10. Using Microsoft AD LDS software 323

12. Print Management 336
12.1. Printers Overview 337
12.2. Create Print Rules 341

13. User Management 358
13.1. Managing System Administrators 359
13.2. Add Domain Users for Print Direct 367

14. Track and Report Print Jobs 371
14.1. Configure Quota Settings 372
14.2. Configure Default Cost Definitions 376
14.3. Configure Cost Definition Profiles 377
14.4. Using Celiveo Reporting tool – TGS 10 380
14.5. Downgrade from TGS 10 to TGS 8 389
14.6. Configure Embedded Tracking for Print-Direct 390
14.7. Add AD Attributes to User Enrollment Schema 391

15. Celiveo.me 393
15.1. Zero Trust Activation 396
15.2. Creation and installation of a Celiveo Shared Virtual Printer 398
15.3. Chromebook Printing 402
15.4. Mobile Printing 406
15.4.1. Office 365 Email Rules 408

16. Celiveo Print-Web 410
16.1. Celiveo Print-Web Installation Guide 411
16.2. Celiveo Print-Web Mobile Gateway Installation Guide 412

17. Technical Information 413
17.1. Celiveo Smart Appliance 414
17.1.1. Celiveo Smart Appliance (CSA) 415
17.1.2. Setup Celiveo Authentication Hardware 418
17.1.3. How to upgrade the Celiveo Version on CSA and Embedded Agents 420
17.1.4. Understanding CSA LED Flashing Behaviors 423
17.2. Multicard Reader – Specifications for Type A 425
17.3. Multicard Reader – Specifications for Type B 427
17.4. [IMPORTANT] Quick and Easy Solution to Disable SSL/ Early TLS Protocols and Enforce TLS 1.2 429
17.5. Managing 32 bit and 64 bit Architectures 434
17.6. Environmental Impacts of Printing – Formulae used in TGS 10 reports 435
17.7. Pushing Print Jobs to Network Attached Storage (NAS) 438
17.8. Celiveo WebAdmin Tools and API 442
17.9. Open Source codes used in Celiveo 8 (Latest version) 448
17.10. Upgrade to Celiveo 8 451
17.11. Migration Support to Celiveo 8 Versions 454
17.11.1. Migrate from SecureJet 7.0.x 461
17.11.2. Migrate from Celiveo 8.0.x 473
17.11.3. SAP Connector Migration 482

18. Troubleshooting 492
18.1. Common Questions 493
18.2. Retrieve Logs 494
18.3. Error Messages 495

19. Disaster Recovery Plan 496

1. Welcome to the Celiveo Technical Documentation!

Introduction

This manual will help you get the best out of the Celiveo solution as quickly as possible!
It covers the functionalities of Celiveo to provide you with information about installing, configuring and using our solution.

Terms and Acronyms

This section lists the standard terminology used in Celiveo.

Acronym	Full-Form	Definition
CSS	Celiveo Server Services	The central authentication and print server.
CRL	Certificate Revocation List	An access control method to a server in a public network. It contains a list of subscribers with their digital certificate status. Includes the list of revoked certificates, reason for revocation, date of certificate issue, who issued them. The server allows or denies access based on the CRL entry for the particular user. Source: http://searchsecurity.techtarget.com/definition/Certificate-Revocation-List
CSV	Comma Separated Values	This file stores tabular data in plain-text form.
DHCP	Dynamic Host Communication Protocol	A networking protocol to automatically distribute IP address to computers from a server
MAC	Media Access Control	Provides address and access for communication among terminals and network nodes
TCP-IP	Transmission Control Protocol-Internet Protocol	The core protocol of the Internet protocol suite.
LAN	Local Area Network	A computer network within a limited area, such as a small office building.

SNMP	Simple Network Management Protocol	A protocol to manage devices on IP networks, usually supported by devices, such as printers, routers, switches, and so on.
EWS	Embedded Web Service	Web portal to access an HP printing device.

Special Text Icons

This section lists the icons used in the document to indicate that the information corresponds to a particular Celiveo edition or is related to a special feature.

Icon	Meaning
PD	Print-Direct Edition
B	Business Edition
B+	Business + Edition
E	Enterprise Edition
P	Premium Edition
PS	Public Sector Connector
FSI	Financial Services Industry Connector
O&G	Oil & Gas Connector
SAP	SAP Connector
SM	Stealth Mode Feature
LFP	Large Format Printers (LFP)
C	Cloud

Last modified: 5 October 2022

2. Legal Information

Last modified: 29 September 2022

2.1. EULA for Celiveo 8

©2011 – 2021 Celiveo Pte Ltd. All rights reserved.
Parts under license from Jetmobile Pte Ltd
Protected by US patent number: 6,889,252
Protected by Singapore patent number: 104066
Protected by Australian patent number: 2002350998

Reproduction, adaptation, or translation without prior written permission is prohibited except as allowed under the copyright laws. The information contained herein is subject to change without notice.

The only warranties for Celiveo products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Jetmobile Pte Ltd and Celiveo Pte Ltd shall not be liable for technical or editorial errors or omissions contained herein.

Device and printer interfaces use technology developed by Jetmobile Pte Ltd and technology under license from Fuji Xerox, HP Inc, Konica Minolta, Lexmark, Ricoh and Xerox. Jetmobile Pte Ltd and our licensors control all intellectual property and copyrights in this product.

Trademark Credits:
Celiveo is a registered trademark of Jetmobile Pte Ltd.
All other marks are the property of their respective owners.
Revision – 01/2021

PLEASE READ CAREFULLY BEFORE USING THIS SOFTWARE PRODUCT: This End-User License Agreement (“EULA”) is a contract between (a) you (either an individual or the entity you represent) and (b) Celiveo Pte Ltd (“CELIVEO”) that governs your use of the software product (“Software”).

This EULA does not apply if there is a separate license agreement between you and CELIVEO for the Software, including a license agreement in online documentation. The term “Software” may include (i) associated media, (ii) a user guide and other printed materials, and (iii) “online” or electronic documentation (collectively “User Documentation”).

RIGHTS IN THE SOFTWARE ARE OFFERED ONLY ON THE CONDITION THAT YOU AGREE TO ALL TERMS AND CONDITIONS OF THIS EULA. BY INSTALLING, COPYING, DOWNLOADING, OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THIS EULA. IF YOU DO NOT ACCEPT THIS EULA, DO NOT INSTALL, DOWNLOAD, OR OTHERWISE USE THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE BUT DO NOT AGREE TO THIS EULA, PLEASE RETURN THE SOFTWARE TO YOUR PLACE OF PURCHASE WITHIN FOURTEEN DAYS FOR A REFUND OF THE PURCHASE PRICE; IF THE SOFTWARE IS INSTALLED ON OR MADE AVAILABLE WITH ANOTHER CELIVEO PRODUCT, YOU MAY RETURN THE ENTIRE UNUSED PRODUCT.
1. THIRD PARTY SOFTWARE. The Software may include, in addition to CELIVEO proprietary software (“CELIVEO Software”), software under licenses from third parties (“Third Party Software” and “Third Party License”). Any Third-Party Software is licensed to you subject to the terms and conditions of the corresponding Third Party License indicated in the documentation. If the Third Party Licenses include

licenses that provide for the availability of source code (such as the GNU Limited General Public License) and the corresponding source code is not included with the Software, then check the knowledge pages of CELIVEO's website (www.celiveo.com) to learn how to obtain such source code.
2. LICENSE RIGHTS. You will have the following rights provided you comply with all terms and conditions of this EULA:
a. Use. CELIVEO grants you a license to Use one copy of the CELIVEO Software. "Use" means installing, copying, storing, loading, executing, displaying, or otherwise using the CELIVEO Software. You may not modify the CELIVEO Software or disable any licensing or control feature of the CELIVEO Software. If this Software is provided by CELIVEO for Use with a specific model of imaging or printing product (for example, if the Software is a printer driver, firmware, or add-on), the CELIVEO Software may only be used with such product and model. Additional restrictions on Use may appear in the User Documentation. You may not separate component parts of the CELIVEO Software for Use. You do not have the right to distribute the CELIVEO Software.
b. Copying. Your right to copy means you may make archival or back-up copies of the CELIVEO Software, provided each copy contains all the original CELIVEO Software's proprietary notices and is used only for back-up purposes.
3. The CELIVEO Software is not licensed for Commercial Use under this End User License Agreement. Unless you obtain a Commercial License from CELIVEO you may not redistribute the CELIVEO software to third parties, bundle the CELIVEO software in products intended for resale, or use the CELIVEO Software to generate revenue by renting it, providing third party management, support or consulting services related to printers, printer supplies or other devices.
4. MAINTENANCE AND SUPPORT. No maintenance or support service is included in this End-User License Agreement for the CELIVEO Software. Such a service may be purchased from CELIVEO or a CELIVEO reseller as a separate Maintenance and Support Agreement.
5. UPGRADES. To Use CELIVEO Software provided by CELIVEO as an upgrade, update, or supplement (collectively "Upgrade"), you must first be licensed for the original CELIVEO Software identified by CELIVEO as eligible for the Upgrade, then have a valid support and maintenance contract from CELIVEO. To the extent the Upgrade supersedes the original CELIVEO Software, you may no longer use such CELIVEO Software. This EULA applies to each Upgrade unless CELIVEO provides other terms with the Upgrade. In case of a conflict between this EULA and such other terms, the other terms will prevail.
6. TRANSFER.
a. Third Party Transfer. The initial owner of the CELIVEO Software may perform a one-time transfer of the CELIVEO Software to another end user within the world region where the original purchase happened: North America, Latin America, Europe, Middle East/Africa, Australia/New Zealand or Asia. This transfer may happen if and only if the solution has not been used before that transfer as it is authorized exclusively to allow resellers to transfer license rights easily.
b. Any transfer will include all component parts, media, User Documentation, this EULA, and if applicable, the Certificate of Authenticity. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the transferred Software will agree to this EULA. Upon transfer of the CELIVEO Software, your license is automatically terminated.
c. Restrictions. You may not rent, lease or lend the CELIVEO Software or Use the CELIVEO Software for commercial timesharing or bureau use.
You may not sublicense, assign or otherwise transfer the CELIVEO Software except as expressly provided in this EULA.
7. PROPRIETARY RIGHTS. All intellectual property rights in the Software and User Documentation are owned by CELIVEO or its suppliers and are protected by law, including applicable copyright, trade secret, patent, and trademark laws. You will not remove any product identification, copyright notice, or

proprietary restriction from the Software.
8. LIMITATION ON REVERSE ENGINEERING. You may not reverse engineer, decompile, or disassemble the CELIVEO Software, except and only to the extent that the right to do so is allowed under applicable law.
9. CONSENT TO USE OF DATA. CELIVEO and its affiliates may collect and use technical information you provide in relation to (i) your Use of the Software, or (ii) the provision of support services related to the Software.
All such information will be subject to CELIVEO's privacy policy.
CELIVEO will not use such information in a form that personally identifies you except to the extent necessary to enhance your Use or provide support services.
10. LIMITED WARRANTY. To the original purchaser, CELIVEO warrants the Software part loaded on the product and provided separately for ninety (90) days from the date the Product is delivered. If during this period a defect in the Software should occur, after written confirmation by CELIVEO or its distributor of the defective status, you may return the product with a copy of your receipt or other proof of payment to an authorized CELIVEO distributor, and CELIVEO will replace the Software without charge. Your sole and exclusive remedy in the event of a defect is expressly limited to a repair or replacement of the part as provided above.
CELIVEO warrants all Celiveo hardware components to be free from defects and will-at this option-repair or replace any hardware part of the product should it fail within one year from the first date of shipment. This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse or unauthorized modification. If the hardware parts of the product fail or does not perform as warranted, your sole recourse shall be repair or replacement as described above.
CELIVEO does not warrant that the functions contained in this Product will meet your requirements that the Product operation will be uninterrupted or error free or that breach of security will never occur, or that the CELIVEO Software or hardware does not infringe any third party rights.
Information contained in the user manual is subject to change without notice and does not represent a commitment on the part of CELIVEO.
FOR PRODUCTS DELIVERED IN AUSTRALIA: Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.
11. LIMITATION OF LIABILITY. Notwithstanding any damages that you might incur, the entire liability of CELIVEO and its suppliers under this EULA and your exclusive remedy under this EULA will be limited to the greater of the amount actually paid by you for the Product divided by the numbers of years it has been used by you or US$5.00. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL CELIVEO OR ANYONE ELSE WHO HAS BEEN INVOLVED DIRECTLY OR INDIRECTLY IN THE CREATION, PRODUCTION OR DELIVERY OF THIS PRODUCT BE LIABLE TO YOU FOR ANY DIRECT OR INDIRECT DAMAGES INCURRED BY THE USE OF THIS PRODUCT.
THESE DAMAGES INCLUDE, BUT ARE NOT LIMITED TO, THE FOLLOWING:
LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THIS PRODUCT, OR FOR ANY CLAIM BY ANY OTHER PARTY, RELATED OR NOT TO INFRINGEMENT. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT AND MANUAL IS ASSUMED BY YOU. THE SOLE AND EXCLUSIVE LIABILITY OF CELIVEO, REGARDLESS OF THE FORM OF ACTION, WILL NOT EXCEED THE PAYMENTS MADE FOR THIS LICENSE. ANY REMEDIES SPECIFIED IN THIS LICENSE AGREEMENT ARE EXCLUSIVE. To the extent permissible, any implied warranty is limited to ninety days from purchase date. Some countries, states or other jurisdictions do not allow the exclusion or

limitation of incidental or consequential damages, in such case the above limitation or exclusion may not fully apply to you.
CELIVEO products are not suitable for use in life-support applications, biological hazard applications, nuclear control applications, or radioactive areas. You understand and agree that none of CELIVEO products or components, software or hardware, are intended for applications that provide life support or any critical function necessary for the support of protection of life, property or business interests.
12. U.S. GOVERNMENT CUSTOMERS. If you are a U.S. Government entity, then consistent with FAR 12.211 and FAR 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed under the applicable CELIVEO commercial license agreement.
13. COMPLIANCE WITH EXPORT LAWS. You acknowledge that the licensed Software, Hardware and related Documentation delivered to you under this Agreement are subject to Singapore and European Union export control laws and regulations, and may also be subject to the jurisdiction in which it was obtained, if outside of Singapore or the European Union. You agree to comply with all applicable export control laws, rules and regulations applicable to the Software, Hardware and Documentation. You specifically agree that You will not export, re-export, or transfer the Software, Hardware or Documentation, in whole or in part, to any country, person, or entity subject to Singapore or European Union export restrictions. You will not, without government authorization, export, re-export or transfer the Software, Hardware or Documentation (i) to any country to which Singapore or the European Union has embargoed or restricted the export of goods or services, or to any national of any such country, wherever located, who intends to transmit or transport the products back to such country; (ii) to any end-user whom You know or have reason to know, will utilize them in the design, development, production or use of nuclear, chemical or biological materials, facilities, or weapons.
14. RESERVATION OF RIGHTS. CELIVEO and its suppliers reserve all rights not expressly granted to you in this EULA.
15. This agreement shall be constructed, interpreted and governed by the laws of Singapore. You agree that this is the complete and exclusive statement of this agreement which supersedes any prior agreement or other communication between us on this subject.

© 2011 – 2021 Celiveo Pte Ltd
Revision 01/2021

Last modified: 29 September 2022

2.2. Terms of Service for Celiveo SaaS Services

Last Updated: August 23, 2021

We, at Celiveo, are on a mission to make Documents management easier, safer and possible wherever your work. We hope you love our products and services — from print jobs encryption over the network to user authentication on printers and high-security SaaS pull print as a plugin to Microsoft 365.
These Terms of Service (“Terms”) describe our commitments to you, and your rights and responsibilities when using our services. Please read them carefully and reach out to us if you have any questions.
Terms of Service
These Terms govern your access to and use of the products and services we provide through the Celiveo.me mobile extension and Celiveo 365 SaaS secure printing (collectively, “Services”).
These Terms also govern visitors’ access to and use of any websites that present our products and services, like the www.celiveo.com, support.celiveo.com or portal.celiveo.com websites.
For some of the Celiveo other products, services, and programs, such as the Celiveo Silver Partner program and the Celiveo Gold Partner program, additional or separate terms may apply.
Please read these Terms carefully before accessing or using our Services. By accessing or using any part of our Services, you agree to be bound by all of the Terms and all other operating rules, policies, and procedures that we may publish via the Services from time to time (collectively, the “Agreement”). You also agree that we may automatically change, update, or add on to our Services, and this Agreement will apply to any changes.
1. Who’s Who
“You” means any individual or entity using our Services. If you use our Services on behalf of another person or entity, you represent and warrant that you’re authorized to accept the Agreement on that person’s or entity’s behalf, that by using our Services you’re accepting the Agreement on behalf of that person or entity, and that if you, or that person or entity, violates the Agreement, you and that person or entity agree to be responsible to us.
Celiveo
• Celiveo Pte Ltd, 1 Goldhill Plaza #03-39, Singapore 308899
We refer to Celiveo as “Celiveo” or “we” throughout these Terms.
2. Your Account
When using our Services requires an account, you agree to provide us with complete and accurate information and to keep the information current so that we can communicate with you about your account. We may need to send you emails about notable updates (like changes to our Terms of Service or Privacy Policy), or to let you know about legal inquiries or complaints we receive about the ways you use our Services so you can make informed choices in response.
We may limit your access to our Services until we’re able to verify your account information, like your email address.
When you create an account on any of our websites and Services, we consider that to be an inquiry about our products and services, which means that we may also contact you to share more details about what we have to offer (i.e., marketing). Don’t worry — if you aren’t interested, you can opt out of the marketing communications, whether it’s an email, phone call, or text message.
You’re solely responsible and liable for all activity under your account. You’re also fully responsible for maintaining the security of your account (which includes keeping your password secure). We’re not liable for any acts or omissions by you, including any damages of any kind incurred as a result of your acts or

omissions.
Don’t share or misuse your access credentials. And notify us immediately of any unauthorized uses of your account or of any other breach of security. If we believe your account has been compromised, we may suspend or disable it.
If you’d like to learn about how we handle the data you provide us, please see our Privacy Policy in that contract.
3. Minimum Age Requirements
Our Services are not directed to children. You’re not allowed to access or use our Services if you’re under the age of 13 (or 16 in Europe). If you register as a user or otherwise use our Services, you represent that you’re at least 13 (or 16 in Europe). You may use our Services only if you can legally form a binding contract with us. In other words, if you’re under 18 years of age (or the legal age of the majority where you live), you can only use our Services under the supervision of a parent or legal guardian who agrees to the Agreement.
4. Responsibility of Visitors and Users
We can’t review any of the documents made available through our Services from your accounts (“Content”). We’re not responsible for any use or effects of Content.
So, for example:
• We don’t have any control over Content.
• We don’t endorse any Content or represent that Content is accurate, useful, or not harmful. Content could be offensive, indecent, or objectionable; include technical inaccuracies, typographical mistakes, or other errors; or violate or infringe the privacy, publicity rights, intellectual property rights, or other proprietary rights of third parties.
• You’re fully responsible for the Content and any harm resulting from that Content. It’s your responsibility to ensure that your Content abides by applicable laws and by the Agreement.
• We aren’t responsible for any harm resulting from anyone’s access, use of Content, or our Services. You’re responsible for taking the necessary precautions to protect yourself and your computer systems from viruses, worms, Trojan horses, and other harmful or destructive content.
Please note that additional third-party terms and conditions may apply to the Services you use.
5. Fees, Payment, and Renewal
a. Celiveo Fees
Fees for Paid Services. Some of our Services are offered for a fee, Celiveo.me, Celiveo 365 Business Edition or Celiveo 365 Enterprise Edition (collectively, “Paid Services”). By using a Paid Service, you agree to pay the specified fees. Depending on the Paid Service, there may be one-time fees, recurring fees, or usage-based fees. For recurring fees, we’ll bill or charge you in the automatically-renewing interval (such as monthly, annually, or biennially) you select, on a pre-pay basis until you cancel, which you can do at any time by contacting the relevant support team. For usage-based fees, you pay us based on your actual usage of our Services for the past month or quarter, as applicable based on the contract.
Taxes. To the extent permitted by law, or unless explicitly stated otherwise during the ordering process, all prices do not include applicable federal, provincial, state, local, or other governmental sales, value-added, goods and services, harmonized or other taxes, fees, or charges (“Taxes”). You’re responsible for paying all applicable taxes relating to your use of our Services, your payments, or your purchases. If we’re obligated to pay or collect Taxes on the fees you’ve paid or will pay, you’re responsible for those Taxes, and we may collect payment.
Payment. If your payment fails, Paid Services are otherwise not paid for or paid for on time (for example, if you contact your bank or credit card company to decline or reverse the charge of fees for Paid Services), or we suspect a payment is fraudulent, we may immediately cancel or revoke your access to Paid Services without notice to you.

Automatic Renewal. To ensure uninterrupted service, recurring Paid Services are automatically renewed. This means that unless you cancel a Paid Service before the end of the applicable subscription period, it will automatically renew, and you authorize us to use any payment mechanism we have on record for you, like credit cards or PayPal, or invoice you (in which case payment is due within 15 days) to collect the then-applicable subscription fee as well as any Taxes. By default, your Paid Services will be renewed for the same interval as your original subscription period, so for example, if you purchase a one-year subscription to a Celiveo 365 Business Edition plan, you'll be charged each year for access for another 12-month period with similar subscription parameters. We may charge your account up to two weeks before the end of the subscription period to make sure pesky billing issues don't inadvertently disrupt your access to our Services. The date for the automatic renewal is based on the date of the original purchase and cannot be changed. If you've purchased access to multiple services, you may have multiple renewal dates.

You can view your renewal date(s) and manage subscriptions for Celiveo Paid Services by visiting the license page in your Celiveo Web Admin portal. For more information about how Celiveo Services subscriptions work, please see our support pages on support.celiveo.com.

You'll need to check your email (including in spam or other filters) for any reminder emails we might send you before your Paid Services renew, they are from `celiveo.com`, celiveo.cloud or @celiveo.me.

Amending the Service details or canceling Automatic Renewal. You can manage and cancel your Paid Services on the Celiveo Web Admin portal, click on the plan you want to amend (i.e. adding extra users), or cancel then follow the instructions to change the number of users, cancel the subscription or turn off auto-renew.

If auto-renew is successfully turned off, you'll see the date on which your subscription expires. If you have multiple Paid Services to cancel, repeat this process for each subscription.

Fees and Charges. We may change our fees at any time in accordance with these Terms and requirements under applicable law. This means that we may change our fees going forward, start charging fees for Services that were previously free, or remove or update features or functionality that were previously included in the fees, with a 90 days notice. If you don't agree with the changes, you must cancel your Paid Service.

Refunds. There are no refunds and all payments are final.

6. Feedback

We love hearing from you and are always looking to improve our Services. When you share comments, ideas, or feedback with us, you agree that we're free to use them without any restriction or compensation to you.

7. General Representation and Warranty

Our mission is to make documents management a better and safer place, and our Services are designed to give you control and ownership over your documents. We encourage you to express yourself freely, subject to a few requirements. In particular, you represent and warrant that your use of our Services:

• Will be in strict accordance with the Agreement;

• Will comply with all applicable laws and regulations (including, without limitation, all applicable laws regarding online conduct and acceptable content, privacy, data protection, the transmission of technical data exported from the United States or the country in which you reside);

• Will not be for any unlawful purposes ;

• Will not infringe or misappropriate the intellectual property rights of Celiveo or any third party;

• Will not overburden or interfere with our systems or impose an unreasonable or disproportionately large load on our infrastructure, as determined by us in our sole discretion;

• Will not disclose the personal information of others;

• Will not involve reverse engineering, decompiling, disassembling, deciphering, or otherwise attempting

to derive the source code for the Services or any related technology that is not open source; and
• Will not involve renting, leasing, loaning, selling, or reselling the Services or related data without our consent.

8. Specific Service Terms

Datacenters. Celiveo uses Microsoft datacenters for its SaaS Services, in multiple regions to comply with main Privacy regulations such as EU GDPR. The datacenter location can be selected during the subscription of the Services from a list of available locations.

It is your exclusive responsibility to select among the Datacenters proposed for Celiveo Services, the location that meets your legal and strategic requirements. Should none of the proposed Datacenter locations meet your requirement, please contact Celiveo through the web portal www.celiveo.com with more information so that we investigate how we can improve the coverage in the future.

Encryption. Documents transmitted by Celiveo benefit from a dual encryption using dynamic and dual-factor keys then using TLS 1.2 or 1.3. Celiveo does not keep the encryption keys for your documents it encrypts.

Zero Trust Access and Certificates. All communication and Services are protected by a Certificate forest built for your account. Each certificate is unique for each node used by the Service, even those present in your company, and Celiveo does not have the private keys for those certificates.

Performances. All the Services communication to the Cloud goes through the Public Internet and directly relies on the quality of your link to the Internet, the speed between your Internet access point and the selected Microsoft Azure Datacenter, and the size of your documents. Celiveo, therefore, declines any liability regarding any performance issue, real or not, reported during the usage of the Services.

Integration with your Microsoft 365 account. By subscribing to the Services, you authorize us to interface those Services, in read-only mode, to your Microsoft 365 account for the following purposes:
• Authenticate the end-users of your company, read their profile in Azure Active Directory to grant them access to the Service
• Collect print jobs sent by those users through Microsoft 365 to list, encrypt and store them pending their release on a printer.
• Install a software module on the Internet browser of print administrators to allow them to discover corporate printers on the network and deploy Celiveo on them.

Confidentiality, GDPR. Celiveo does not keep any personal information about users on its system databases besides those needed for technical contacts and for billing matters. User information is replaced by a hash of that information in system logs to ensure there is no possible information leak. The only information kept about users is related to billing, to document the Service usage charge. You can opt-in to anonymize that information on the Celiveo Web Admin portal, then you waive your right to request from Celiveo the detailed information on the users of your account who are using or have been using Celiveo Services.

9. Intellectual Property

The Agreement doesn’t transfer any Celiveo or third-party intellectual property to you, and all right, title, and interest in and to such property remains (as between Celiveo and you) solely with Celiveo. Celiveo, Jetmobile, SecureJet, and all other trademarks, service marks, graphics, and logos used in connection with our websites or Services are trademarks or registered trademarks of Celiveo (or Celiveo’s licensors). Other trademarks, service marks, graphics, and logos used in connection with our Services may be the trademarks of other third parties. Using our Services doesn’t grant you any right or license to reproduce or otherwise use any Celiveo or third-party trademarks.

10. Third-Party Services and Products

While using the Services, you may enable, use, or purchase services, products, software, hardware, drivers, or applications developed by a third party or yourself (“Third-Party Services”) in Microsoft Windows, macOS, Android, iOS, Linux, Microsoft 365 or in Microsoft Azure or any other Cloud.

If you use any such Third-Party Services in conjunction with Celiveo Services, you understand that:
• Third-Party Services aren't vetted, endorsed, or controlled by Celiveo.
• Any use of a Third-Party Service is at your own risk, and we won't be responsible or liable to anyone for Third-Party Services.
• Your use is solely between you and the respective third party ("Third Party") and is governed by the Third Party's terms and policies.
• Some Third-Party Services may request or require access to your data — or to your users' data. If you use the Third-Party Service or grant them access, the data will be handled in accordance with the Third Party's privacy policy and practices, which you should carefully review before you use any Third-Party Services. Third-Party Services may not work appropriately with our Services and we may not be able to provide support for issues caused by any Third-Party Services.
• If you have questions or concerns about how a Third-Party Service operates or need support, contact the Third Party directly.
If you subscribe to Google Chrome Enterprise Services, there are a few other things we want to highlight: these services are provided by Google, and your use of them is subject to Google's Terms of Use for the services, which you'll accept before using them. We make no warranties about Google's services, and decline any liability related to the usage, or non-usage, of their services. Google will provide technical support for its services, per its Technical Support Services Guidelines.
11. Changes
We may update, change, or discontinue any aspect of our Services at any time with a 90 days prior notice. Since we're constantly updating our Services, we sometimes have to change the legal terms under which they're offered. The Agreement may only be modified by a written amendment signed by an authorized executive of Celiveo, or if Celiveo posts a revised version. We'll let you know when there are changes, by sending send you an email to your billing contact 90 days before the changes become effective. Your continued use of our Services after the new terms take effect will be subject to the new terms, so if you disagree with the changes in the new terms, you should stop using our Services. To the extent you have an existing subscription, you may be eligible for a prorated refund.
12. Termination
We may terminate your access to all or any part of our Services at any time, with or without notice, effective immediately if you have unpaid Service subscription invoices. We will have no obligation to provide a refund of any fees previously paid.
You can cancel at any time the automatic renewal of your Service subscription, subject to the Fees, Payment, and Renewal section of these Terms.
13. Disclaimers
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE", WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND CELIVEO, ITS LICENSORS, AND DISTRIBUTORS (COLLECTIVELY REFERRED TO AS "CELIVEO" FOR THE REST OF THIS SECTION 13) HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE SERVICES, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.
CELIVEO DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SERVICES WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF
THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, THAT ANY SERVICE WILL CONTINUE TO BE MADE AVAILABLE, THAT ALL DEFECTS IN THE SERVICES WILL BE CORRECTED, OR THAT THE SERVICE WILL BE COMPATIBLE OR WORK WITH ANY THIRD-PARTY SOFTWARE, APPLICATIONS OR THIRD-PARTY SERVICES.

YOU ACKNOWLEDGE THAT THE SERVICES ARE NOT INTENDED FOR CONSUMERS AND ONLY INTENDED FOR CORPORATIONS, COMPANIES, NON-PROFIT AND PUBLIC SERVICES, AND THAT CONSUMER PROTECTION RIGHT DOES NOT APPLY TO THEIR SUBSCRIPTION.
YOU FURTHER ACKNOWLEDGE THAT THE SERVICES ARE NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE THE FAILURE OR TIME DELAYS OF, OR ERRORS OR INACCURACIES IN, THE CONTENT, DATA, OR INFORMATION PROVIDED BY THE SERVICES COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE, INCLUDING WITHOUT LIMITATION THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT OR WEAPONS SYSTEMS.
NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY CELIVEO OR A CELIVEO AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE SERVICES PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION TO THE EXCEPTION OF FIX IN THE SERVICES.
LIMITATION OF LIABILITY: TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT SHALL CELIVEO, ITS AFFILIATES, AGENTS, OR PRINCIPALS BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, CORRUPTION OR LOSS OF DATA, FAILURE TO TRANSMIT OR RECEIVE ANY DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE SERVICES OR ANY THIRD-PARTY SOFTWARE, APPLICATIONS OR SERVICES IN CONJUNCTION WITH THE SERVICES, HOWEVER, CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF CELIVEO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL CELIVEO TOTAL LIABILITY TO YOU FOR ALL DAMAGES EXCEED THE AMOUNT OF FIFTY AMERICAN DOLLARS (US$50.00).

14. Jurisdiction and Applicable Law.

Except to the extent any applicable law provides otherwise, the Agreement and any access to or use of our Services will be governed by the laws of Singapore. The proper venue for any disputes arising out of or relating to the Agreement and any access to or use of our Services will be the courts of Singapore.

15. Limitation of Liability

In no event will Celiveo, or its suppliers, partners, or licensors, be liable with respect to any subject matter of the Agreement under any contract, negligence, strict liability or other legal or equitable theory for: (i) any special, incidental or consequential damages; (ii) the cost of procurement for substitute products or services; (iii) for interruption of use or loss or corruption of data; or (iv) for any amounts that exceed $50. Celiveo shall have no liability for any failure or delay due to matters beyond its reasonable control. The foregoing shall not apply to the extent prohibited by applicable law.

16. US Economic Sanctions

You may not use the Services if such use is inconsistent with U.S. sanctions law or if you are on any list maintained by a U.S. government authority relating to designated, restricted, or prohibited persons.

17. Translation

These Terms were originally written in English (US). We may translate these terms into other languages, and in the event of a conflict between a translated version of these Terms and the English version, the English version will prevail.

18. Miscellaneous

The Agreement (together with any other terms we provide that apply to any specific Service) constitutes the entire agreement between Celiveo and you concerning our Services. If any part of the Agreement is unlawful, void, or unenforceable, that part is severable from the Agreement, and does not affect the

validity or enforceability of the rest of the Agreement. A waiver by either party of any term or condition of the Agreement or any breach thereof, in any one instance, will not waive such term or condition or any subsequent breach thereof.
Celiveo may assign its rights under the Agreement without condition. You may only assign your rights under the Agreement with our prior written consent.

Last modified: 29 September 2022

3. Architecture Overview

Celiveo provides the following independent features to protect your print job information:

Print Job Retention

Server-based Pull Printing

Serverless Pull Printing

Print Job Encryption

Last modified: 29 September 2022

3.1. Print Job Retention

Print job retention and controlled release ensure that the printed documents reach the hands of the authorized personnel only.
Celiveo provides three ways to perform print job retention:

- Push Printing
- Server-based Pull Printing
- Serverless Pull Printing

Push Printing

In Push Printing, jobs are sent to the device for authentication and release. Push Printing is convenient as it makes a powerful serverless secure printing solution. On the other hand, the limited hard disk drive capacity on a device can be an issue as compared to that of a server, if large jobs are to be retained. The print jobs can also be released only from the device where they are stored.

> ! Push Printing is supported on HP devices with a hard disk drive and minimum disk space of 30GB. The Push Printing feature is not supported on CM8050 and CM8060 multi-function printers. Printers must have storage media (HDD, USB stick) with 50MB free, and an active TCP-IP LAN connection.

Last modified: 29 September 2022

3.2. Server-based Pull Printing

Server-based Pull Printing occurs when a print job is stored on a designated server until a user authenticates at a Celiveo-enabled device, and pulls the selected job from the server to the printer. Retention on print servers require more configuration but is more scalable.

The Server-based Pull Printing architecture involves the central print server for user authentication, job listing, and release. Print jobs are retained on the hard disk drive of Celiveo Server Services for later release from any Celiveo-enabled printing device upon user authentication.

> ! The storage capacity is configurable and a user or a department can be allocated up to 100 print jobs or 25 MB, depending upon the capacity of the hard disk drive on the server.

Last modified: 29 September 2022

3.3. Serverless Pull Printing

In Serverless Pull Printing, a print job is stored on the client machine until a user authenticates at a Celiveo-enabled device, and pulls the selected job from the client machine to the printer. Serverless Pull Printing reduces the load on the central Print Server (central Celiveo Server Services) by moving all the job-processing activities from the server machine to the client machine, and by caching the client machine details on device storage media (hard disk, USB, Compact Flash). With this implementation, the user is not entirely dependent on the Celiveo Server Services for authentication, or for print job listing.

Serverless Pull Printing makes use of the authentication cache and the Pull Printing directory cache on the device. The central Celiveo Server Services acts as the authentication and printing server for the first user session. In the subsequent user sessions, the Serverless Pull Printing architecture uses the Authentication
cache as a failover mechanism to authenticate users (if the central Celiveo Server Services or the Direct LDAP/AD server is down) and the Pull Printing Directory cache is used as the primary mechanism for retrieval of the print job from the last used client machine.

The authentication cache stores the user details after the first successful authentication through Celiveo Server Services or through the Direct LDAP/AD profile. The device looks up user details from the authentication cache for user authentication if Secure Server Services or the Direct LDAP/AD server is down in the subsequent user sessions.

After the first session, the print job is retrieved using the IP address of the client machine, which is stored in the Pull Printing Directory cache. The print jobs are retrieved from the client machines running the Serverless Pull Printing client software.

> The authentication cache and the Pull Printing Directory cache options can be enabled from the Celiveo Web Admin Software.

Benefits of Serverless Pull Printing

Serverless Pull Printing reduces the load on Celiveo Server Services (CSS) by diverting the job processing load on to the client machines, providing a seamless printing experience:

- The user can be authenticated on the device even when Celiveo Server Services goes down.
- The user can print jobs, even if the database server that stores print job details is unavailable.
- The user can be authenticated on the device and can print jobs, even when both Celiveo Server Services and the database server are down.

Last modified: 29 September 2022

3.4. Print Job Encryption

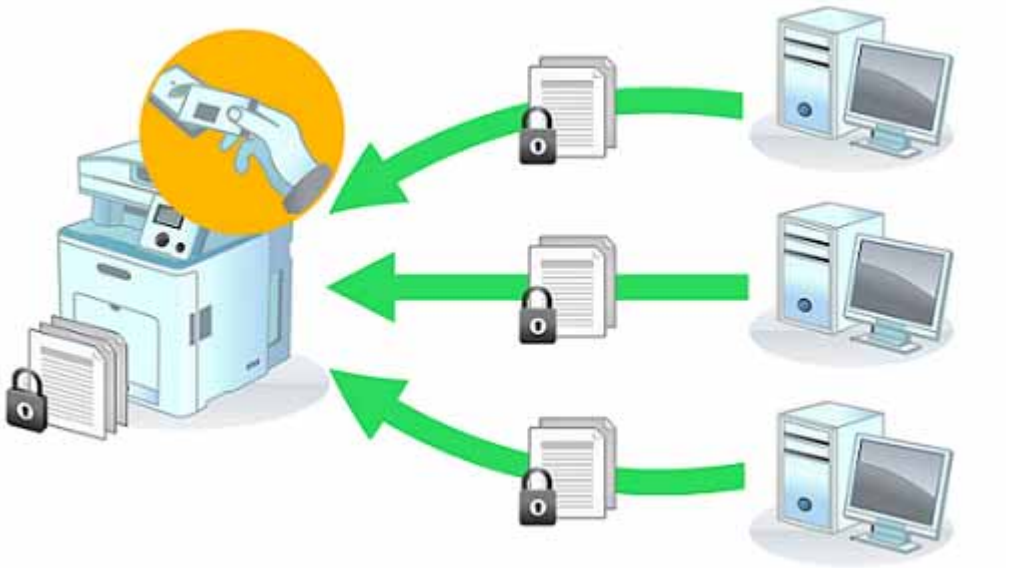
Print job encryption ensures that no one sees or alters the print job data. The following encryption actions are available:

- Job encryption only
- Control of job release only
- Job encryption and control of job release

Sample configurations of encryption

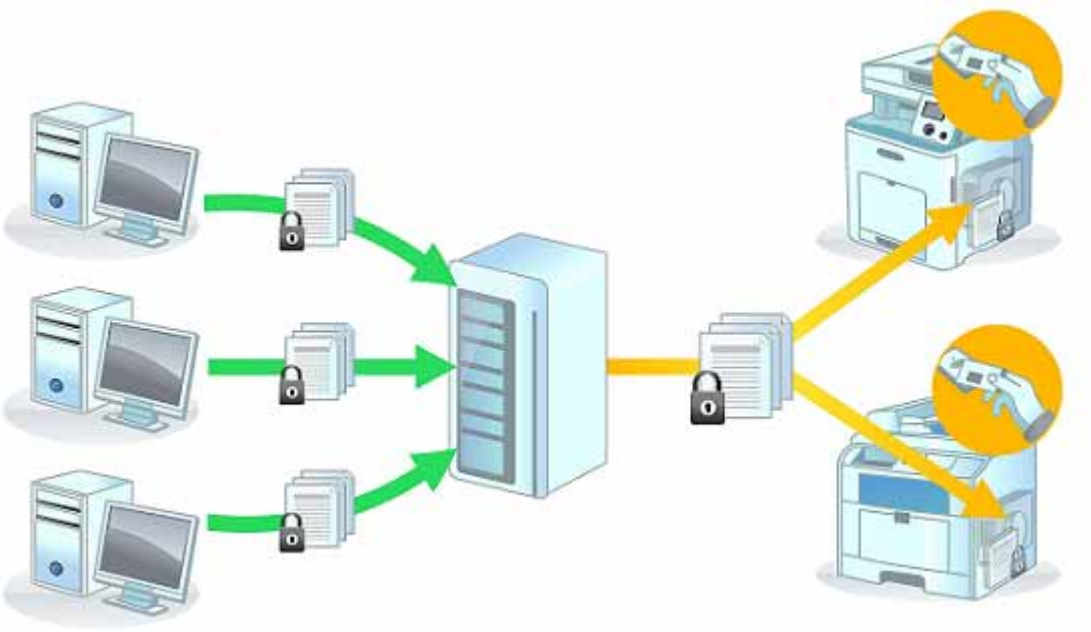
Jobs must be processed by the Celiveo plug-in, and need to be accepted by Celiveo. The Celiveo plug-in can be installed either on the client PCs, or on the print server.

Direct Printing to device with Celiveo Plug-in Installed on Client Machine



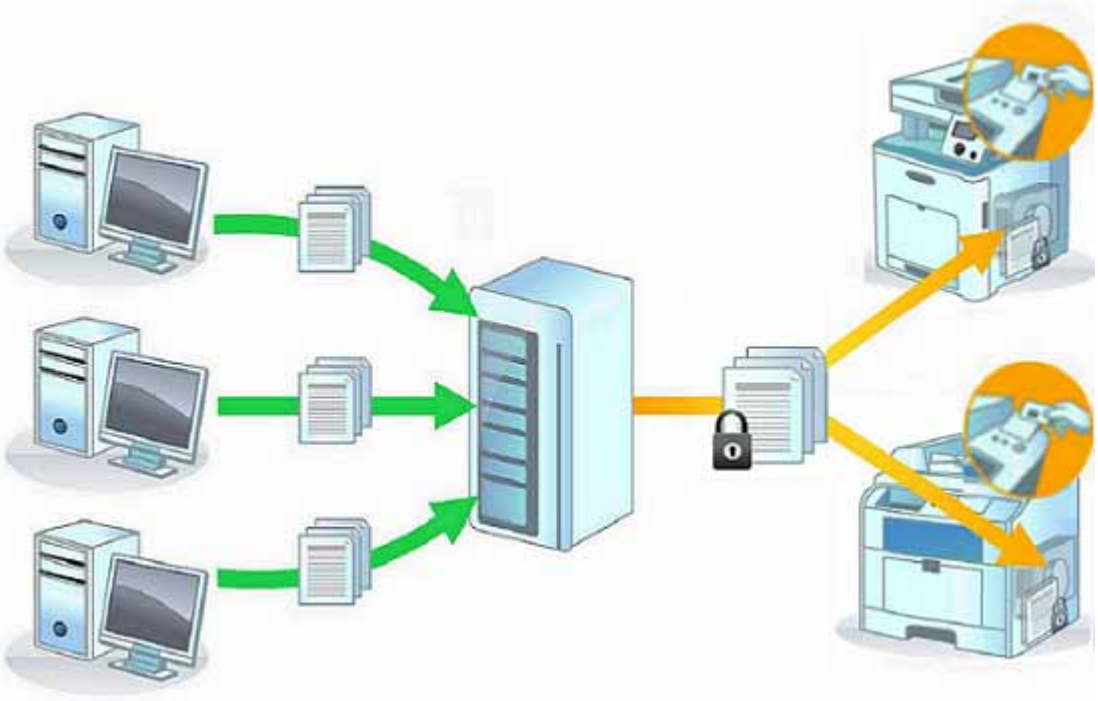
- Jobs are encrypted from the client machine to the device.
- Jobs are retained on the hard disk drive of the printing device for release upon authentication.

Server-Based Printing with Celiveo Plug-in installed on the Client Machine



- Jobs are encrypted all the way from the client machines to the device through the print server.
- Jobs are retained on the hard disk drive of the printing device for release upon authentication.

Server-Based Printing with Celiveo Plug-in installed on the Print Server

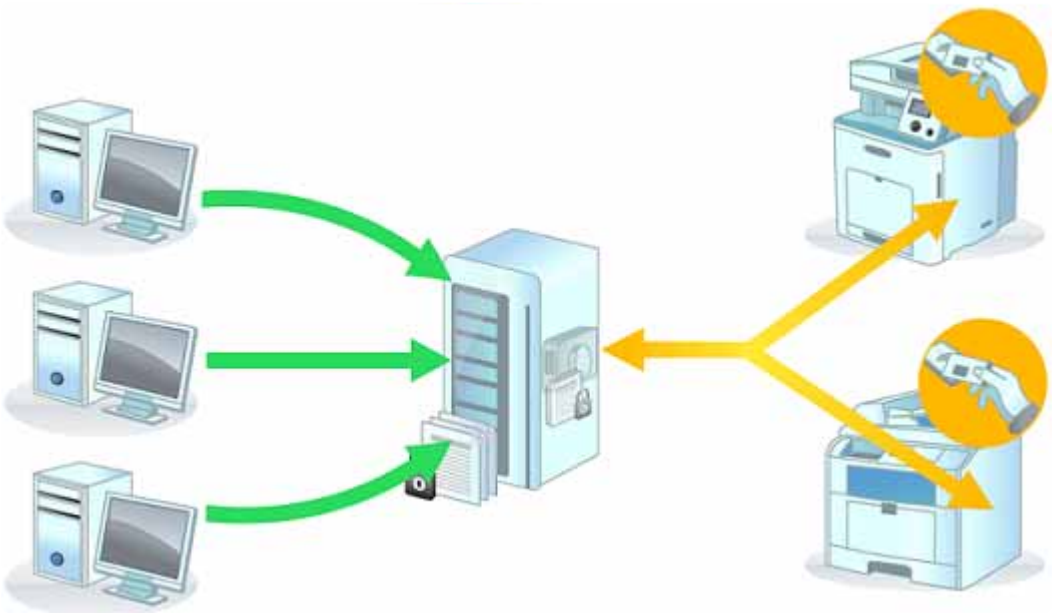


- Jobs are encrypted from the server print queue to the device.
- Jobs are retained on the hard disk drive of the printing device for release upon authentication.

Server-Based Pull Printing with Celiveo Driver Plug-in installed on the Client machine and Celiveo installed on the Print Server

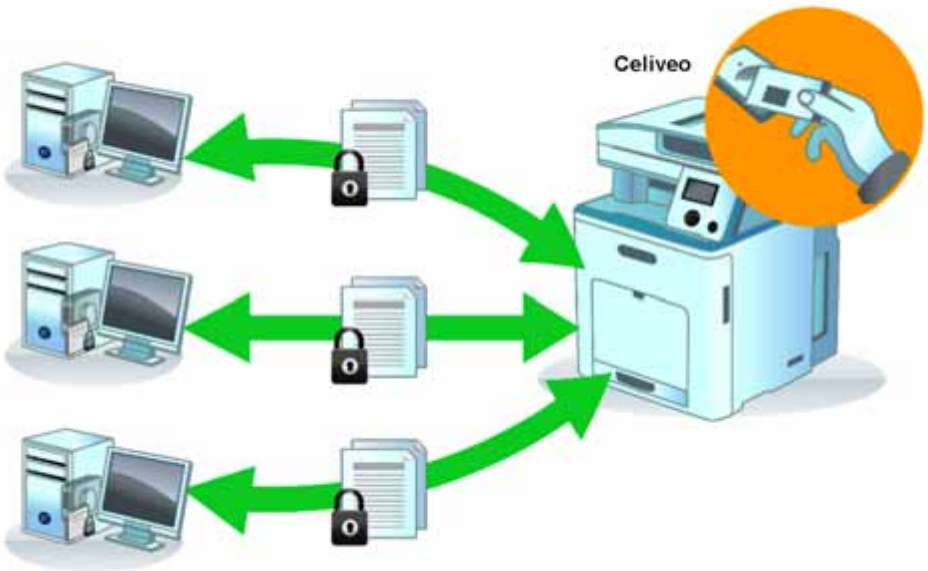
- Jobs are encrypted all the way from the client machines to the device.
- Jobs are retained on the print server for release from any Celiveo-enabled device upon authentication.

Server-Based Pull Printing with Celiveo installed on the Print Server



- Jobs are encrypted from the server print queue to the device.
- Jobs are retained on the print server for release from any Celiveo-enabled device upon authentication.

Serverless pull printing with Celiveo installed on the print server



- Jobs are encrypted at the Serverless Pull Print client machine.
- Jobs are retained at the Serverless Pull Print client machine.

Last modified: 29 September 2022

4. Downloads Celiveo 8 – Current Release Installers

CORE PACKAGE			
COMPONENT	**RELEASE NOTES**	**INSTALLER VERSION**	**COMPONENT DESCRIPTION**
CELIVEO WEB ADMIN	PDF	8.9.52.2	This installer comprises of Web Admin, CVP, DA and Printer Embedded Agent (for HP FutureSmart and Ricoh SOP models). This product installer is 64-bit compatible and should only be installed on Windows Server systems running on 64-bit OS. It is not recommended to install WA on Windows Client systems, except for demonstrative purposes. For more information, refer to System Requirements for Celiveo 8.
TRACK-GREENSAVER (TGS 10)	PDF	10.0.12.2	Unique reporting tool for Celiveo 8. The Celiveo Web Admin (Celiveo 8) application must be installed on the same Server and successfully launched prior to the installation of TGS 10.
SUBPACKAGE UPDATES			
COMPONENT	**RELEASE NOTES**	**INSTALLER VERSION**	**COMPONENT DESCRIPTION**
CELIVEO VIRTUAL PRINTER	PDF	8.9.21.2	This installer can be released along with Web Admin (major release) or as a hotfix. CVP is compatible with both 32-bit and 64-bit operating systems. The appropriate version will be automatically deployed based on the OS running on the client/ server systems.
CELIVEO MOBILE EXTENSION	PDF	8.9.21.2	Celiveo Mobile Extension for secure printing via email and chromeOS.
CELIVEO SMART APPLIANCE AGENT	PDF	8.9.022.1026	Celiveo firmware that runs on Celiveo Smart Appliance (CSA). This installer can be deployed to CSA-based printers via Web Admin.
RICOH PRINTER AGENT (BUSINESS EDITION)	PDF	8.8.2.2	Celiveo Printer Agent that runs on Ricoh SOP Android G2.0 and G2.5 printers. This installer can be deployed to such printer via Web Admin
HP PRINTER AGENT	PDF	8.9.122.1004	Celiveo Printer Agent that runs on HP FutureSmart Classic and Modern devices. **Note:** This Printer Agent version requires minimum HP Firmware 3.9.7 or 4.11.2 or 5.2 on HP Classic devices in order to run.

			Click here for further information about this.
CELIVEO STANDALONE POPUP NOTIFIER (FOR SHARED SERVER-BASED PULL PRINTING)		Standalone Popup Notifier	The Celiveo Shared Print Queue standalone popup notifier is a windows software installed on client machines to get notifications from the Print Server when printing through a Server-based print queue where the CSVP is installed. The popup notifies the user of any print-rule-related information, cost of the print, quota status, and remaining quota available.
CELIVEO SERVER SERVICES FOR MacOS	PDF	8.9.022.0222	Deployment package for Celiveo Server Services for MacOS.
CELIVEO-PRINT-WEB	README	4.3.0.1103	Celiveo® Print-Web is a mobile print software solution that installs inside the customer's private network and lets users print from any smartphone, tablet, or computer.

Upgrade Process

"Upgrade to Celiveo 8"

Explains how to upgrade from existing Celiveo solution to the latest release.

TOOLS & MISCELLANEOUS		
COMPONENT	RELEASE NOTES	INSTALLER VERSION
CELIVEO MIGRATION TOOL FOR SECUREJET 7.0.6/ CELIVEO 8.0.1/2 TO CELIVEO 8 VERSIONS	This tool allows the migration of SecureJet 7.0.6 or Celiveo 8.0.1/2 installation to the new Celiveo 8 versions.	Migration Tool
CELIVEO MIGRATION TOOL FOR CVP		V8.7.020.1016
SAMPLE OFFICE FLOOR MAPS 800 × 800		Sample Office Floor Maps
SECURE PUSH PRINTING DRIVER PLUGIN	**For HP FutureSmart Printers only**	Push Printing Driver Plugin

Last modified: 27 October 2022

5. Quick Start Guide

These are the basic steps to follow in order to start using the Celiveo solution:

How to install the Celiveo Hardware
Installing the Celiveo Web Admin
Installing TGS 10
After Installation
Web Admin First Run
Add Printers and their settings to the Web Admin
Tag Printers and Users
Set up Access
Configure Default Cost Definitions
Synchronize Printers

Last modified: 29 September 2022

6. Compatibility

Before installing the Celiveo solution and the Celiveo Hardware, please make sure you have all the requirements to ensure a clean and efficient installation.

System Requirements for Celiveo 8
Requirements for Hardware
Role Based Access Control for Celiveo
Ports and Communication
SNMP Settings
Celiveo Versions Compatibility with Windows 10

Last modified: 29 September 2022

6.1. System Requirements for Celiveo 8

Before you start installing Celiveo product, make sure the hardware and software requirements for the servers and client machines are met.

	Celiveo Web Admin [1] /TGS 10 (Applicable for Track-Green Saver 10)	**Celiveo Virtual Printer[2]**	**Celiveo Server Services for macOS[3]**
Minimum Hardware Requirements			
RAM	4 GB	4 GB	2 GB
Free hard disk space[4]	4 GB	4 GB	4 GB[5]
Server Operating System			
Windows Server 2022 (64-bit edition) Windows Server 2019 (64-bit edition) Windows Server 2016 (64-bit edition) Windows Server 2012 R2 (64-bit edition) Windows Server 2012 (64-bit edition) Note: Active Directory is required to run Celiveo 8 full feature set.	√	√[10]	
SQL Server 2019 [6] SQL Server 2017 [6] SQL Server 2016 [6] SQL Server 2014 [6]	√	√	√
Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package MFC Security Update (8.0.61001) Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package MFC Security Update (9.0.30729.6161) Microsoft OLE DB Driver for SQL Server (Version 18 or more, latest is preferred)		√	
Internet Information Services (IIS) Manager versions 10/ 8.5/ 8.0/ 7.5	√		
Windows Powershell[8]	√	√	
Workstation/ Client Operating Systems			
Windows 10 Home Edition (32-bit and 64-bit)	X	√	

Windows 10 Pro, Enterprise, Education Edition (32-bit and 64-bit) To learn more about Celiveo Editions compatibility with Windows 10, please see this article. Windows 8.1 (32-bit and 64-bit) Windows 8 (32-bit and 64-bit) Windows 7 SP1 (32-bit and 64-bit)	√[9]	√[10]	
macOS Catalina[11] [12] macOS Big Sur macOS Monterey macOS Ventura			√
.NET Framework 4.5		√	
.NET Framework 4.8[7]	√	√	
Web Browsers			
Microsoft Edge Chromium with Click-Once enabled (learn more).	√	√	

[1] Servers or client machines running Celiveo Enterprise Solution deployed using the Celiveo Web Admin Installer.

[2] MSI package with capabilities of Print-Direct and Celiveo Server Services.

[3] Client machine running Celiveo Server Services.

[4] Excludes the requirement of additional hard disk space for the installation and storage of SQL Server Express. Depending your organization's network setup, ensure there is additional space or access to a network storage appliance to store the users' print jobs. Ensure OS is installed with latest updates.

[5] Celiveo Server Services requires lesser than 100 MB of storage space.

[6] SQL DB Minimum Supported Compatibility Level is 120. Customers that migrated Celiveo databases from older SQL Servers (Levels lower than 120) need to ensure that the SQL DB level on SJPS and CeliveoDB databases is set at a minimum value of 120 on the new SQL Server that they have been migrated to.

To identify the SQL DB level execute the following SQL DB Query:

```
SELECT NAME, COMPATIBILITY_LEVEL FROM SYS.DATABASES WHERE NAME = 'INSERT_DATABASE_NAME_HERE'
```

To upgrade the SQL DB level execute the following SQL DB Query:

```
ALTER DATABASE INSERT_DATABASE_NAME_HERE SET COMPATIBILITY_LEVEL = 120
```

Further information here about SQL Database Levels.

[7] .NET Framework 4.8 is required by Celiveo and is enabled by the Celiveo installer itself. For older

version of Windows where installation by enabling features is not possible, the installer installs it with pre-packaged bundles.

[8] Ensure Windows Powershell is allowed on the servers where Celiveo solution is installed, and on client machines where Celiveo Virtual Printer (CVP) is deployed.

[9] When using Celiveo be aware of the following services operational needs:

Service	Description	Operation Type
Email Notifications	Celiveo Web Admin has several services that send emails to administrators such as, Authentication, Enrollment, Unenrollment, Reenrollment, Release or failed print jobs, IP Address not found in the defined IP range list, License Status, Celiveo System Logs.	Real-time
User Data AD/ LDAP-SQL Sync	When SQL DB enrollment is selected, Celiveo will sync the user information between AD and SQL DB based on the defined schedule to guarantee that SQL contains the latest user information.	Scheduler
Auto User Unenroll	When auto user unenroll is enabled, Celiveo checks if there’re any inactive users and removes them from the solution. This operation is performed daily and based on the user inactivity configuration on Web Admin.	Daily Operation
Orphan Print Job Clean Up	Orphan Print Jobs Clean checks daily if there’re any print jobs that were not deleted while the SQL DB was unreachable when the CVP or Printer Agent tried to delete a print job.	Daily Operation
Web Admin Recycle Bin Cleanup	When Web Admin Recycle Bin is enabled, Celiveo checks any data that is in the Recycle Bin and deletes it based on the maximum Recycle Bin life time configured on the Web Admin	Daily Operation
License Update	This is only applicable for rental customers. Celiveo will try to update the license against Celiveo Cloud Licensing Servers to get the latest License applicable for the customer.	Scheduler
Temp Data Cleanup	Celiveo cleans the temporary data that is generated by Web Admin in day-to-day operations.	Daily Operation
Celiveo SQL DB Replication Sync	When using Primary and Regional SQL DB Celiveo will try to execute DB sync every 30 seconds in case there’s new data in the Primary DB it will replicate it to all existent Regional DB.	Every 30 Seconds
Quota Update	When Quota is enabled, Celiveo will need to update quota based on the schedulers set by the administrator.	Potentially Real-time
ID Code Portal Generation	End-User Web Portal where users can login and generate their Numeric or Alphanumeric ID Code.	Real-time

Track-GreenSaver 10	Track-GreenSaver is a Web Portal used by management to generate and schedule printing reports generation.	Potentially Real-time

Note: Celiveo Web Admin product installer is only 64-bit compatible.

[10] Celiveo Virtual Printer is compatible for both 32-bit and 64-bit operating systems. Appropriate Virtual Printer (32-bit or 64-bit installer) will be deployed based on the OS in the client/ server machine.

[11] Supports Catalina version 10.12 and higher.

[12] Requires sudo rights for installation purposes.

Last modified: 23 November 2022

6.2. Requirements for Hardware

For Celiveo Smart Appliance:

- Fixed IP or DHCP-reserved IPv4
- MAC address (as printed on Celiveo Smart Appliance)

For printers connected with Celiveo Smart Appliance:

- Active TCP-IP 100BT LAN connection
- Active Simple Network Management Protocol (SNMP) v1/v2
- A printer with either fixed IP or DHCP-reserved IP address
- Printer specific settings before Celiveo solution installation (See the respective sections on Printer specific requirements).
- The Celiveo Smart Appliance (CSA) aligns with the latest high security standards and FIPS compliance.
  Therefore the following ciphers shall be available on PC and printers to allow a TLS encrypted communication to be established with the CSA:
  ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES256-GCM-SHA384, DHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES128-SHA256, AES256-GCM-SHA384, AES128-GCM-SHA256, AES256-SHA256, AES128-SHA256, AES256-SHA, AES128-SHA
  Furthermore, the CSA is compliant with the Microsoft Server FIPS mode.
  https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-cipher-suites-in-windows-10-v1903

Last modified: 29 September 2022

6.3. Operating System, SQL and Active Directory rights to install and use Celiveo

Operating System Rights

Component	Installation			Operations		
	Account	**Privileges**	**Password change / Account expiry**	**Accounts**	**Privileges**	**Password change / Account expiry**
Celiveo Smart Appliance (CSA)	Registered user on WA as Admins	**WA** – No additional privileges required	N/A	N/A	**OS/ DB** – No privileges required	N/A
Embedded Solution (HP FutureSmart)	Registered user on WA as Admins	**WA** – No additional privileges required	N/A	N/A	**OS/ DB** – No privileges required	N/A
Celiveo Virtual Printer (CVP/CSVP)	Windows Account	**OS** – Local Administrator privileges	NO	Local System	**OS** – No additional privileges required.	**Password change** – Required **Not to Change**. If password is changed, it needs to be updated in WA.Configuration settings file *config.ini* should be updated in all workstations.
	N/A	**DB** – N/A	NO	CeliveoDB User (credentials set in encrypted connection string)	**DB** – Require *dbreader*, *dbwriter* and *ddladmin* roles and *EXEC* permission to execute stored procedures on databases (SJPS/ CeliveoDB)	**Password change** – Required **Not to Change**. If password is changed, it needs to be updated in WA. Configuration settings file *config.ini* should be updated in all workstations.

SQL service account rights

There are 2 ways to install and run Celiveo Web Admin based on database user privileges that can be provided:

1. Using any user, who has the privilege to create a database on SQL Server. Typically default roles sysadmin, dbcreator have these privileges. And any role/user with “CREATE ANY DATABASE”, “VIEW ANY DATABASE”, “CONNECT” server-level permissions will also qualify.
   When this option for service user is chosen, enter a user with the above roles/permissions on the Celiveo WA installer and it will take care of creating both databases (CeliveoDB, SJPS) and install Web Admin keeping the entered user as service accounts for Celiveo with respect to database server.

2. Another way to specify the DB service user for Celiveo when this service user must not be able to create databases. In this case, before installing Celiveo Web Admin:
   a. Manually create 2 databases on SQL Server i.e. CeliveoDB and SJPS.
   b. Create login on SQL server with SQL Authentication.
   c. Create user in CeliveoDB and SJPS for created login and then give appropriate permissions to that user. There are 2 ways to give permission to user: built roles and explicit permissions. The following table describes permissions/roles required by Celiveo:

Database Name	Role	Permissions
CeliveoDB	db_datareader, db_datawriter, db_ddladmin	**SERVER** – VIEW SERVER STATE **DATABASE** – “CREATE TABLE”, “CREATE VIEW”, “CREATE PROCEDURE”, “CREATE FUNCTION”, “CREATE RULE”, “CREATE DEFAULT”, “CREATE TYPE”, “CREATE ASSEMBLY”, “CREATE XML SCHEMA COLLECTION”, “CREATE SCHEMA”, “CREATE SYNONYM”, “CREATE AGGREGATE”, “CREATE SYMMETRIC KEY”, “CREATE ASYMMETRIC KEY”, “CREATE FULLTEXT CATALOG”, “CREATE CERTIFICATE”, “CONNECT”, “ALTER ANY SCHEMA”, “ALTER ANY ASSEMBLY”, “ALTER ANY FULLTEXT CATALOG”, “ALTER ANY SYMMETRIC KEY”, “ALTER ANY ASYMMETRIC KEY”, “ALTER ANY CERTIFICATE”, “SELECT”, “INSERT”, “UPDATE”, “DELETE”, “REFERENCES”, “ALTER ANY DATABASE DDL TRIGGER”, “VIEW DATABASE STATE”, “EXECUTE”
SJPS	db_datareader, db_datawriter, db_ddladmin	**SERVER** – VIEW SERVER STATE **DATABASE** – “CREATE TABLE”, “CREATE VIEW”, “CREATE PROCEDURE”, “CREATE FUNCTION”, “CREATE RULE”, “CREATE DEFAULT”, “CREATE TYPE”, “CREATE ASSEMBLY”, “CREATE XML SCHEMA COLLECTION”, “CREATE SCHEMA”, “CREATE SYNONYM”, “CREATE AGGREGATE”, “CREATE SYMMETRIC KEY”, “CREATE ASYMMETRIC KEY”, “CREATE FULLTEXT CATALOG”, “CREATE CERTIFICATE”, “CONNECT”, “ALTER ANY SCHEMA”, “ALTER ANY ASSEMBLY”, “ALTER ANY FULLTEXT CATALOG”, “ALTER ANY SYMMETRIC KEY”,

		“ALTER ANY ASYMMETRIC KEY”, “ALTER ANY CERTIFICATE”, “SELECT”, “INSERT”, “UPDATE”, “DELETE”, “REFERENCES”, “ALTER ANY DATABASE DDL TRIGGER”, “VIEW DATABASE STATE”, “EXECUTE”

NOTE – Please note that you can either set roles or permissions. When you have set roles for the user, you don’t need to explicitly set any permissions, because the roles specified above contain all those permissions.

You can also use the following scripts to create a login, user, and set permissions for service account –

1. **Create Service Account with roles.sql** – This file creates a login, user, and assigns db_datareader, db_datawriter and db_ddladmin roles to that user in SJPS and CeliveoDB databases.
2. **Create Service User with permissions.sql** – This file creates a login, user and then adds all minimum required permissions for the user.

NOTE – Please remember to rename your username and provide your own password in the script. Command-line in SQL script denotes the place where username and password need to be changed.

Active Directory service account rights

The Active Directory service account is used by Celiveo Web Admin, Celiveo Printer Agent and Enrollment Portal to read and write data from and to Active Directory depending on type of selected enrollment.

- **Active Directory Enrollment** – The service account is used to read and write information from and to the Active Directory every time the user enrolls and authenticates.
- **SQL Enrollment** – The service account is used to read information from Active Directory and store it in the Celiveo SQL DB User Enrollment table upon enrollment. Additionally the Celiveo administrator can define a scheduler to query Active Directory to get user data to Celiveo SQL DB in order to keep parity with Active Directory.

Enrollment Type	Permissions	Field Operations
Active Directory	Read/Write	postOfficeBox: **Read/Write** department: **Read** displayName: **Read** sAMAccountName: **Read** description: **Read** mail: **Read** homeDirectory: **Read** domain: **Read** l: **Read/Write**

		memberOf: **Read** OU: **Read** Group: **Read**
SQL	Read	department: **Read** displayName: **Read** sAMAccountName: **Read** description: **Read** mail: **Read** homeDirectory: **Read** domain: **Read** memberOf: **Read** OU: **Read** Group: **Read**

Note: The Active Directory fields described above are used by default in Celiveo, these can be modified to other standard or custom Active Directory/LDAP fields. Further information about authentication profiles.

TGS 10

For TGS 10, the service user that you enter needs to have db_datareader, db_datawrite, db_ddladmin roles, or the same permissions as that of Web Admin. Therefore you can use the same service user as that of WA in TGS 10. TGS 10 always needs to be installed after Web Admin.

Note:
Tags applied decide the level of authority for the user in WA. To know more about Tags and System Administrator Management, refer to:

Tag Printers and Users
Managing System Administrators

Last modified: 10 November 2022

6.4. Ports and Communication

The table below provides a comprehensive list of all the ports used by Celiveo solutions and describes the ports and applications used for communication between the Celiveo components that consist of the Celiveo Server Services, Web Admin Server, Active Directory, Database (SQL) server, the device, and the PC/laptop/workstation.

Origin	Destination	Application name/service, exe	Destination Port	Protocol	Comments
Common for Serverless / Server-based Pull Printing and Print-Direct					
Web Admin	Active Directory [1]	lsass.exe	636 or 389 [2]	TCP	To configure and test Access Control Profiles used by other celiveo modules
	Celiveo Virtual Printer	celiveo virtual printer service.exe	65219	TCP	**Optional:** Celiveo Virtual Printer troubleshooting log download
	SMTP Server	Email Server	587 or 25 [3]	TCP	**Optional:** Sends administrative notifications and password recovery emails to celiveo administrators
	Printing Device [1]	Printing Device	443 or 80 [4]	TCP	Logins to device and initiates installation process
			9100	TCP	Sends Celiveo Printer Agent bootstrap and SQL connection settings to target Printer
			8181	TCP	**Optional:** Celiveo Printer Agent log collection from Web Admin
	Celiveo Cloud Services	celiveo.cloud/api	443	TCP	**Optional:** Used to auto-update Asset and Rental licenses
Web Admin / Celiveo Printer Agent [1]	SQL Server	sqlbrowser.exe	1434	UDP	Retrieves the dynamic port established by SQL Server from SQL Server Browser service and uses it from that point onward
		sqlservr.exe	1433 or Dynamic [5]	TCP	Used contact SQL Server for transactional operations
Celiveo Printer Agent [1]	Active Directory	lsass.exe	636 or 389 [2]	TCP	Active Directory connection for user authentication, user enrollment and user metadata

Celiveo Discovery Agent	Printing Device	Printing Device	161	UDP	Retrieves printer data over SNMP v1/v2/v3
			N/A	ICMP	Ping Device for availability information
	Web Admin	celiveoprinterdiscoveryagentservice.exe	22201	TCP	Uploads printer metadata and Driver + Settings to Celiveo Database via Printer Discovery Agent Service in Web Admin
Server-based Pull Printing					
End-User Workstation	Celiveo Shared Virtual Printer	NetBIOS Datagram Service	139	TCP	Microsoft services that provide network computers access to shared printers
		NetBIOS Name Resolution	138	UDP	
			137	UDP	
		SMB	445	TCP	
		Printer Sharing Spooler Service RCP [6]	49152-65535	TCP/UDP	
Celiveo Printer Agent	Celiveo Shared Virtual Printer	SJ Print-PS Server.exe	22000	TCP	Requests Print Jobs to be released on soliciting printer, requests Print Job list when Printer Agent is in High-Availability mode.
Celiveo Shared Virtual Printer	Celiveo Printer Agent	Printing Device	9100	TCP	Sends print jobs to the requesting printer
	Celiveo.me	celiveo.me/api	443	TCP	**Optional:** To collect Print Jobs submitted via Celiveo.me
	End-User Workstation – Celiveo Notification service	celiveo notification service.exe	22001	TCP	**Optional:** Notify end-users with popup printing rules messages
	SQL Server	sqlbrowser.exe	1434	UDP	Retrieves the dynamic port established by SQL Server from SQL Server Browser service and uses it from that point onward
		sqlservr.exe	1433 or Dynamic [5]	TCP	Used contact SQL Server for transactional operations
		N/A	N/A	IC	Ping Server for availability information

				MP	
	Web Admin	w3wp.exe	443 or 80 [4]	TCP	**Optional:** Retrieves SQL Server Connection Settings, only used as failover when SQL is not available
Common for Serverless Pull Printing and Print-Direct					
Celiveo Virtual Printer	SQL Server	sqlbrowser.exe	1434	UDP	Retrieves the dynamic port established by SQL Server from SQL Server Browser service and uses it from that point onward
		sqlservr.exe	1433 or Dynamic [5]	TCP	Used contact SQL Server for transactional operations
		N/A	N/A	ICMP	Ping Server for availability information
	Web Admin	w3wp.exe	443 or 80 [4]	TCP	**Optional:** Retrieves SQL Server Connection Settings, only used as failover when SQL is not available
Serverless Pull Printing					
Celiveo Printer Agent	Celiveo Virtual Printer	SJ Print-PS Server.exe	22000	TCP	Requests Print Jobs to be released on soliciting printer, requests Print Job list when Printer Agent is in High-Availability mode.
Celiveo Virtual Printer	Celiveo Printer Agent	Printing Device	9100	TCP	Sends print jobs to the requesting printer
Print-Direct					
Celiveo Virtual Printer	Printing Device	Printing Device	161	UDP	Retrieve printer status over SNMP v1/v2/v3
			9100	TCP	Sends print jobs to selected printer
	Active Directiry	lsass.exe	636 or 389 [2]	TCP	**Optional:** For advanced tracking purposes CVP collects user information from AD

[1] Functionality only used by Print-Direct when advanced Celiveo Virtual Printer tracking or Printer Agent tracking are configured. Printer Agent tracking only applicable for HP Devices.

[2] Port 636 LDAPS or 389 LDAP usage depends on the customer Active Directory and Web Admin Access Control configuration.

[3] Port 587 SMTPS or 25 SMTP usage depends on the customer Email Server and Web Admin Email Server configuration.

[4] Port 443 HTTPS or 80 HTTP usage depends on the device configuration. Celiveo always use 443 first with failover to 80.

[5] 1433 is the default static port setting configuration, Celiveo Web Admin SQL Connection settings can also be configured with alternative static ports. If Dynamic Ports are used, these are retrieved via port 1434 UDP and used from that point onward.

[6] Depends on Windows Server Configuration

Last modified: 2 December 2022

6.5. SNMP Settings

SNMP (Simple Network Management Protocol) is a standard network management protocol (based on TCP/IP) to monitor and map network availability, performance, and error rates when a printer is added in Celiveo Web Admin. To identify the different printer types after the printer is contacted, the SNMP protocol retrieves information such as the system description, system type, printer serial number, and printer model name.

Set SNMP v1/v2 settings

Setting	Activity
[Enable SNMP v1/ v2]	Enabled by default.
[Community Name]	Enter the community name of the printer type required during the communication between Celiveo Web Admin and the printer. The request messages are accepted only if the community name in the message matches the community name of the printer type specified on the printer web page.

Set SNMP v3 settings

Setting	Activity
[Enable SNMP v3]	Enable SNMP v3 settings.
[User Name]	Enter the user name required during authentication while contacting the printer.
[Context Name]	Enter the context name of the printer type required during the communication between Celiveo Web Admin and the printer. The request messages are accepted only if the context name in the message matches the context name of the printer type specified on the printer web page.
[Authentication Protocol (Hash)]	The authentication protocol is used for proper authentication by ensuring the identity of the users, and the correct and appropriate encryption mechanism for security purposes. Select one of the options: • **[None]** • **[MD5]**: a message digest algorithm • **[SHA1]**: an optional alternative algorithm
[Authentication Password]	Enter an alphanumeric password of 8 to 12 characters that is required for the authentication mechanism.
[Privacy Protocol (Encryption)]	Privacy protocols allow for encryption of SNMP v3 messages to ensure confidentiality of data. It is a secondary security constraint for SNMP v3 to ensure privacy of the request for the proper channeling of a response. Select one of the options: • **[None]**: No Privacy Protocol

	• **[DES]**: Data Encryption Standard (DES) mode of encryption • **[AES128]**: 128-bit Advanced Encryption Standard (AES) mode of encryption • **[AES192]**: 192-bit Advanced Encryption Standard (AES) mode of encryption • **[AES256]**: 256-bit Advanced Encryption Standard (AES) mode of encryption • **[TripleDES]**: Triple Data Encryption Standard mode of encryption

Last modified: 29 September 2022

6.6. Celiveo Versions Compatibility with Windows 10

Windows 10 Release Version	SecureJet 7.0.6 Serverless Pull Print Client	Celiveo 8.0.2 Serverless Pull Print Client	Celiveo 8 Celiveo Virtual Printer 8.6.x and 8.7.x
Version 2002	√	√	√
Version 1909	√	√	√
Version 1903	√	√	√
Version 1809	√	√	√

Last modified: 29 September 2022

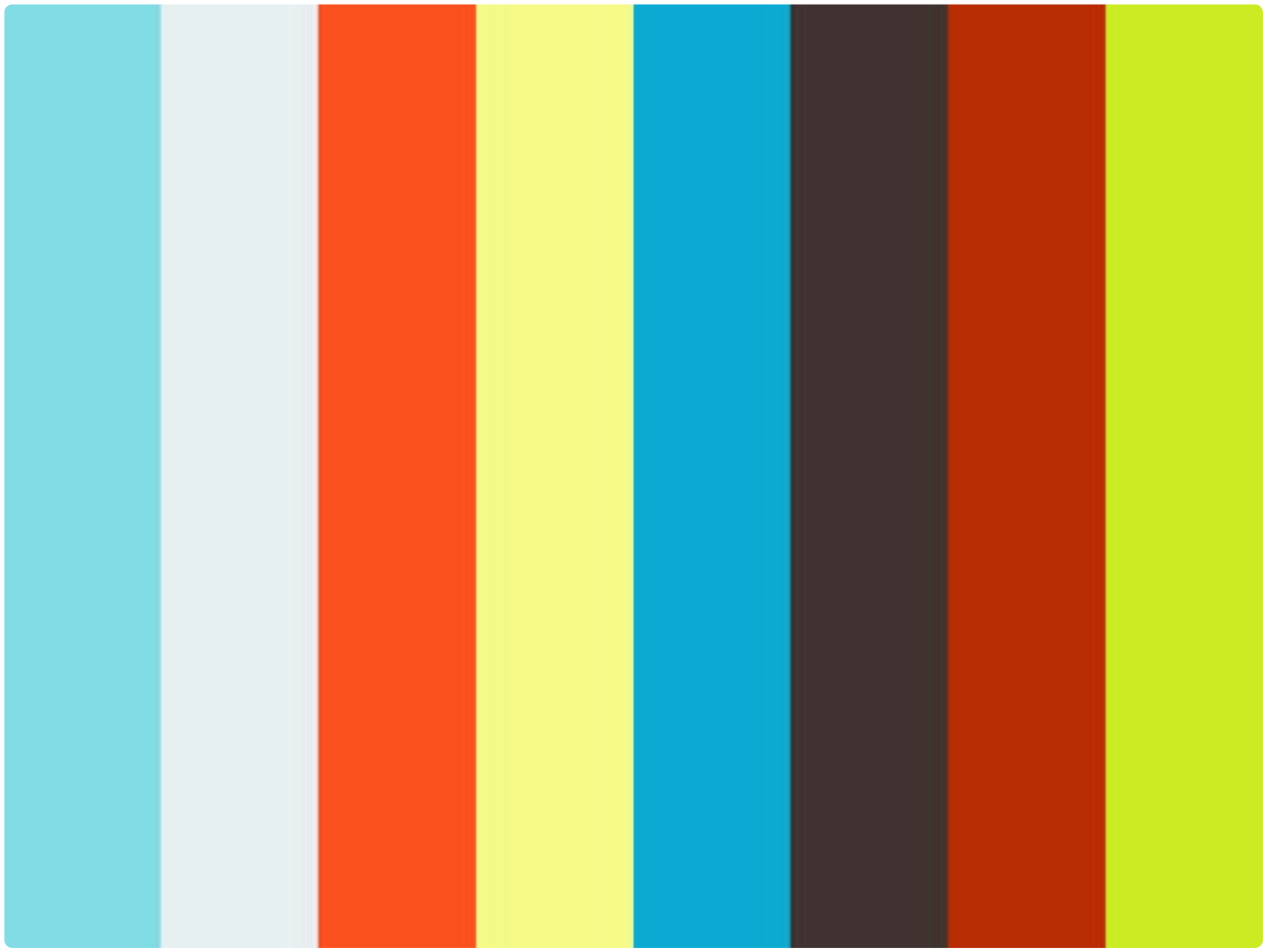
7. Installation

This section details the installation process for all Celiveo components.

How to install the Celiveo Hardware
Installing the Celiveo Web Admin
Installing TGS 10
After Installation
Web Admin First Run
Viewing and Updating Your Celiveo License
Multicard Reader – Specifications for Type A
Multicard Reader – Specifications for Type B

Last modified: 29 September 2022

7.1. How to install the Celiveo Hardware



https://player.vimeo.com/video/230735011

IMPORTANT NOTES:

Printer time and date:

- Celiveo uses the date and time from the printer for jobs tracking, automatic updates, rules, scheduled tasks etc. Therefore make sure the date and local time are correctly set on the printers, with the correct time zone defined and the time should ideally be synced with a time server.

Network connections on CSA:

- Ensure CSA has both Ethernet (Printer and LAN) ports connected, in order to work properly.
- Do not connect the CSA to a POE-powered network cable.
- When the Ethernet cable between the CSA and the printer is re-plugged there is a delay of 20 seconds before the printer can be used, due to an internal network verification process.

CSA Manual Configuration

To learn more about manually configuring the CSA, please refer to the following article.

Last modified: 29 September 2022

7.2. Installing the Celiveo Web Admin

> **IMPORTANT NOTE**: SQL Server® 2016 SP1 is not supported on Windows 7 and Windows 2008 R2 Operating systems. For Windows Servers running on Windows Server 2008 R2 OS, it is recommended to install a lower version of SQL Server (preferably SQL Server® 2012 Express) and then follow the instructions.

The Celiveo 8 Web Admin installer package comprises of the following components:

- Printer Discovery Agent
- Celiveo Virtual Printer deployment package

The new tracking and reporting tool Track- Green Saver (TGS 10) is a stand-alone installer package. This should be installed in the Server right after Web Admin installation. The instructions for installing TGS 10 can be found in here.

Before you start, ensure the following:

- Both the application and database servers are in the same domain.
- IIS is installed on the secondary database if there is any, with version 5.1 minimum.
- SQL Authentication is set to Mixed Mode.
- The SQL Server database is configured to allow remote connection:
  - The SQL Server Browser Service is running.
  - TCP/IP protocol for the SQL Server is enabled.
  - The firewall allows remote connection

Follow these steps to install Celiveo Web Admin on Windows Server.

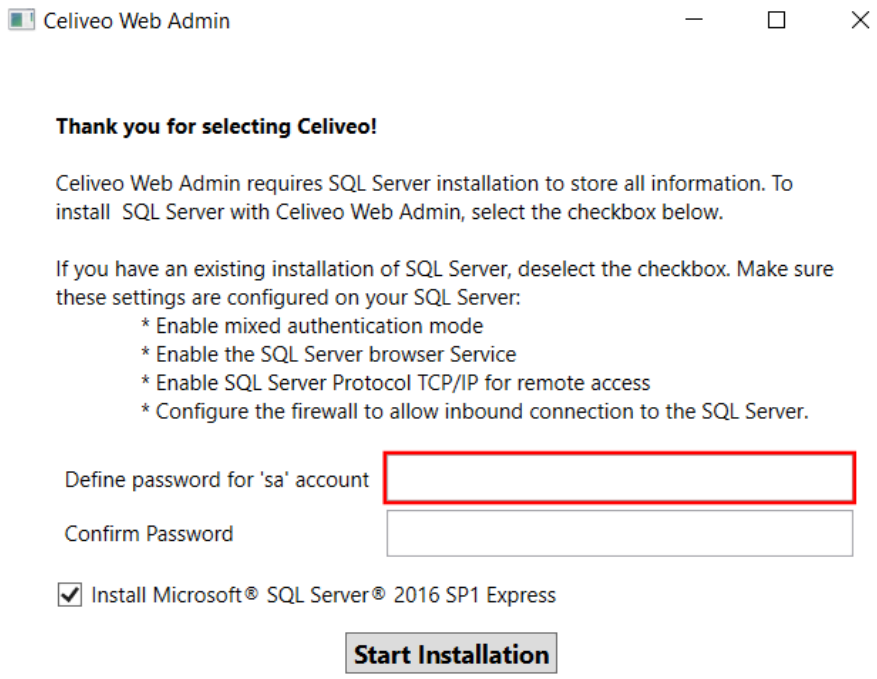
1. Start Installation
2. Install SQL Server Express
3. Install Celiveo 8
4. Finalize Installation
5. Change Database Password After Installation

1. Start Installation

1. Copy the Celiveo Web Admin installer package to the desktop. You can download the latest version from Downloads.
2. Select the installer and right-click on **[Run as administrator]**.

2. Install SQL Server Express

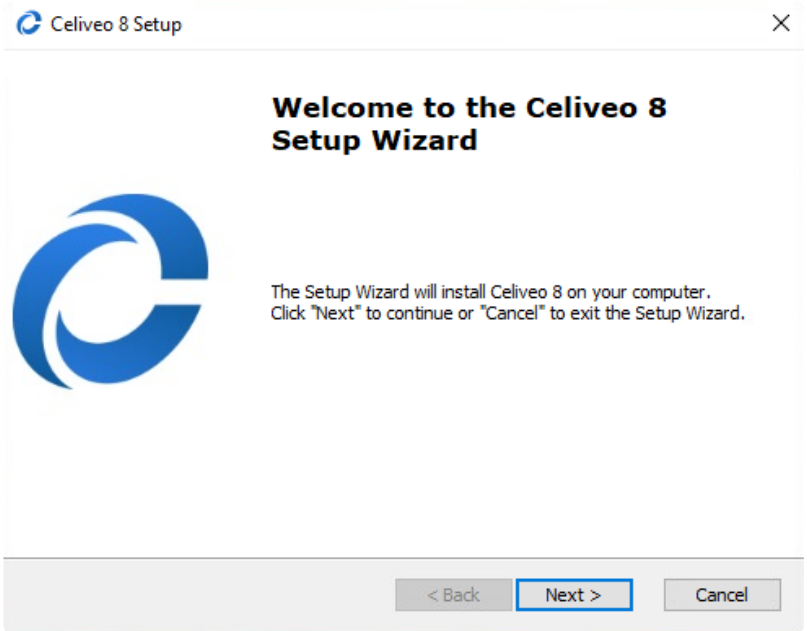
1. In the welcome window, select **[Install Microsoft SQL Server® 2016 SP1 Express]**. If SQL Server already exists in your machine, do not select this option.
2. Define the password for the account with System Administrator (role) access on the SQL server.
3. Click **[Start Installation]**.



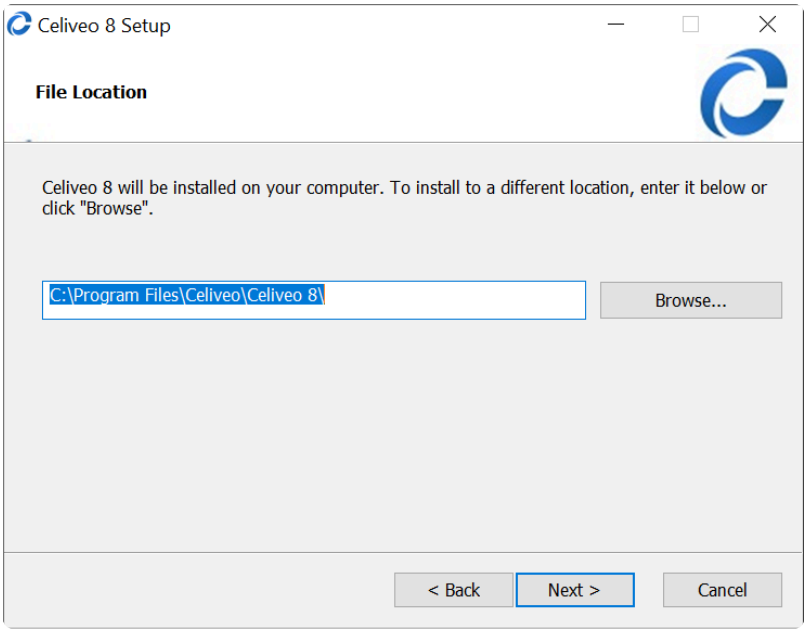
4. Follow on-screen instructions to install **SQL Server® 2016 SP1 Express**.
5. When prompted to reboot the machine, click **[Yes]**.

3. Install Celiveo 8

1. To continue the installation after the machine reboots, click **[Next]**.



2. Be informed of the license terms and conditions. To continue installation, select the checkbox to accept and click **[Next]**. To cancel, click **[Cancel]**.
3. If required, edit the file location and click **[Next]**.

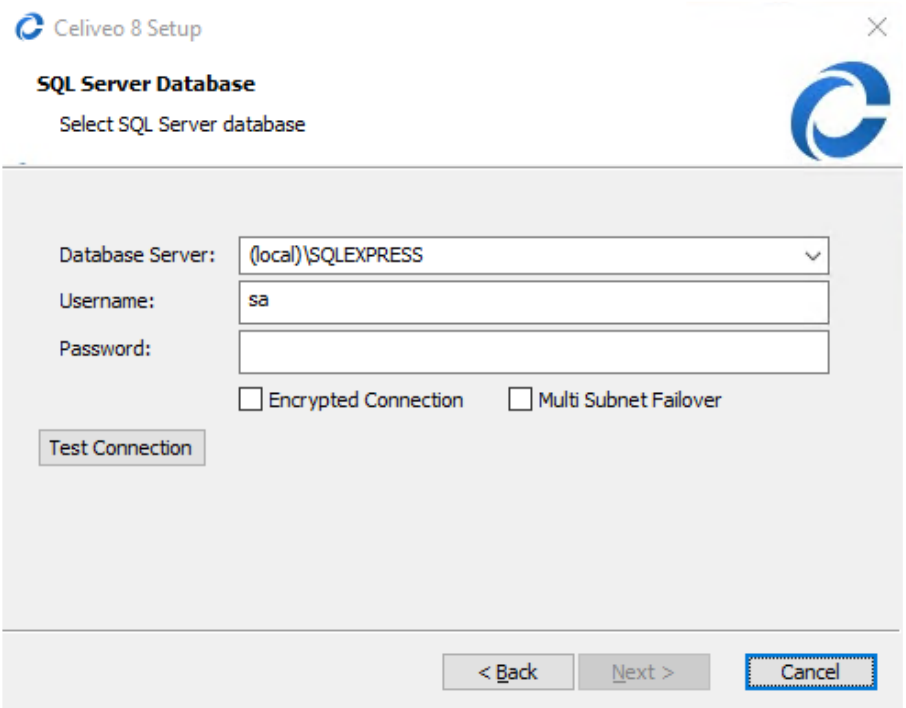


4. Select the SQL Server IP address/hostname in the **[Database Server]** list.

> **Important**: If you are intending to use Multi-SQL configuration, it is **highly recommended** to provide an IP address/hostname at the **[Database Server]**.

5. The default database is (local)\SQLEXPRESS.

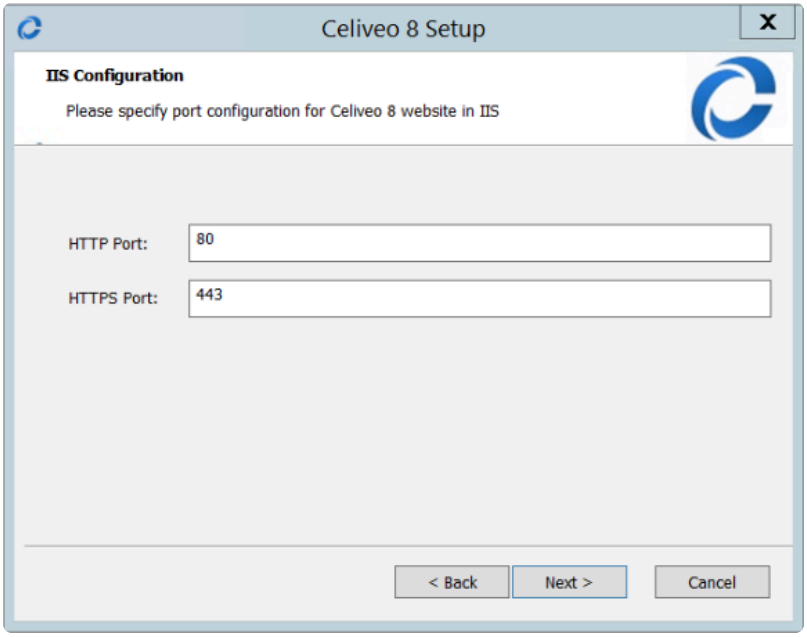
> **Note:** System Administrator account is required only at the time of installation. You may delete/disable this account after installation. See OS and SQL rights to install and use Celiveo to view permissions used for TGS Service account and Celiveo database accounts.



Options:

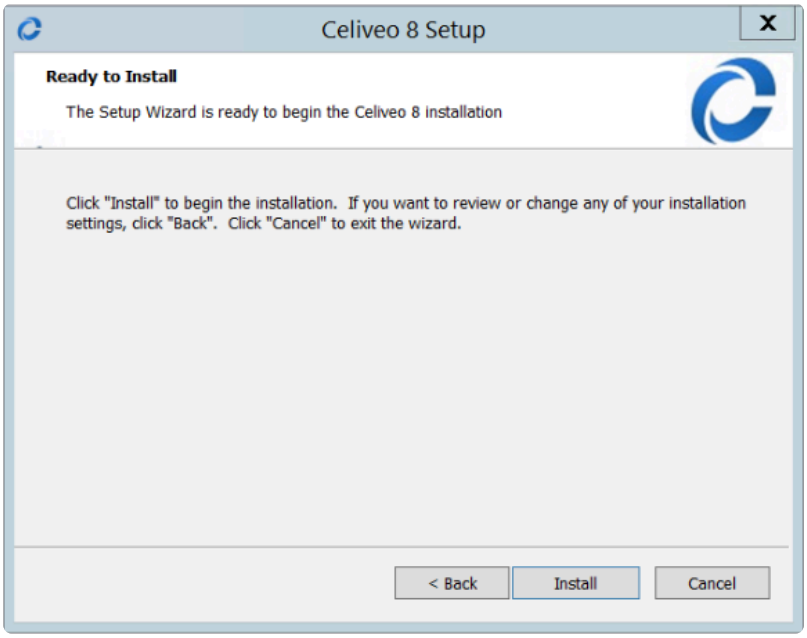
- Select [Encrypted Connection] checkbox to enable secured communication with SQL Server.
- Select [Multi Subnet Failover] checkbox to enable connection to (Always On) Availability Groups in case of a failover in a multi-subnet environment.

6. Click **[Test Connection]**.
7. Once the connection test is successful, click **[Next]**.
8. In the IIS Configuration window, enter the **[HTTP Port]** and **[HTTPS Port]** details. The default values are provided as 80 and 443 respectively. If required, change the port details and click **[Next]**.

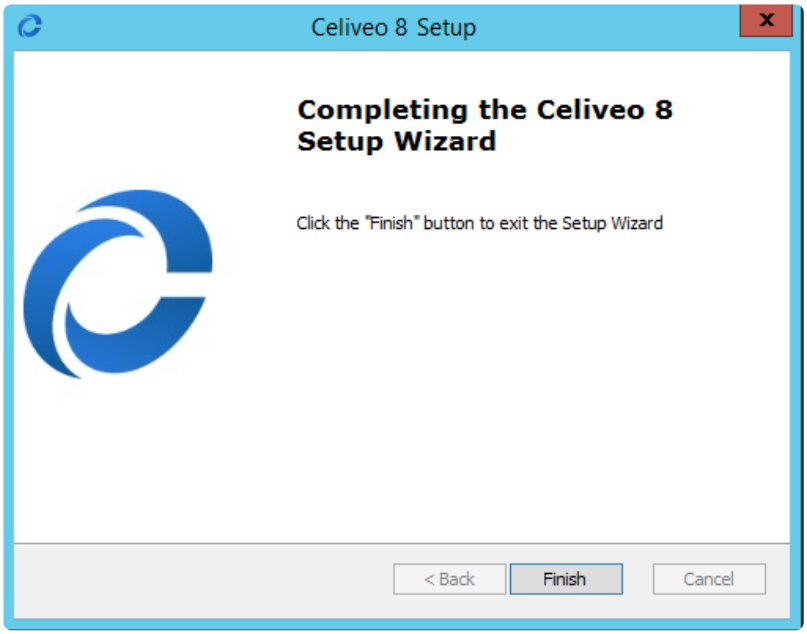


4. Finalize installation

9. When prompted, click **[Install]**.



10. When prompted to exit the Setup Wizard, click **[Finish]**.



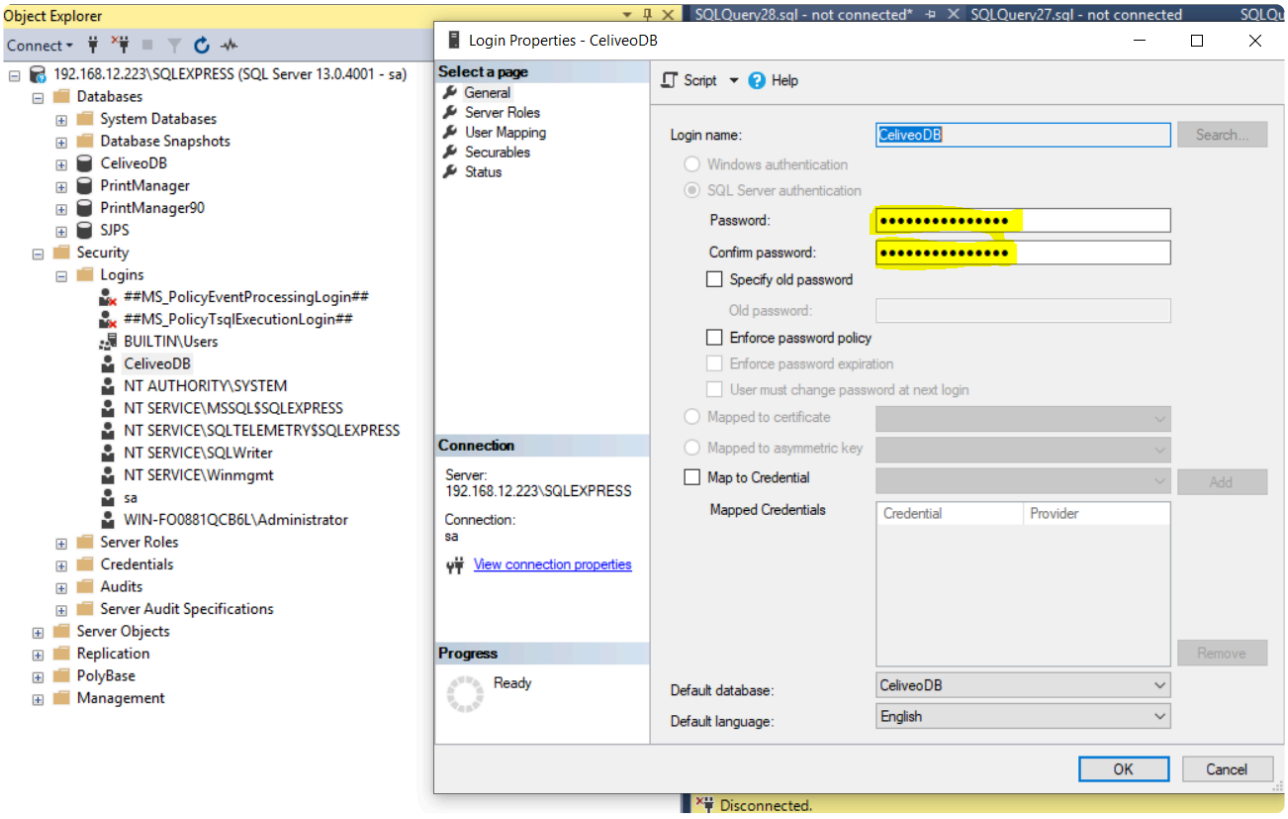
The Celiveo Web Admin icon is added to the desktop.

5. Change database password after installation

For security purposes, it is recommended to change the default password of SQL Server right after installation. You can update the password on the SQL server for Celiveo database (CeliveoDB) account and then update the same password for the database profile in Web Admin.

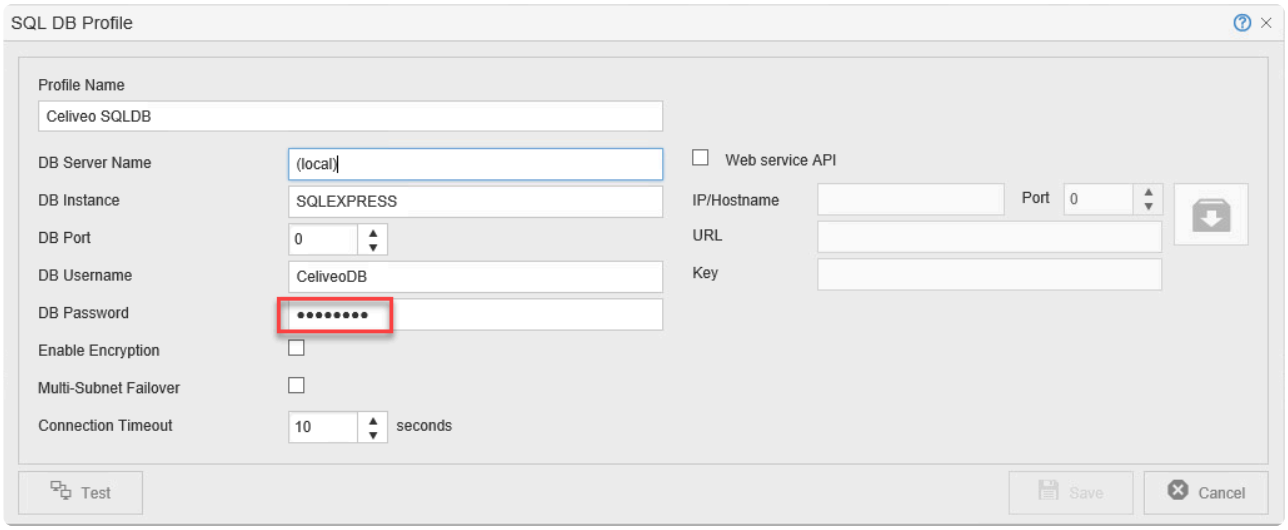
On SQL Server:

1. Go to **Security > Login**.
2. Right-click on **CeliveoDB** account and choose **Properties**.
3. Go to **General** page.
4. Set a new password for CeliveoDB in **[Password]** field
5. Re-enter the password in **[Confirm Password]** field.
6. Click **[OK]**.



On Web Admin

1. On Celiveo Web Admin Home page, click the **Setup** icon.
2. Choose **DB settings** tab.
3. On the SQL DB profile row, click the Edit icon.
4. Update the **[DB password]** with the new password set for CeliveoDB account.
5. Click **[Save]**.

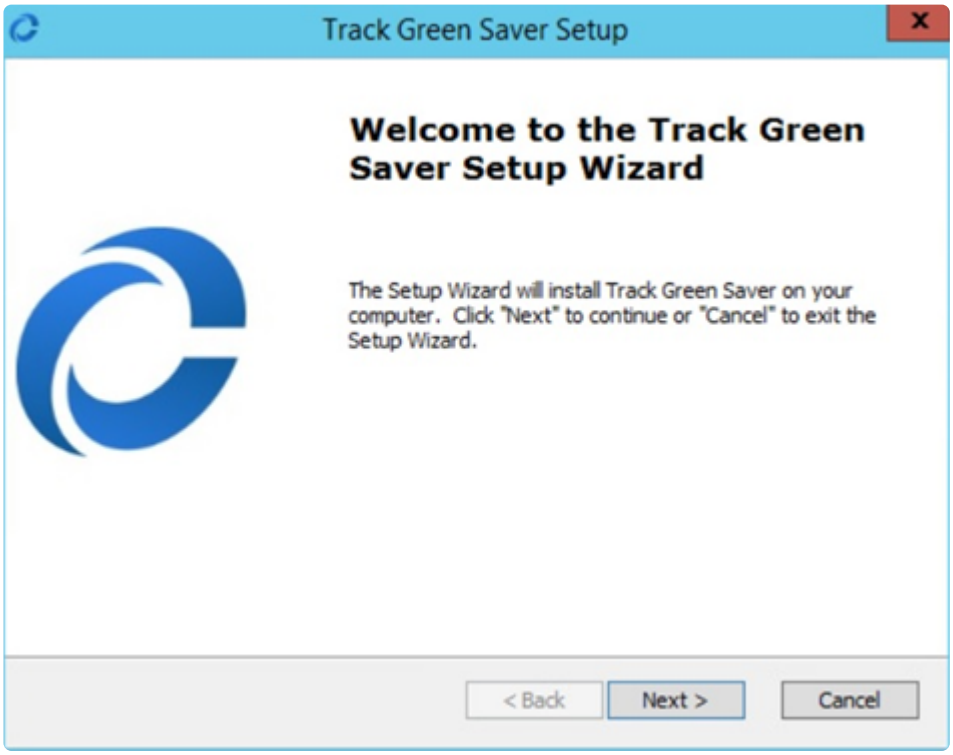


Last modified: 29 September 2022

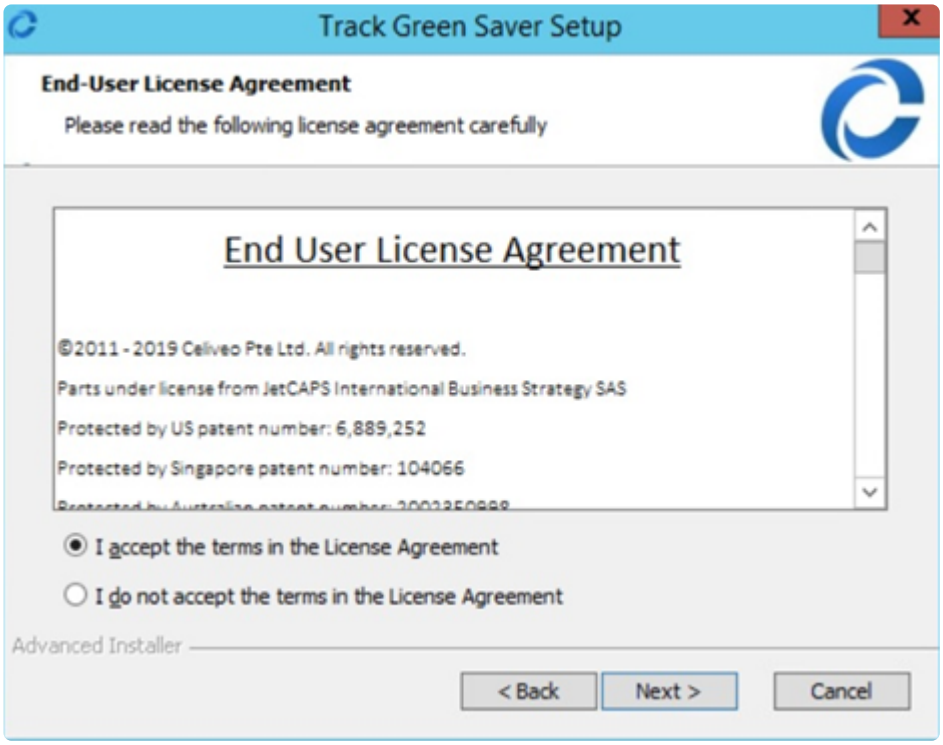
7.3. Installing TGS 10

> **IMPORTANT**: Celiveo Web Admin application MUST be installed and successfully launched prior to the installation of TGS 10. Ensure that TGS 10 and Web Admin are installed in the same system.

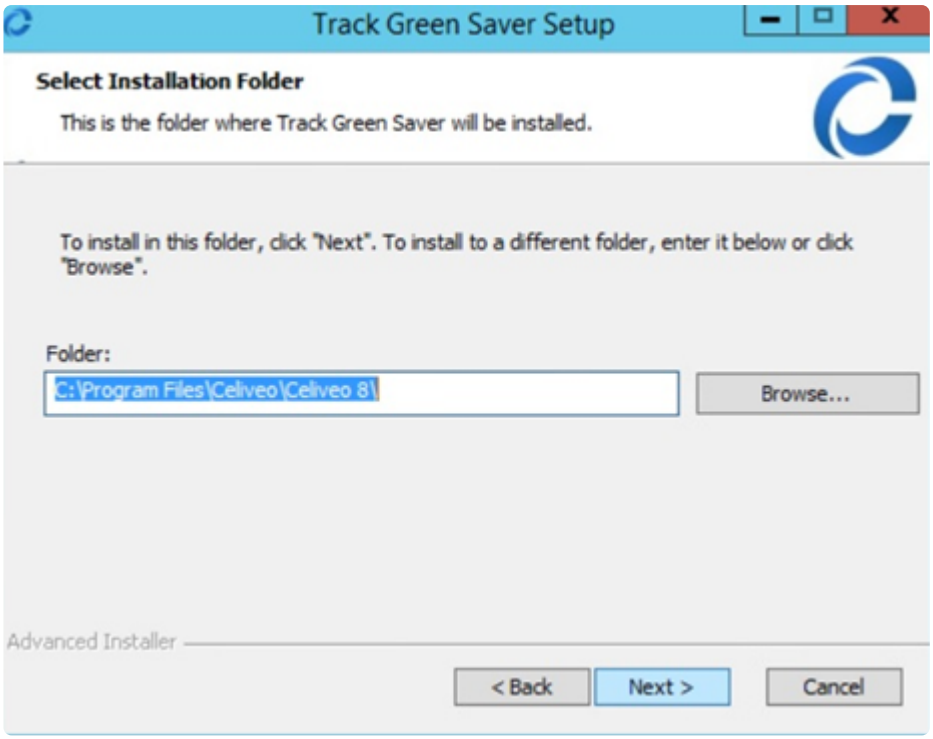
1. Copy the Track-Green Saver Installer package to the desktop.
2. Select the installer and right click on **[Run as Administrator]**.



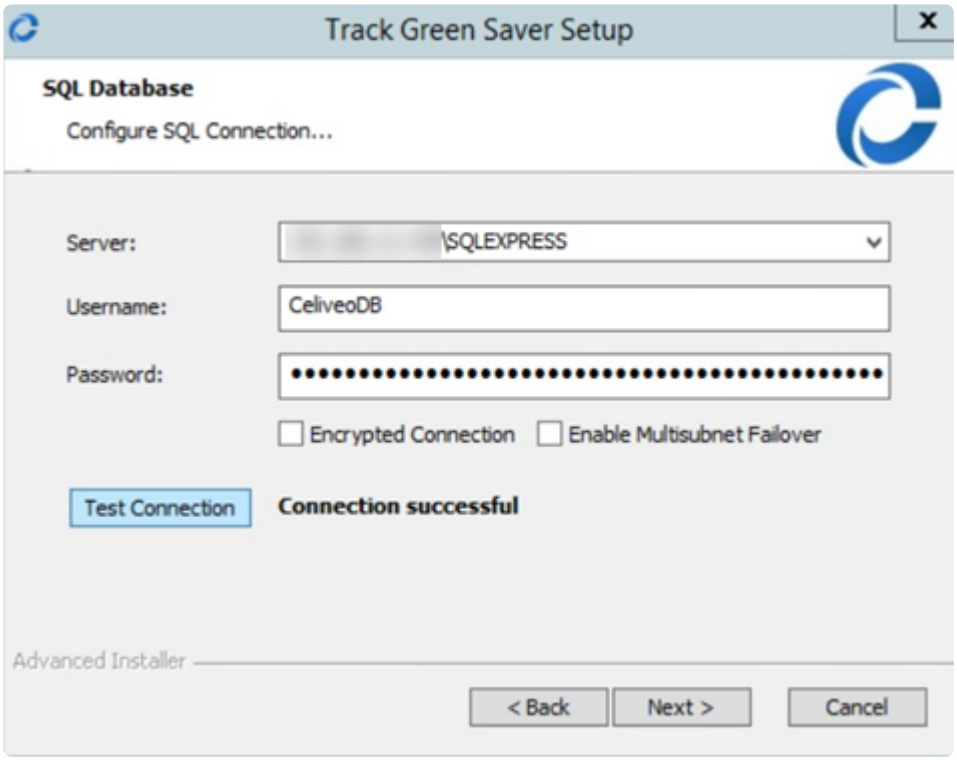
3. Click **[Next]**.
4. Be informed of the license terms and conditions. To continue installation, accept and click **[Next]**. To cancel, click **[Cancel]**.



5. If required, edit the file location and click **[Next]**.



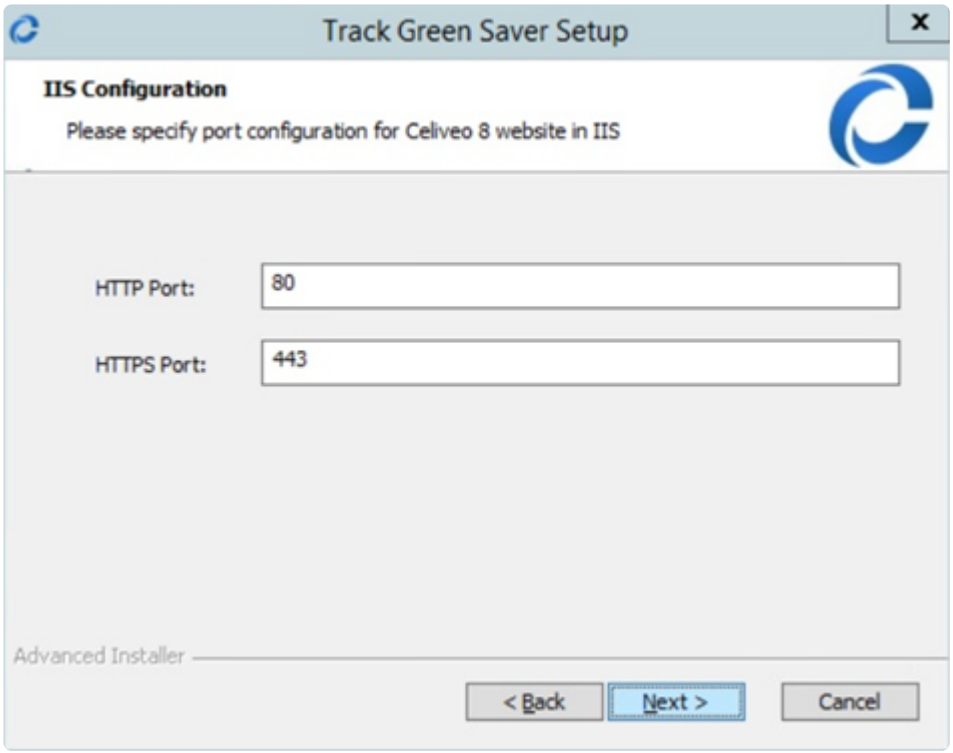
6. Enter the user name and password for an account with System Administrator (role) access on the SQL server. The default database is (local)\SQLEXPRESS.



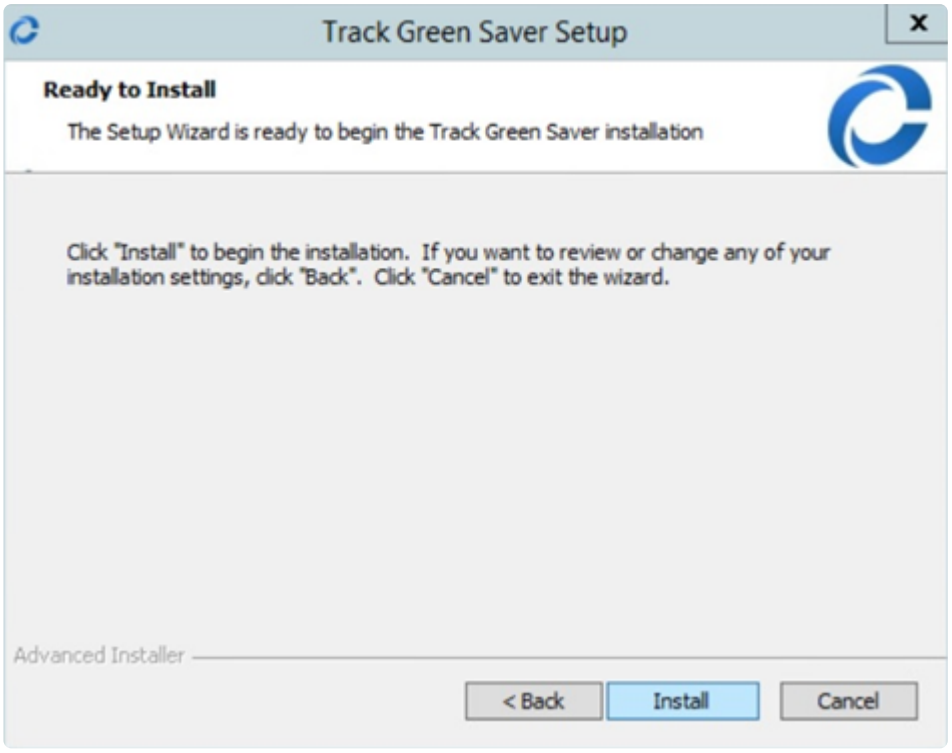
Options:

- Select **[Encrypted Connection]** checkbox to enable secured communication with SQL Server.
- Select **[Multi Subnet Failover]** checkbox to enable connection to (Always On) Availability Groups in case of failover in a multi-subnet environment.

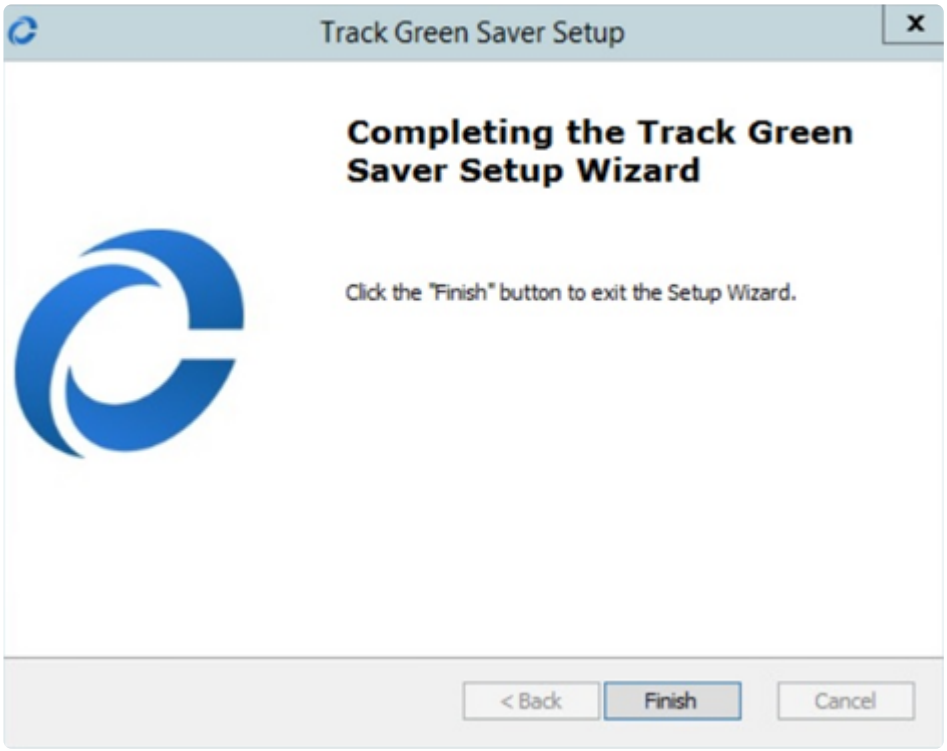
7. Click **[Test Connection]**.
8. Once the connection test is successful, click **[Next]**.
9. In the IIS Configuration window, enter the **[HTTP Port]** and **[HTTPS Port]** details. The default values are provided as 80 and 443 respectively. If required, change the port details and click **[Next]**.



10. When prompted, click **[Install]**.



11. When prompted to exit the Setup Wizard, click **[Finish]**.



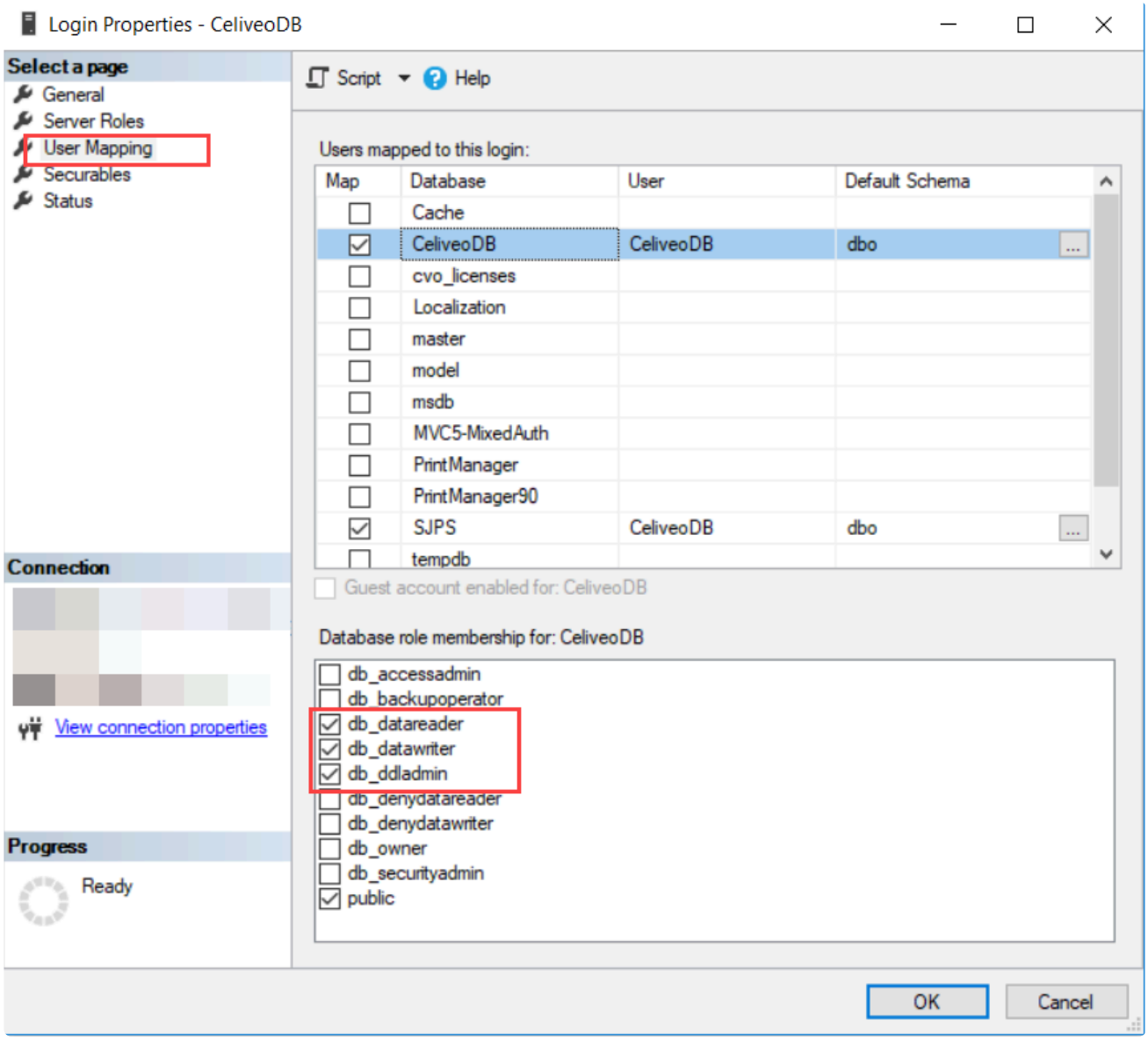
The Celiveo Reporting icon is added to the desktop.

Last modified: 29 September 2022

7.4. After Installation

After installation it is recommended to downgrade the rights for both set of SQL account credentials (TGS Service account and Celiveo database account) to their minimal level which are:

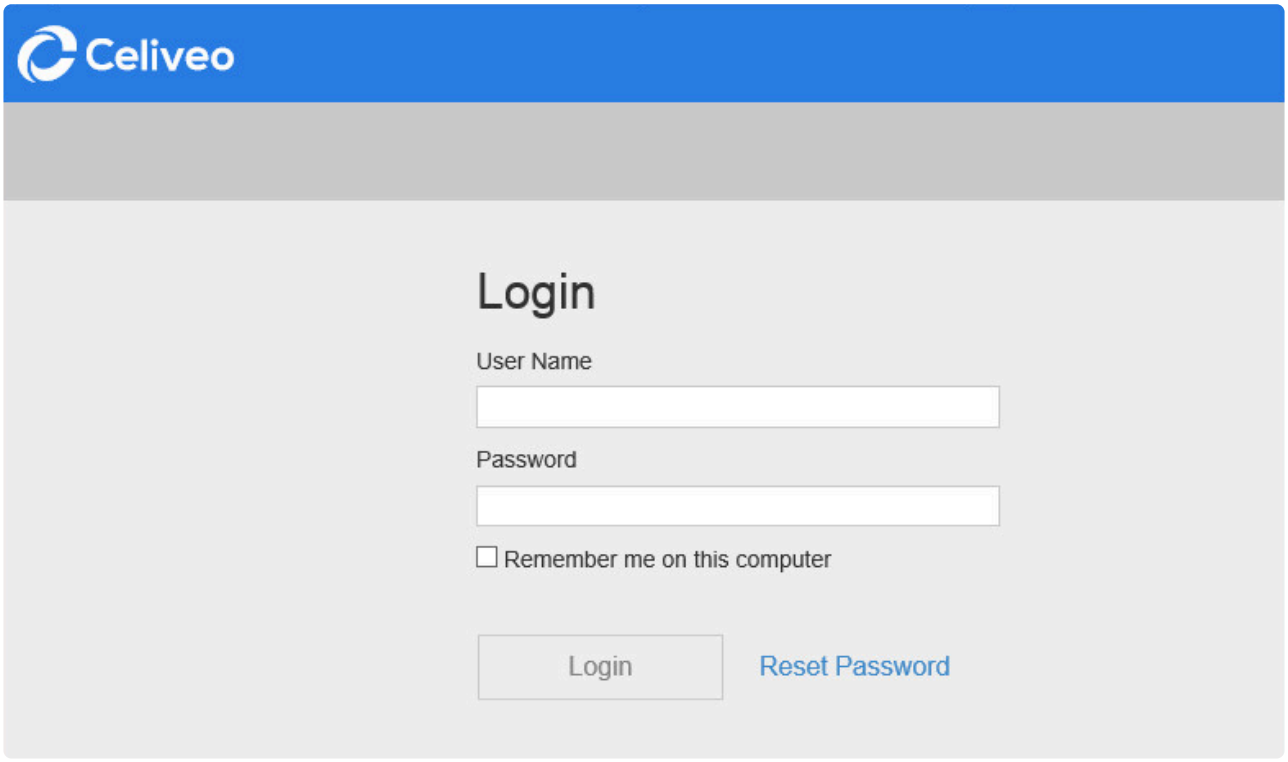
- *dbdatareader*
- *dbdatawriter*
- *ddladmin*



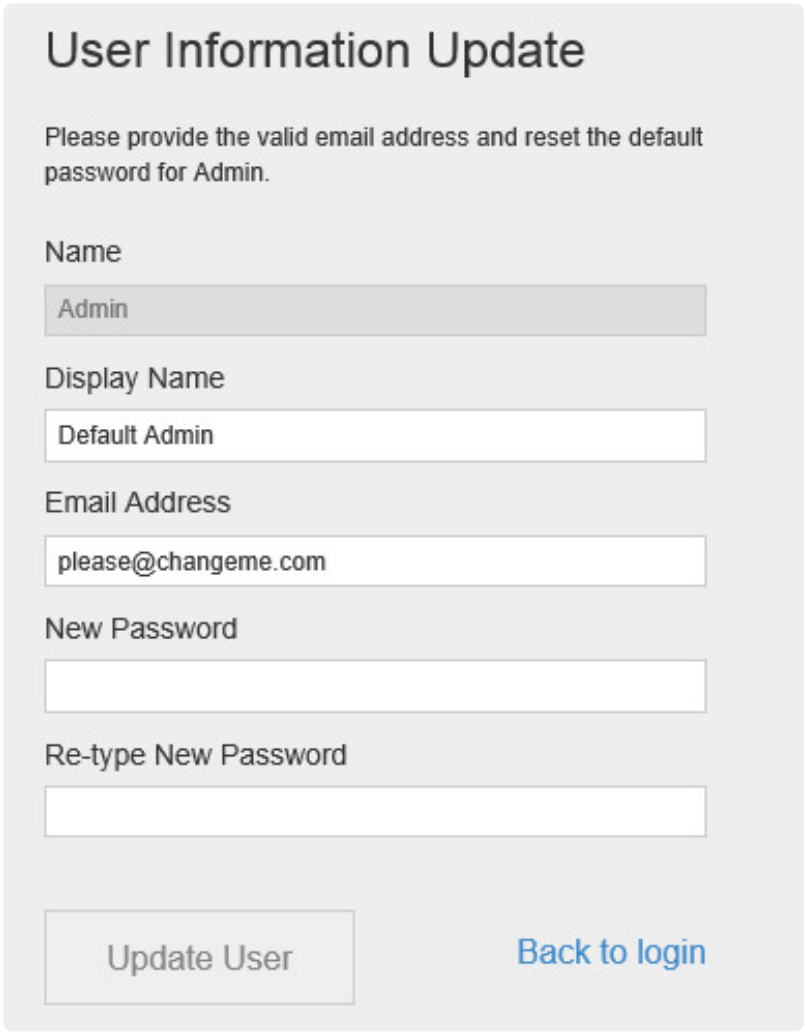
Last modified: 29 September 2022

7.5. Web Admin First Run

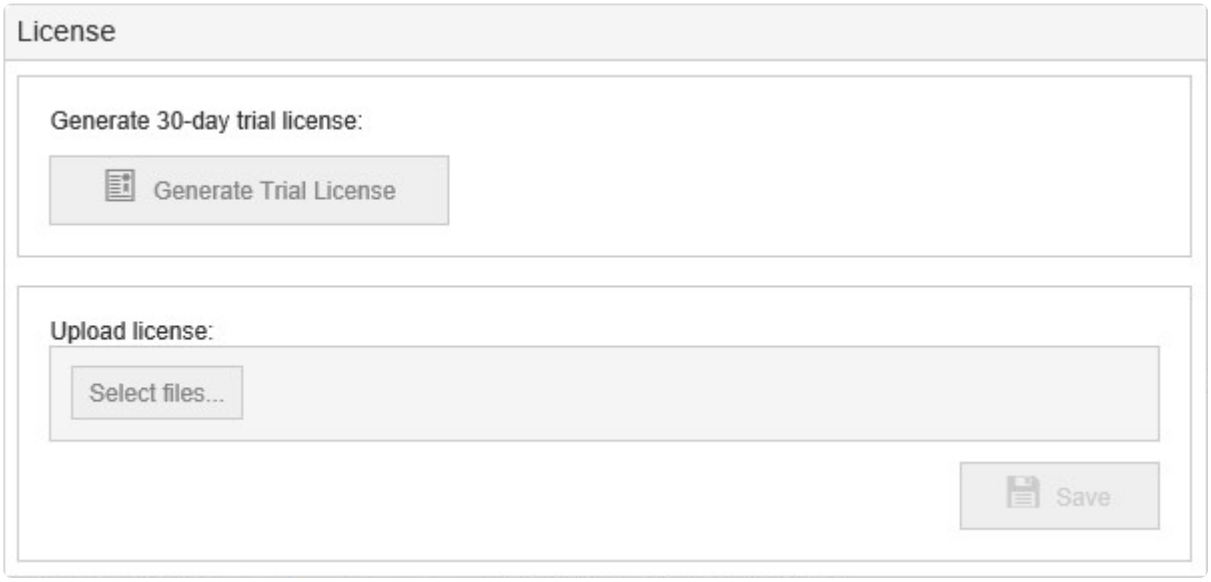
1. Double click the Celiveo Web-Admin icon on the desktop ( ). The initial logon screen of the Web Admin displays.



2. Specify admin as both the **[User Name]** and **[Password]**.
3. Click **[Login]**. The User Information Update screen displays.



4. At **[Email Address]**, specify a valid email address.
5. Specify a new password for the Default Admin user account.
6. Click **[Update User]**. The License screen is displayed.



Login with Non-Domain and Domain Users

Celiveo interfaces with two types of administrator users for Login:

1. **Non-Domain** users like the default administrator user, these are built-in in Celiveo Web Admin

and can be manually created. This configuration can be found on Managing System Administrators under **Create a Non-Domain User as an Administrator**

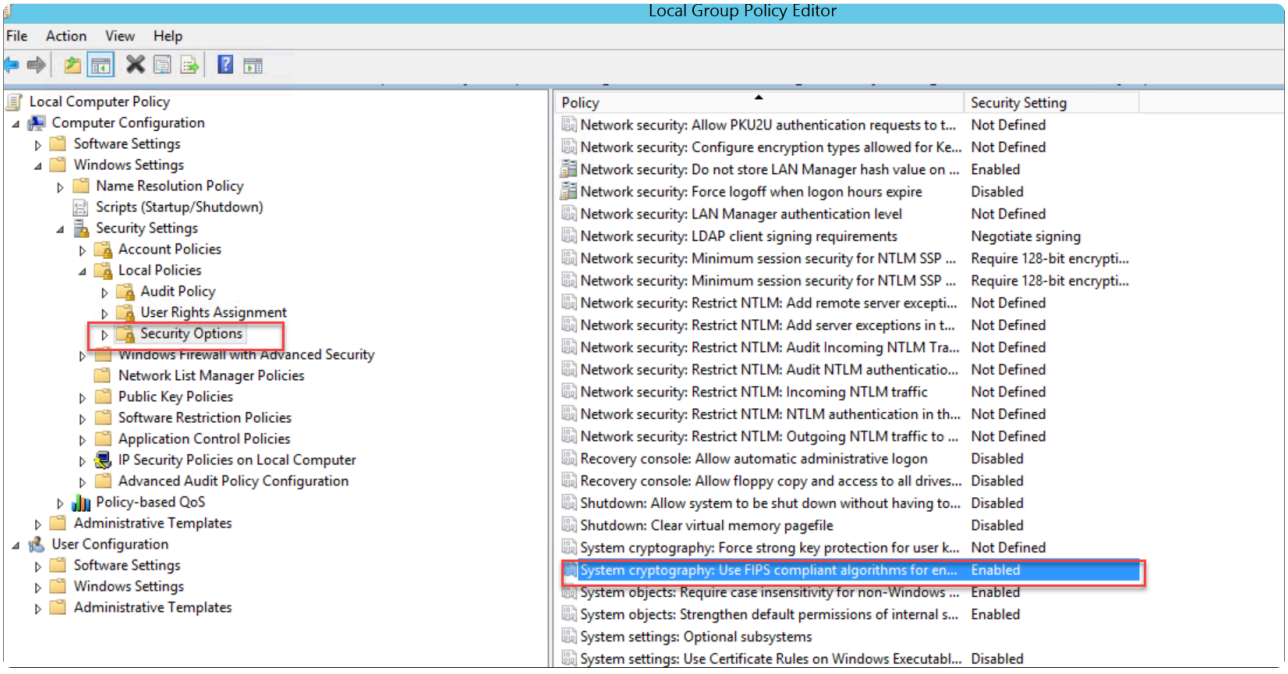
2. **Domain** users like the one that is used to login to the computer require configuration as the Web Admin requires to know to which Active Directory services it needs to contact to validate the user. This configuration can be found on Managing System Administrators under **Add Domain Users as Administrators**

> ! **IMPORTANT**: If your Windows Server is FIPS compliant (FIPS mode is enabled), make sure to disable FIPS mode before uploading the license. Once the license is successfully uploaded, you can enable FIPS mode again.

Click **[Select File]** to upload the license file provided, or click **[Generate Trial License]** to run as Celiveo Print-Direct for 30 days.

To disable/enable FIPS:

1. Log on to Windows Server as a Windows system administrator.
2. Click **Start**.
3. Click **Control Panel**.
4. Click **Administrative Tools**. (You may have to switch to large Icons for the next step.)
5. Click **Local Security Policy**. The **Local Security Settings** window appears.
6. In the navigation pane, click **Local Policies**, and then click **Security Options**.
7. In the pane on the right, double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.**



8. In the dialog box that appears, click **Disabled** to disable FIPS or **Enabled** to enable it again, and then click **Apply**.
9. Click **OK**.
10. Close the **Local Security Settings** window.
11. Open the command prompt terminal, enter **gpupdate /force**, and then reboot the system to apply the modifications. This ensures that policy settings change is applied successfully.

Last modified: 29 September 2022

8. Configuration

This sections details all configuration procedures for the Celiveo modules.

Add Printers in Web Admin
ZeroConfig
Multi- SQL Configuration
Configuring SQL Database for AlwaysOn Availability feature
Deploy a Celiveo Shared Virtual Printer Package on a Print Server
Deploy a Celiveo Virtual Printer on a User's Work Station
Deploy a Celiveo Virtual Printer on a User's Work Station
Set up Access
Synchronize Printers
Set the Session Timeout
Configuration to be done at the Printer

Last modified: 29 September 2022

8.1. Add Printers and their settings to the Web Admin

Celiveo Printers Discovery Agent helps you to import printers from an existing Print Server or find printers on the network.
You can also add printers manually.

Before you start

If the Web Admin is configured to run in HTTPS mode and Discovery Agent is run on a different machine than the one on which Web Admin is installed and Celiveo certificate is used then you need to import the Celiveo self-signed certificate to Trusted Root CA store where the Discovery Agent is running to import the printer/driver (use MS CertMgr).
The Celiveo self-signed certificate is found in the Web Admin installation directory:
…\Program Files\Celiveo\Celiveo 8\Web Admin
The certificate name is *.cer*
*Note:*The default setting is the usage of the Celiveo certificate, a self-signed certificate that is used during installation to configure the IIS to host the Web Admin.

If you want to use your own certificate:

- Install your own certificate whose issuer is trusted by all PCs on IIS.
  The certificate should have “localhost” in SAN (Subject Alternative Name) list
  OR
- You can change the sql.xml file to reflect the hostname/IP that your certificate supports.

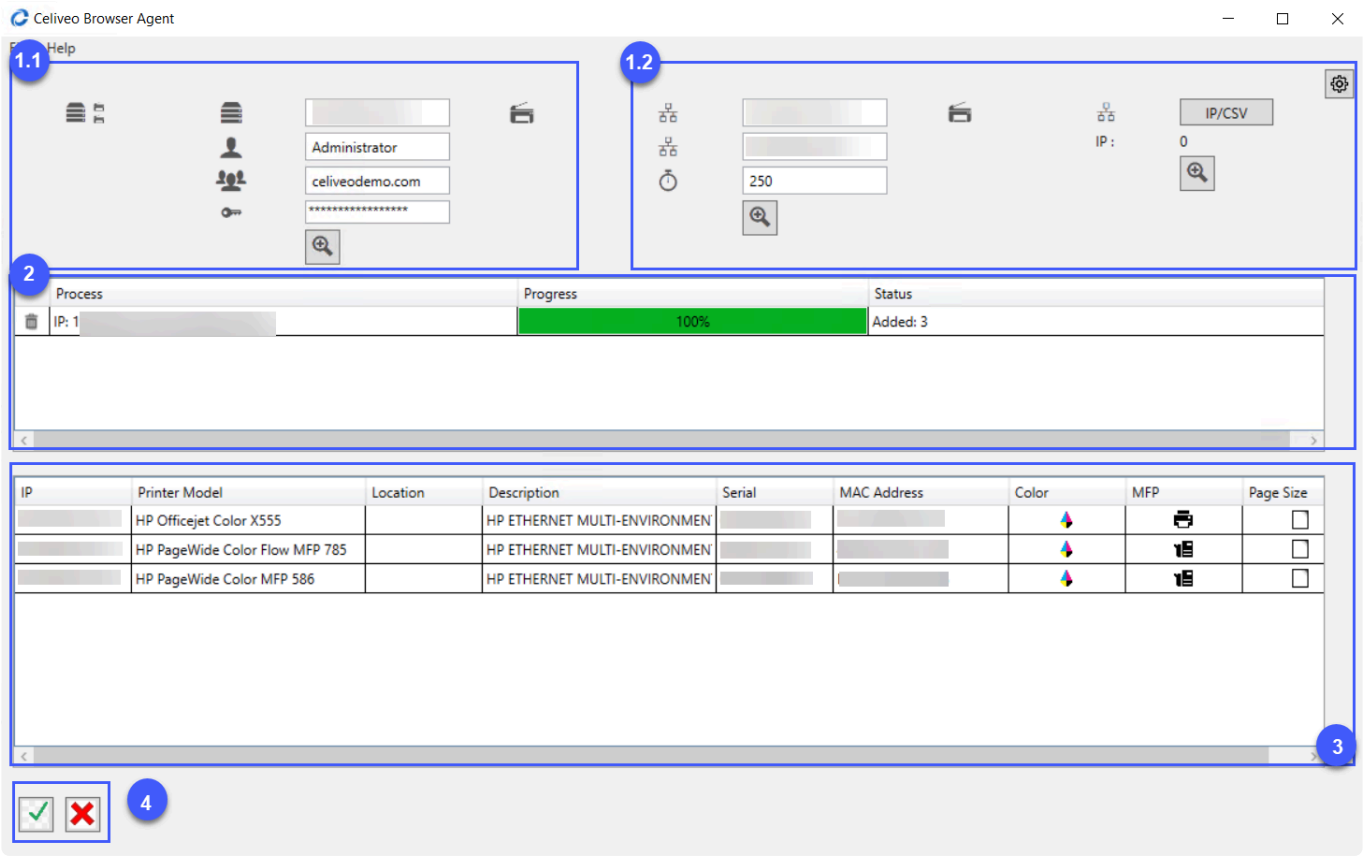
Workflow

Follow the below instructions to add printers to Web Admin:

Stage 1: Start Printer Discovery Agent

1. At the Main menu, click .
2. At the Printer menu, click .
3. At the Add Printer menu, click .

Note: If the Discovery Agent has not been installed earlier, the system downloads the installer and prompts you to install the Discovery Agent. Once installed the Discovery Agent starts.



Stage 2: Discover Printers

You can use one or both of the available options to search for printers in the network.

2.1 Discover printers from a print server

In the area marked 1.1 in the illustration above, enter the information and click on the Search icon.

- hostname or IP address of domain server,
- domain server administrator login,
- domain name and
- domain password.

2.2 Discover printers by scanning the network

In the area marked 1.2 in the illustration above, enter the information and click on the search icon.

- start range of the IP address to scan
- end range of the IP address to scan
- the timeout period for the scan duration (seconds)

Discovery is performed by executing an SNMP query. To change the SNMP settings, click on the settings icon.

Stage 3: Add Printer from Search Results

Search results are shown in the section marked 3 in the illustration above.

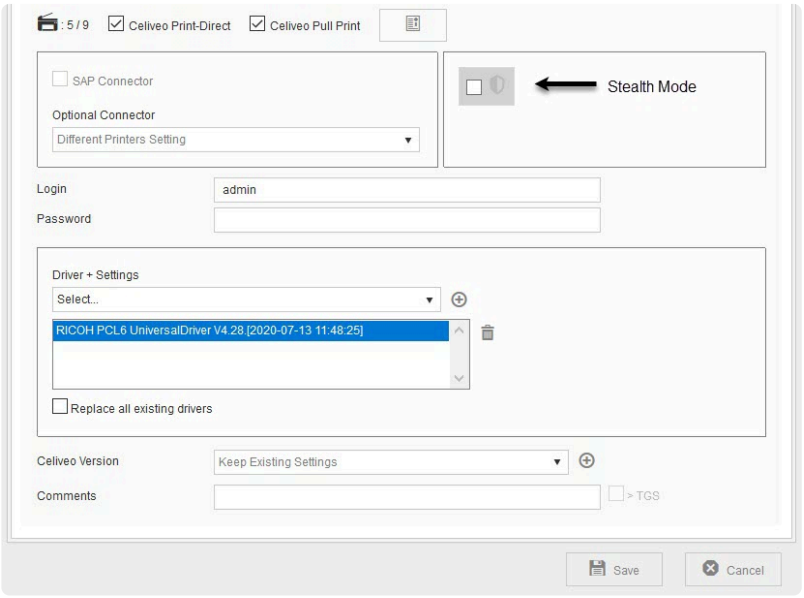
1. From the search results, select the printers you want to add.
2. Click ✔ at the bottom-right (see 4 in illustration above).
   You are returned to the Add Printer wizard. The printers that are reachable are displayed on the top half of the screen, while the printers that are unreachable are displayed on the bottom half of the screen.
3. Click **[Next]**.

Stage 4: Configure Printer Specific Information

The next stage displays a tabbed dialog box, where each printer type has a separate tab. The information you specify for each printer differs from one printer to another.

- Common Settings
- HP and HP Futuresmart Settings
- Ricoh Settings
- Konica Minolta Settings
- Lexmark Settings
- Xerox Settings
- Advanced Settings

Stage 4.1: Common Settings



1. You may choose **[Celiveo Pull Print]** or **[Celiveo Print Direct]** based on your configuration requirements.

Note: The Pull Printing feature is not available for Print Direct edition. Ability to select both Direct IP printing (Print-Direct) and Pull printing options is available only in

Business and Enterprise editions.

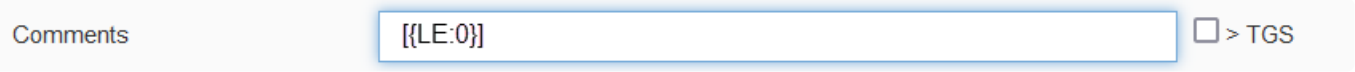
2. Click the **[License]** icon to view the information of product licenses that are available, applied, and/or expired.
3. **SAP Connector / Optional Connector**:
    - With Celiveo connectors, you benefit from a print solution tailor-made for the company's special needs while maintaining tight control over security, compliance, and costs. It enables you to release pull print jobs generated by the specified vertical connectors. You can choose the optional connector from the drop-down if you have a license acquired for the connector.
4. **Stealth Mode**:
    - This feature allows you to securely print confidential documents. While performing a pull print event, all your print jobs are displayed under the Print job list when you authenticate at the printer. The information is also tracked in tracking reports. Enabling this option for the printer, masks the document name. The document name will be replaced with four asterisks symbols prefixed and suffixed respectively with the first and last character of its original name. In the tracking reports, the document name will appear as "[first character]****[last character]".

Note: An Optional Connector with Stealth Mode (license) should be active to use this option.

5. **(Optional) Enter comments**:

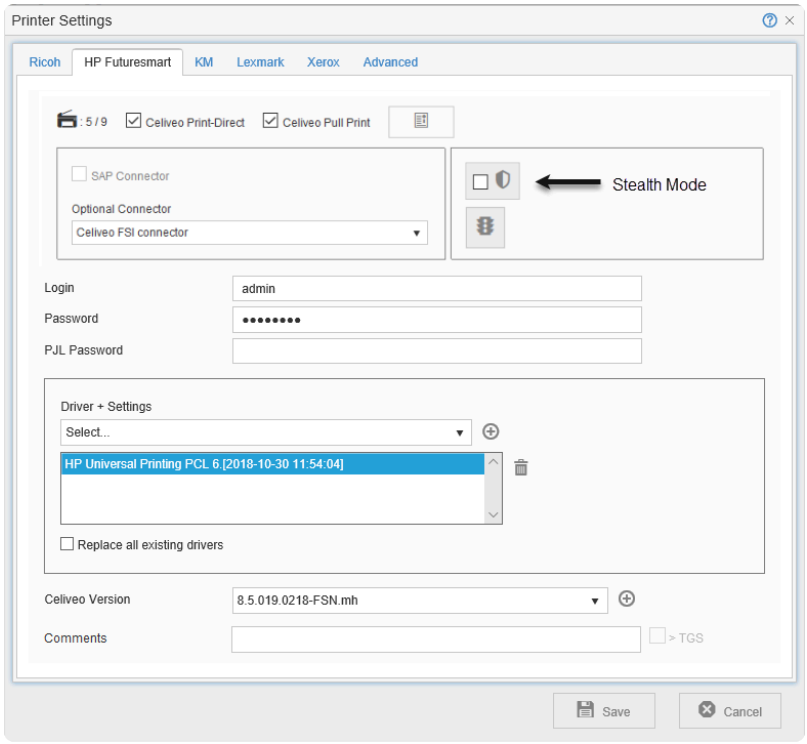
Enter any information for reference later. You can also use this field to define a reference code and opt to include it in the tracking information for Print-Direct printers.
To do so:
In the Printer Settings, enter a reference code in the Comments section and enable the **> TGS** checkbox.

Disable Log Encryption
It is possible to disable log encryption using the Comments field. To do so, enter the following command in the Comments field: ***[{LE:0}]***.



Note: If you are using **Celiveo Enterprise** edition, you can assign up to five drivers per printer. Thereby, you can have five different sets of printing preferences for the same printer, which translates into five print queues for the user. By renaming the driver+settings meaningfully, users can perceive each print queue as a preset for the same printer.

Stage 4.2: Settings for HP FutureSmart Printers

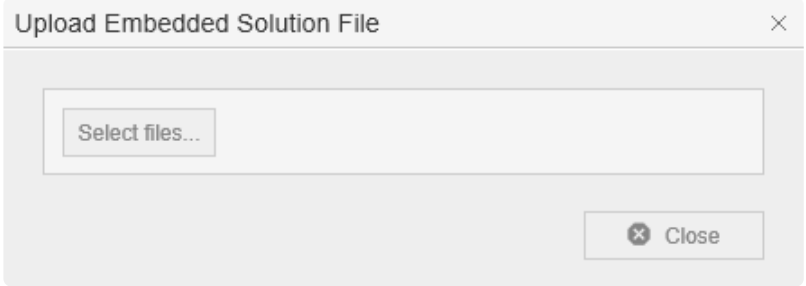


The button allows you to upload a customized OXPd Authorization Agent Configuration file. To learn more, see Custom Access Control for HP FutureSmart Printers

1. At **[Login]**, specify an account name with administrator privileges.
2. At **[Password]** specify the corresponding password.
3. At **[PJL Password]**, specify the password that authorizes Print Job Language (PJL) command strings.
4. At **[Driver+Settings]**, select the printer driver from the list. To add a new printer driver through Celiveo Printer Discovery Agent, click ⊕.

> **Note**: If HP Universal Print Driver (PCL5, PCL6 and PostScript emulation) is used to create the target print queue, it is **mandatory** to set it up in **Traditional Mode** and not Dynamic Mode.
> For further information on the differences between these two modes, see https://en.wikipedia.org/wiki/HP_Universal_Print_Driver

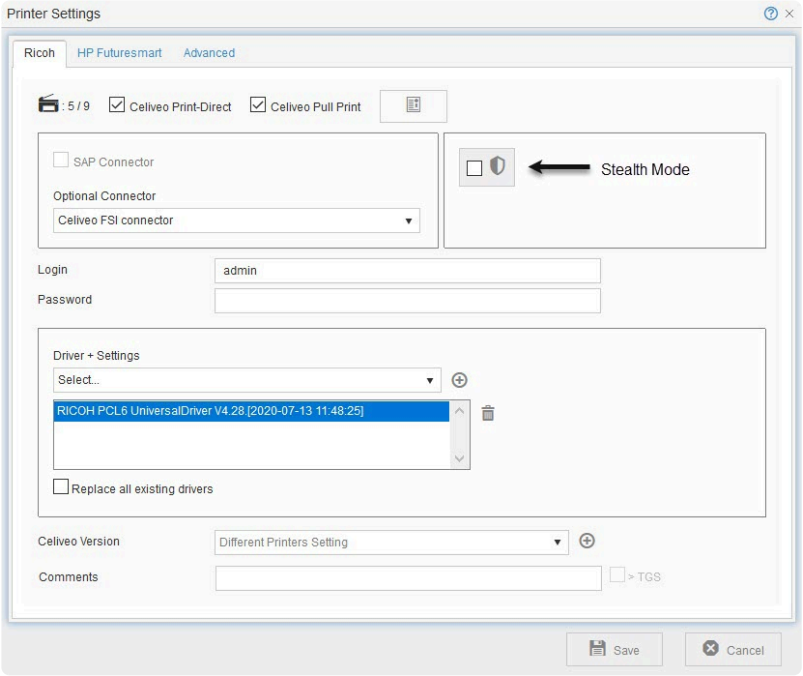
5. At **[Celiveo Version]**, click ⊕. The Add Celiveo Version dialog displays.



6. Select the firmware file provided by Celiveo to “Celiveo-enable” HP FutureSmart printers (*.mh).
7. For non-FutureSmart (Celiveo Smart Appliance agent enabled printers), choose the (* .mc/*.bmc)

file.

Stage 4.3: Settings for Ricoh Printers

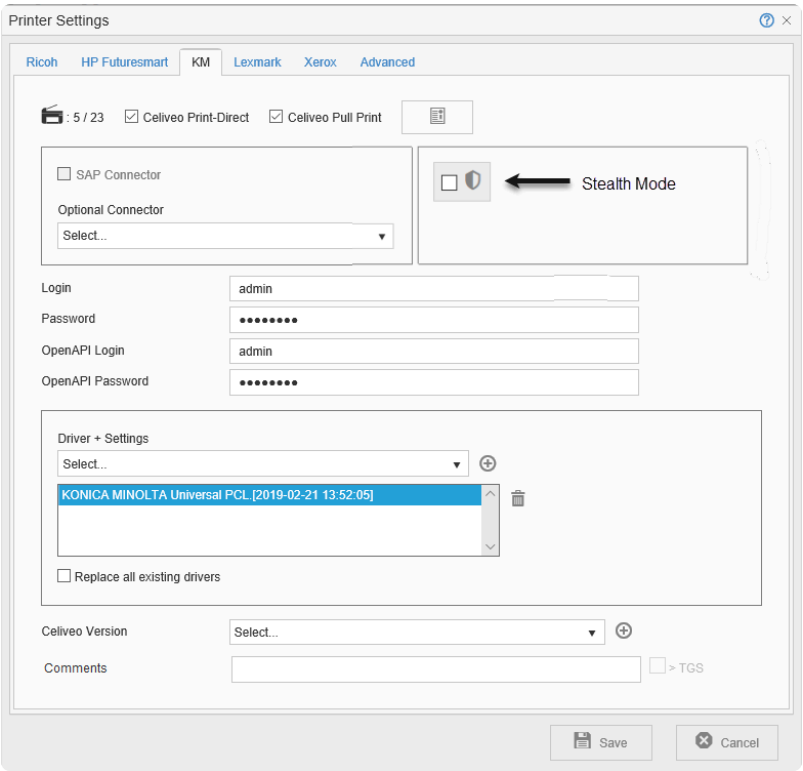


1. At **[Login]**, specify a user name with administrator privileges.
2. At **[Password]** specify the corresponding password.
3. At **[Driver+Settings]**, select the printer driver from the list. To add a new printer driver through Celiveo Printer Discovery Agent, click ⊕.

> **Note**: If you are using a Ricoh printer, please make sure you only use PCL6 drivers.

4. At **[Celiveo Version]**, for Ricoh Android SOP 2.x printers, choose the **.mr file to install the Business Edition Embedded agent for Ricoh. For CSA agent enabled printers, choose the *.mc/**.bmc file.

Stage 4.4: Settings for Konica Minolta Printers

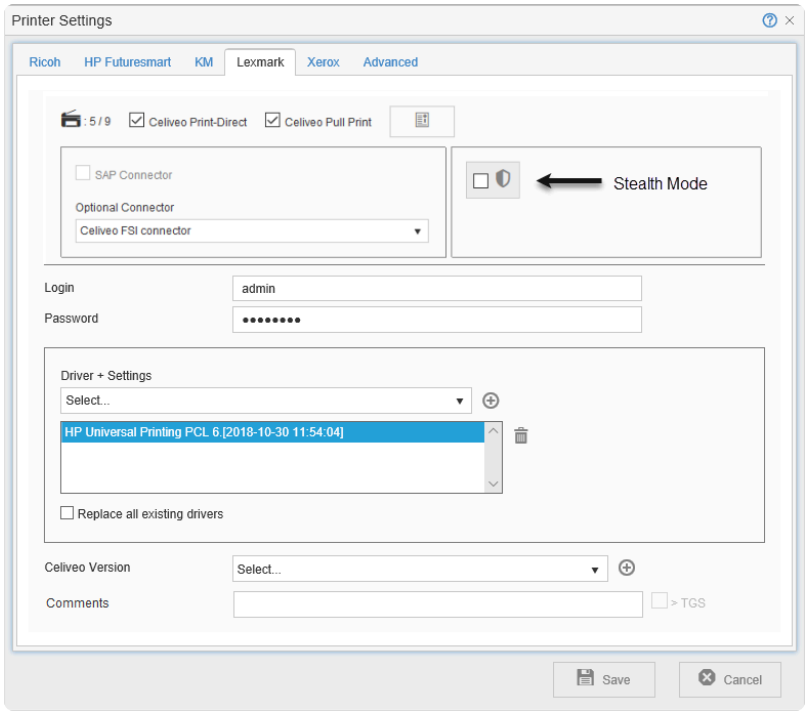


1. At **[Login]**, specify the administrator user name.
2. At **[Password]** specify the administrator password.
3. At **[OpenAPI Login]** specify the login name for the Open API authentication layer.

> Note: You need to specify the Open API settings only if the Konica Minolta printer uses the authentication layer.

4. At **[OpenAPI Password]** specify the password for the Open API authentication layer.

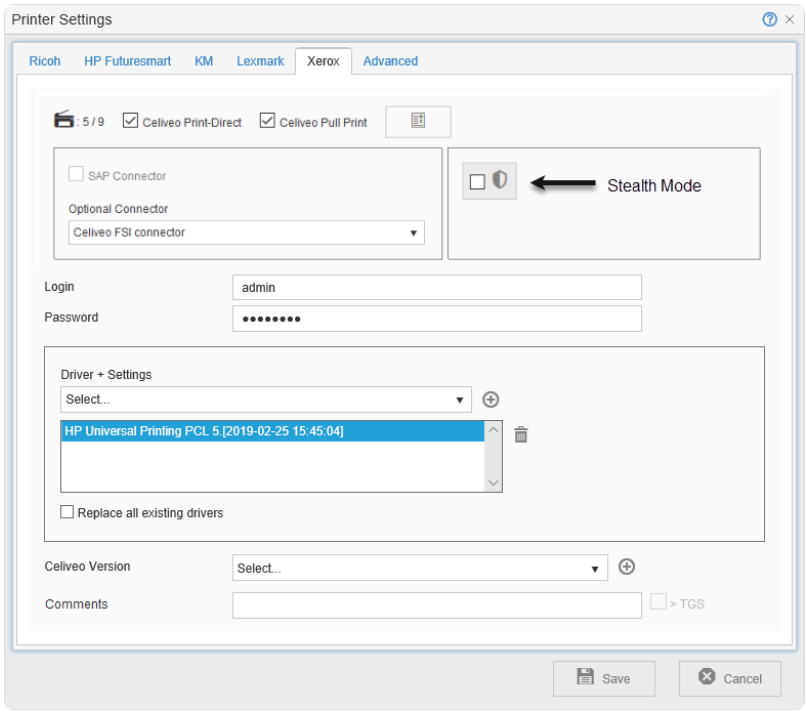
Stage 4.5: Settings for Lexmark Printers



At **[Login]**, specify an account name with administrator privileges.
At **[Password]** specify the corresponding password.
At **[Driver+Settings]**, select the printer driver from the list. To add a new printer driver through Celiveo Printer Discovery Agent, click ⊕.

> **Note**: Recommended drivers for Lexmark printers are PCL6/PS. In some cases, the PCL6 driver processes the jobs as B/W but the spool is marked as color which generates errors in the tracking reports.

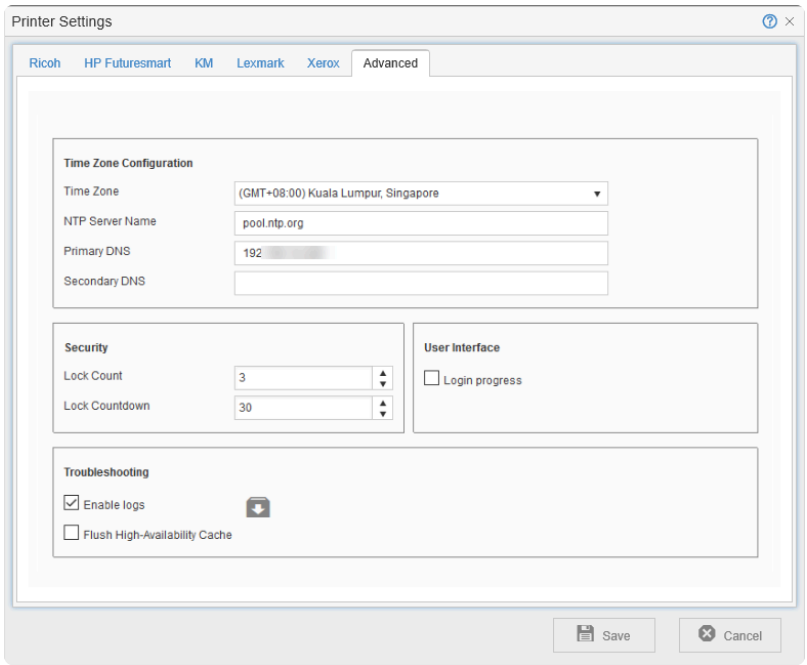
Stage 4.6: Settings for Xerox Printers



At **[Login]**, specify the System Administrator login name.
At **[Password]** specify the corresponding password.
At **[Driver+Settings]**, select the printer driver from the list. To add a new printer driver through Celiveo Printer Discovery Agent, click ⊕.

> ! For Xerox printers, it is compulsory to use the Xerox PullPrint Postscript Driver, available here.

Stage 4.7: Advanced Settings



These settings help you to:

- Configure the time zone settings for tracking of information by the printer.

> This option is not available for non-CSA agent-based printers, i.e. printers where Celiveo Smart Appliance agent is not installed.

Menu option	Description
Time Zone	Select the preferred time zone.
NTP Server Name	The Network Time Protocol (NTP) is typically used by hundreds of millions of computers and devices to synchronize their clocks over the Internet. Edit the IP address or domain name of the NTP server if required.
DNS Primary	Automatically pre-filled with the IP address of the primary domain server from Web Admin. Edit the address if required.
DNS Secondary	Automatically pre-filled with the IP address of the backup domain server from Web Admin. Edit the address if required.

- Configure Security settings on the Printer screen for failed authentication.

Menu option	Description
Lock Count	Defines the number of failed authentications before the printer screen locks. Lock Count default value is 3 but can be modified to a value between 1 and 9.
Lock Countdown	Defines the time in seconds the printer screen locks after the number of failed authentications defined by **[Lock Count]** is reached. Lock Countdown default value is 30 but can be modified to a value between 15 and 180.

- Configure settings for troubleshooting.

Menu option	Description
Enable Logs	Logs provide information on the activities of Celiveo and the connected printers. Select **[Enable logs]** to enable collection of logs. **IMPORTANT NOTE: This option should only be set at the request of Celiveo and for the indicated duration. It produces an encrypted file that is not usable by end-users.**
Flush High-Availability Cache	This is applicable if an Optional Connector with high-availability feature (license) is available for the printer(s). If the license is not applied to the printer, then this option is disabled. Selecting this option enables data to be purged from the cache regularly at predefined intervals. **NOTE: It is important to synchronize the printer(s) after selecting this option**.

If you are adding a printer with the Add Printer wizard,

Click **[Next >]** to go to the next step of the Add Printer wizard.

If you are editing the settings of a connected printer,
Click **[Save]** to continue.
To apply the settings on the target printer, click the “synchronize printer” icon.

Stage 5: Finalize

1. Click **[Next]**. until you arrive at the Save Confirmation dialog.
2. Click **[Save]**.

Last modified: 6 December 2022

8.2. Add Printers Manually

Before you begin…

While adding a printer, you may need to upload its driver to the Celiveo database. The Add Printer wizard launches the Discovery Agent to enable you to import the driver from the workstation you are running the wizard on. So before you start, make sure that the workstation you are working on has all the required printer drivers installed on it.

Note: Celiveo cannot import class drivers, so ensure that the drivers installed on the workstation is not a class drivers.

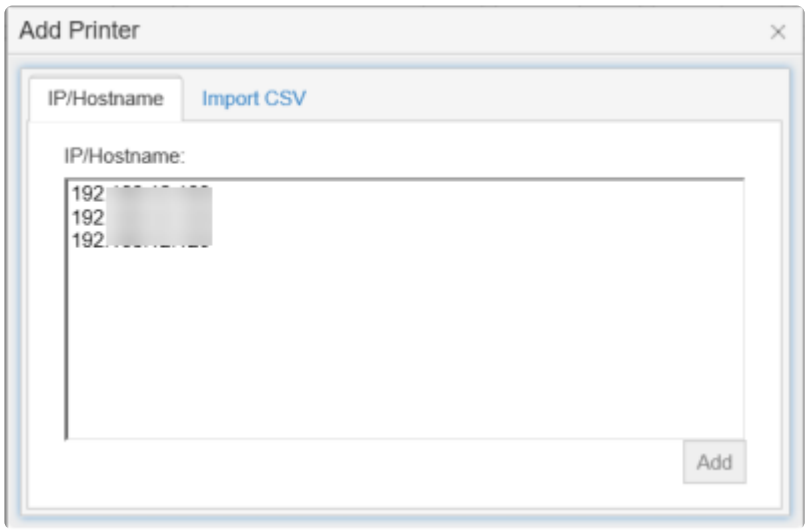
Stage 1: Start Add Printer Wizard

1. At the Main menu , click Display Printers.
2. At the Printer menu, click .
3. At the Add Printer menu, click . The Add Printer dialog displays.

Stage 2: Specify Printers

You can specify IP addresses of printers, by directly entering them to the Web Admin, or importing them from a comma separated values (CSV) file.

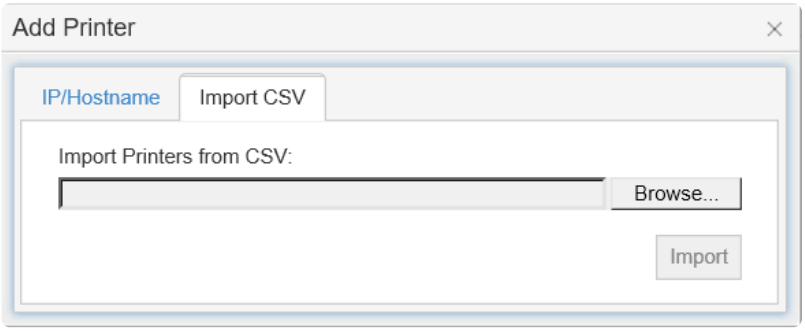
2.1 Specify Printers by IP Address or Hostname



1. At **[IP/Hostname]**, enter the IP address or host names of the printers.
2. Click **[Add]**.
3. When prompted to start the Discovery Agent, click **[Open]**.

Note: If the Discovery Agent has not been installed earlier, the system downloads the installer and prompts you to install the Discovery Agent. Once installed, the Discovery Agent starts.

2.2 Specify Printers by Importing their IP Addresses from a CSV File



1. Click the **[Import CSV]** tab.
2. Click **[Browse]**.
3. Select the CSV file to upload and click **[Open]**.
4. Click **[Import]**.
5. When prompted to start the Discovery Agent, click **[Open]**.

Note: If the Discovery Agent has not been installed earlier, the system downloads the installer and prompts you to install the Discovery Agent. Once installed, the Discovery Agent starts.

Stage 3: Select Printers

The Discovery Agent validates the IP Addresses / Hostnames you provided. If any of them are not reachable, a message is displayed to inform you what IP Addresses / Hostnames are invalid.

Note: Validation is performed by executing an SNMP query. To change the SNMP settings, click on the ⚙ settings icon.

1. From the list of valid printers, select the printers you want to add.
2. Click ✓ at the bottom-right.
   You are returned to the Add Printer wizard.
3. Click [Next].

Stage 4: Configure Printer Specific Information

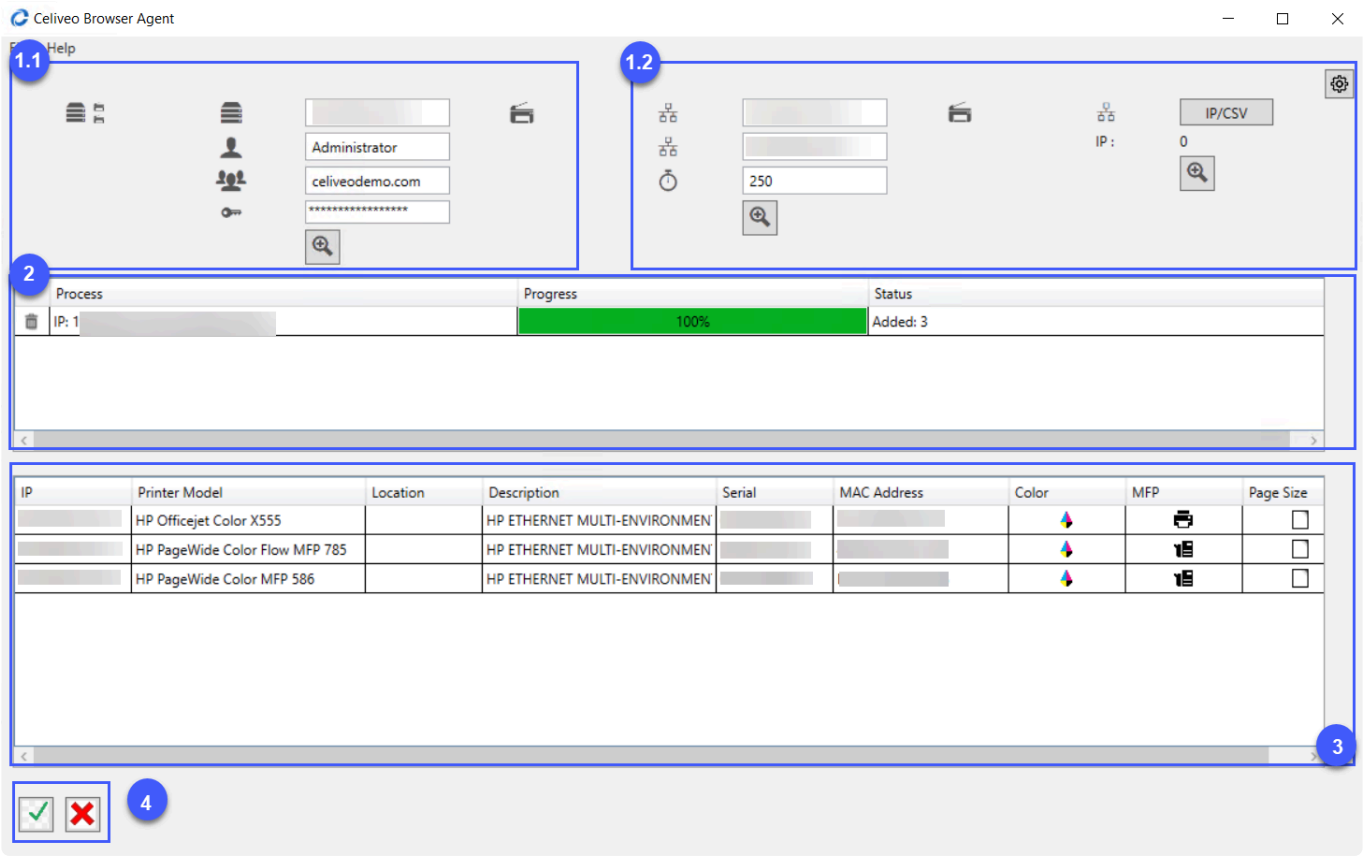
The next stage displays a tabbed dialog box, where each printer type has a separate tab. Repeat the instructions below for each tab.

Stage: 4.1: Basic Information

1. Ensure that the **[Celiveo Print Direct]** check box is selected.
2. If the printer you are adding is an HP printer, and a PJL password had been set in the HP Embedded Web Services, in the **[PJL Password]** box, specify the password.

Stage 4.2: Specify Driver

Typically, when you import printers from a Print Server, it imports the required drivers and default preferences as well. However, if you add printers by scanning IP addresses, you must import the printer drivers from the workstation you are running the Add Printer wizard from.



From the [Driver + Settings] drop-down, select a printer driver.
If the driver that matches the printer is not on the list:

1. Click the **[+]** icon adjacent to the **[Driver + Settings]** drop-down . The Discovery Agent displays.
2. In the area marked 1, click on the Search icon. The search results are displayed in the area marked 3.
3. Select the driver to use.
4. Click at the bottom-right (see 4 in illustration above).
5. From the **[Driver + Settings]** drop-down, select the printer driver you just added.
   You are returned to the Add Printer wizard.

Stage 4.3: Specify Celiveo Version

The Celiveo Version refers to the Celiveo firmware that runs on a printer or Celiveo Smart Appliance agent (CSA). Typically, the CSA agent comes pre-loaded with the correct firmware. However, if you are adding a printer that does not require a CSA (for example, a HP FutureSmart printer or Ricoh Android SOP 2.x printer) you must explicitly upload the Celiveo Version.

If the printer you are adding requires a CSA:

At **[Celiveo Version]**, select [Keep Existing Settings].

If the printer you are adding does not require a CSA:

1. Click the **[+]** icon adjacent to the **[Celiveo Version]** drop-down. The Add Celiveo Version dialog displays.
2. Click **[Select Files]**.

3. Pick the **.mc /**.mh /*.bmc /*.mr file provided for the printer.

Note: If not already provided, you can download the Celiveo Version files from the Downloads section.

Stage 4.4 (Optional) Enter Comments

Enter any information for reference later. You can also use this field to define a reference code and opt to include it in the tracking information for Print-Direct printers.
To do so:
In the Printer Settings, enter a reference code in the Comments section and enable the **> TGS** checkbox.

Stage 5: Finalize

1. Set up Access
2. The remaining steps on the Add Printer wizard can be specified later, and not essential for Celiveo to be functional. For the purpose of this tutorial, we will skip these steps.
3. Click **[Next]** until you arrive to the Save Confirmation dialog.
4. Click **[Save]**.

Last modified: 29 September 2022

8.3. ZeroConfig

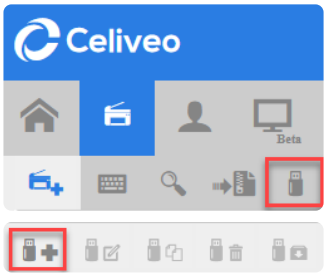
What is ZeroConfig?

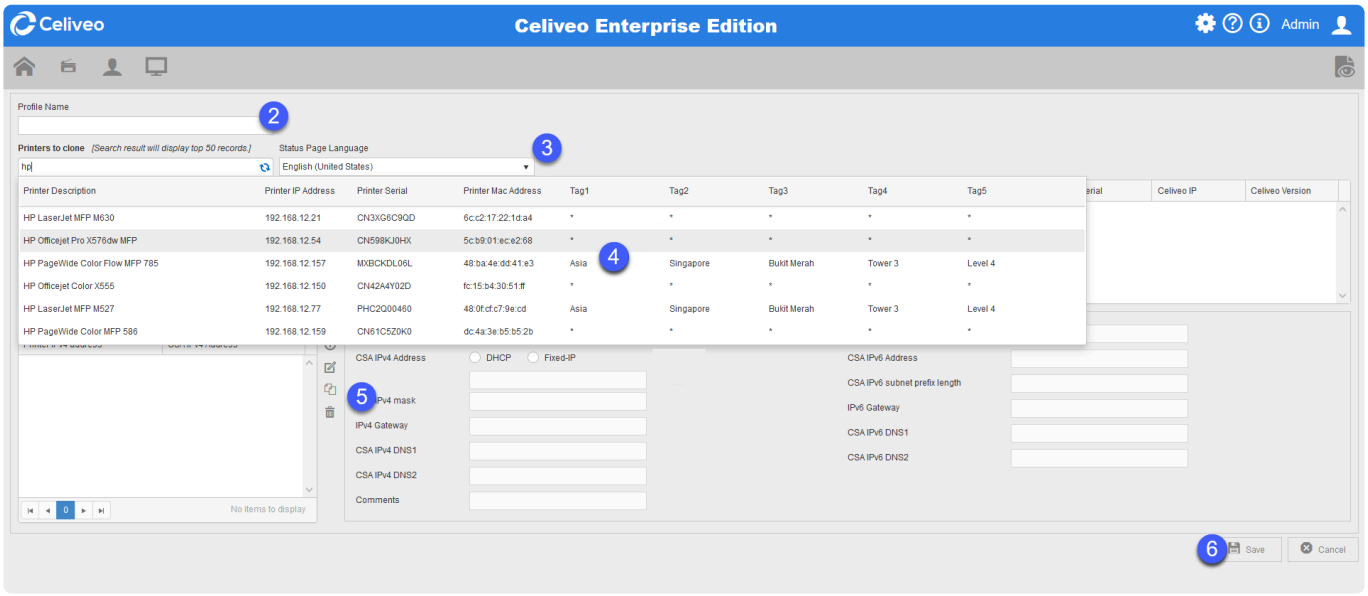
Celiveo ZeroConfig allows you to create Printer Configuration Profiles to deploy on multiple printers without having to synchronize them.

ZeroConfig installation for Celiveo Smart Appliance

Add a ZeroConfig Profile in Web Admin

1. In the Add Printer section, click the ZeroConfig button. Then click the **Add** button.



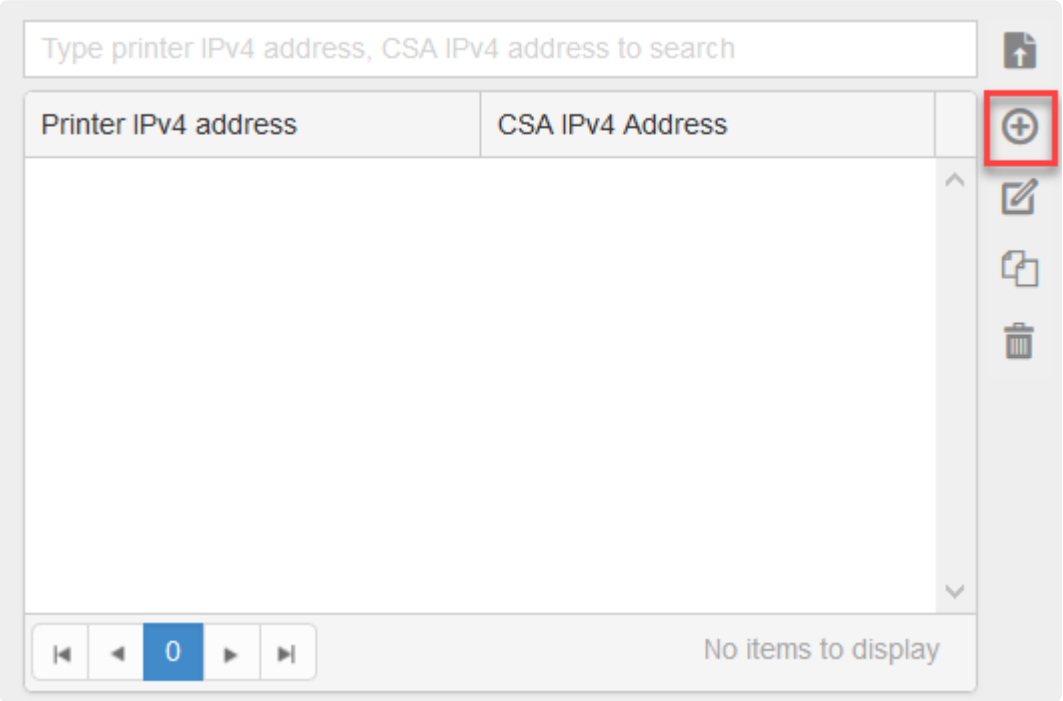


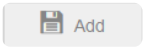
2. Enter a profile name.
3. In the **Status Page Language** drop down-list, select the language of the CSA Status Page to display.
4. In **Printers to clone**, select the master printers to use as a reference.
5. Add or import IP Profiles.
6. Click **Save** to save the configuration profile.

Create or import an IP Profile

Create a new Profile

To create a new profile, click the + button



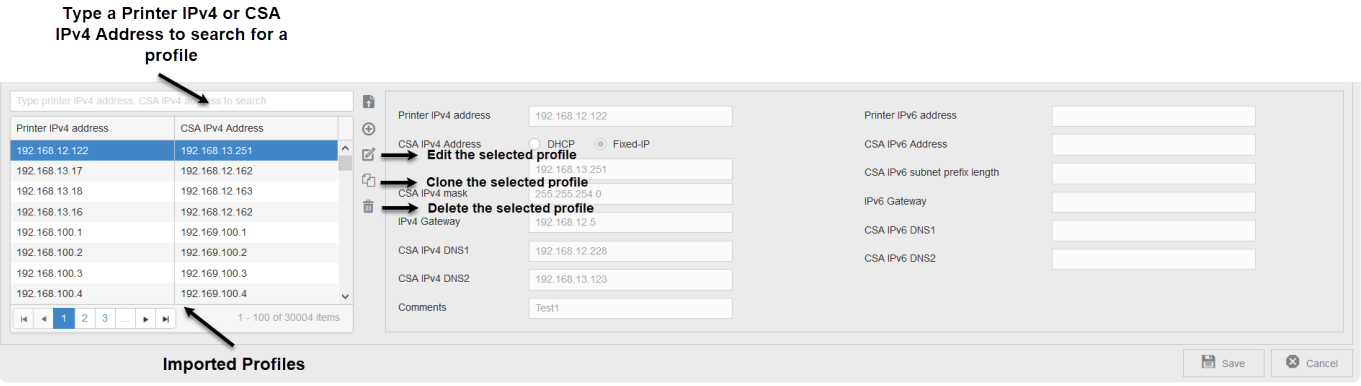
1. Select the type of CSA IPv4 Address.
2. Enter the details.
3. Click the **Add**  button to save the new profile.

Import IP Profiles

It is possible to import a CSV file containing a list of IP Profiles. To do so:

1. Click the **Import** button.
2. Select your CSV file and click **Open**.

The imported profiles appear on the left.

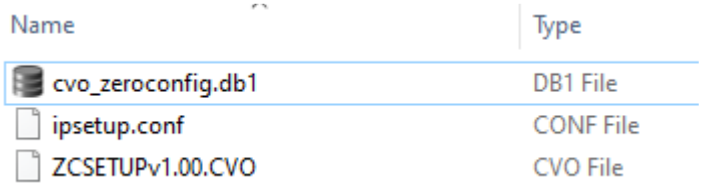


Download the Configuration Profile

1. Select the profile.
2. Click the **Download ZeroConfig Package** icon .

Deploy the Configuration Package

1. Unzip the downloaded package. It contains the following files:



2. Copy the files to a USB drive.
3. Power off the CSA and connect the USB drive.
4. Power on the CSA. Once the process is successful:
    - A print out from the printer saying that the zero config is successful is sent.
    - The Web Admin now contains a new record for the printer with synchronization successful status.

Note: if the CSA is not listed in the Update directory on the USB drive, then it will be updated, even if the CSA firmware is the same as the one on the USB drive.

ZeroConfig installation for HP FutureSmart Printers.

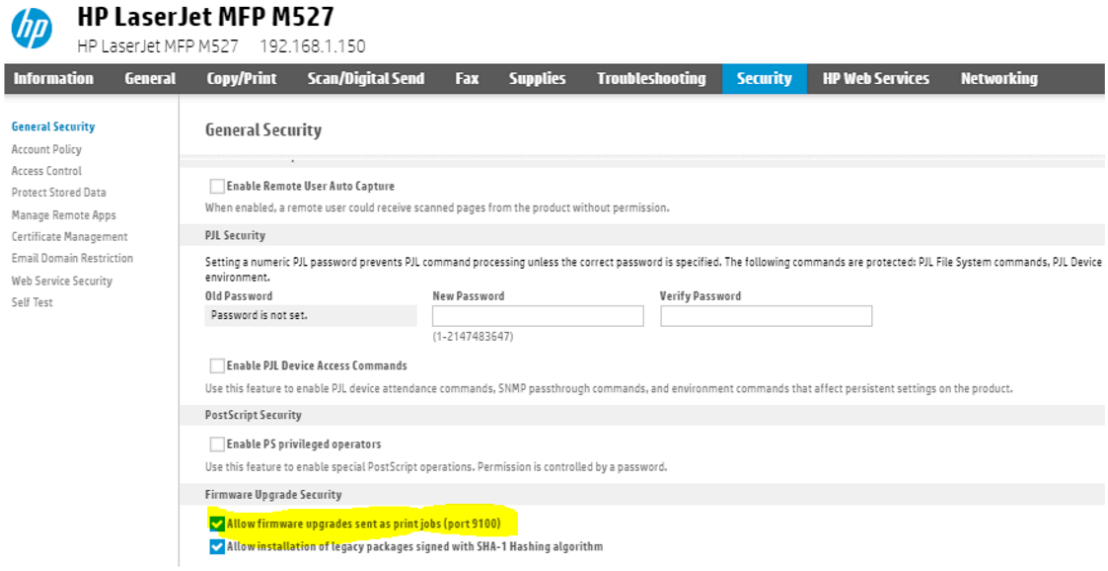
Prerequisites

Important Note:

- The new printer must have the **same EWS username and password as the master printer**.
- The supported HP firmware is FutureSmart **4.7.3.1 or later**.

If you are using **HP firmware FutureSmart 4.10 or later**, please enable the below setting via EWS:

Navigate to **Security** and enable the **Allow firmware upgrade sent as print job (port 9100)**.

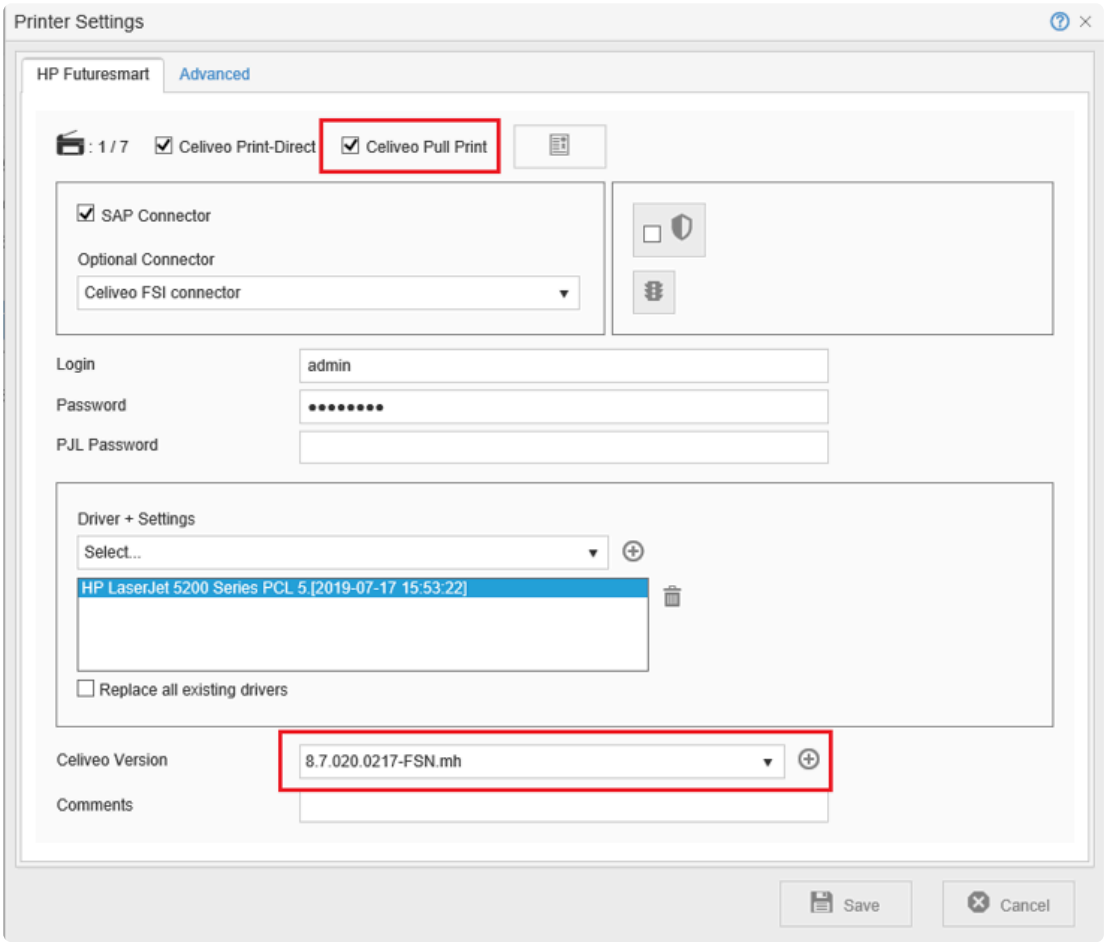


Preparing a master printer for ZeroConfig installation

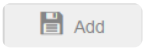
Define an HP Future Smart printer as master printer in the Web Admin. The master printer model should match the printer which will be installed by ZeroConfig.

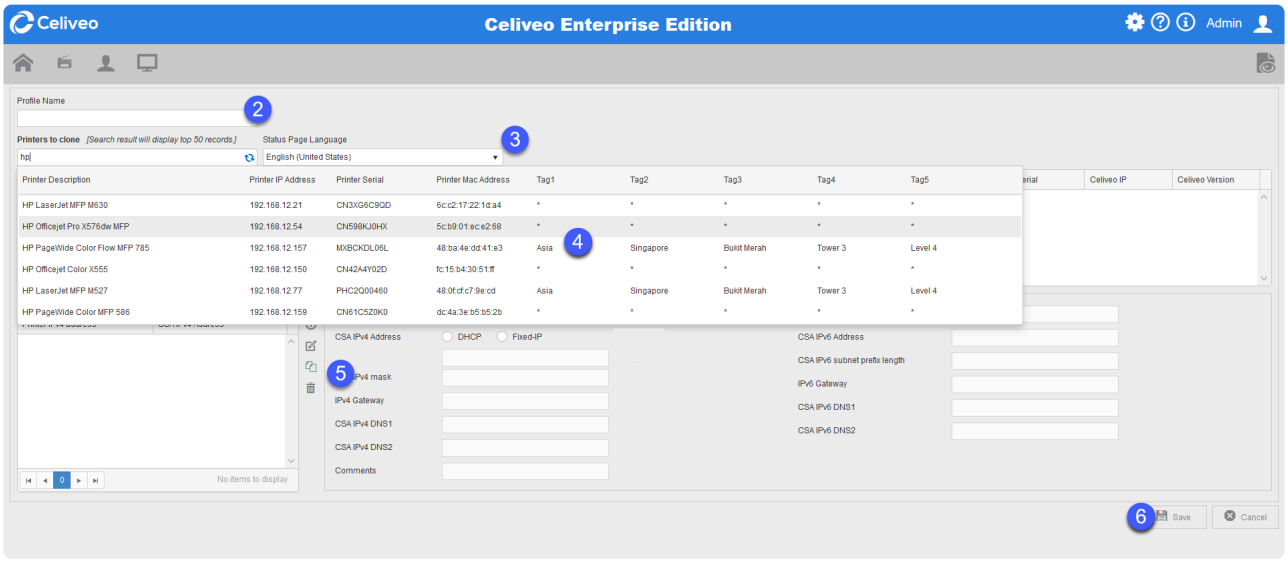
E.g. the master printer for an HP Color LaserJet MFP **M553** should be an HP LaserJet **M553**.

1. In the printer settings of the master printer, enable the **Celiveo Pull Print** checkbox and select the latest .mh file.



Add a ZeroConfig Profile in Web Admin

1. Click the **Add**  button.



2. Enter a profile name.
3. In the **Status Page Language** drop down-list, select the language of the Status Page to display.
4. In **Printers to clone**, select the master printers to use as a reference.
5. Add or import IP Profiles. To learn more about IP Profiles, see above.
6. Click **Save** to save the configuration profile.

Download the Configuration Profile

1. Select the profile.
2. Click the **Download ZeroConfig Package** icon .

Install the Celiveo Solution by ZeroConfig

1. Turn off the printer and insert the USB drive to the printer USB port.
2. Turn on the printer to install Celiveo Solution by ZeroConfig. The process for installing the solution can take up to 15 minutes.

Important Note:

Please make sure that new printers have the same EWS username and password as the master printer.

3. Once the process is done, a printout from the printer saying that the ZeroConfig is successful is sent. It might take some time (up to 1 minute) to have the Celiveo Solution on the Printer Panel. If it is synchronized successfully, the new printer appears in the Web Admin.

Last modified: 29 September 2022

8.4. Celiveo Virtual Printer for Windows

The Celiveo Virtual Printer (CVP) is an autonomous client package including UI, services, and a port monitor. It is meant to be installed on a Windows or macOS Client PC, to provide ZeroServer Pull Print service. Print jobs are retained on the PC of the user who prints them, therefore reducing network traffic, increasing security, and removing the need for a print server. It is configured on the Celiveo Web Admin portal as a virtual printer, and the self-sufficient and compact package is downloaded with just a click and can be deployed silently by any remote installation software, or manually.

Topics:

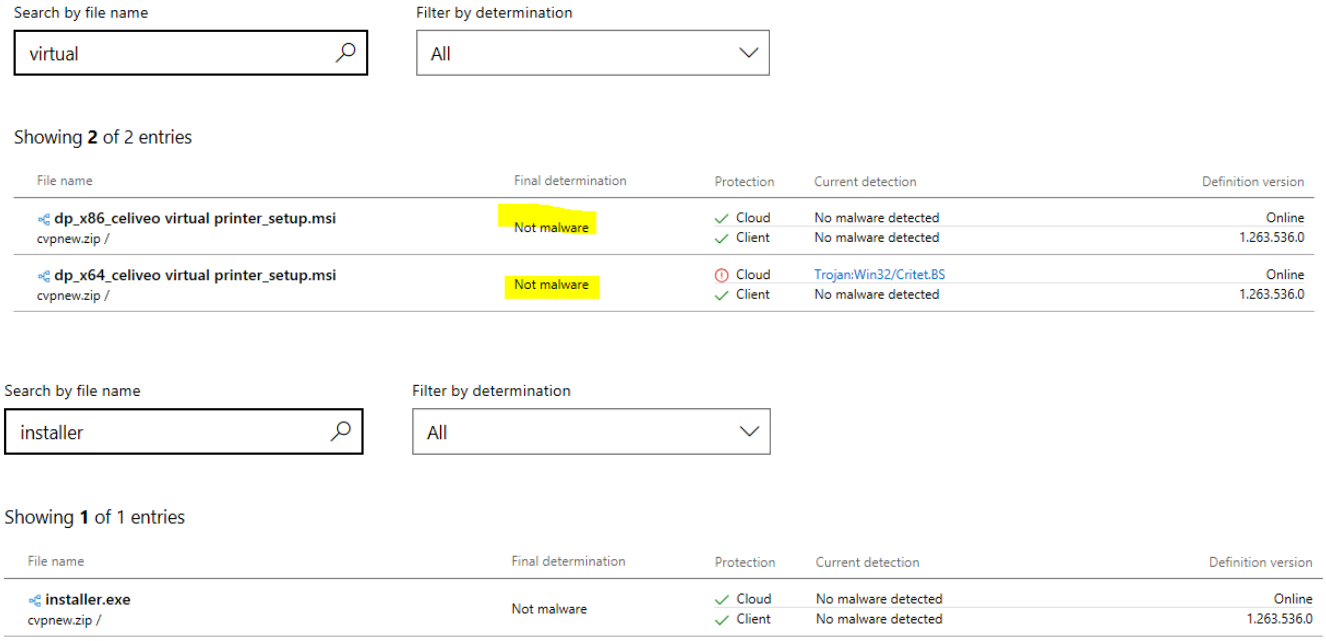
Antivirus False Positive cases
Add a Celiveo Virtual Printer to Web Admin
Add a Celiveo Shared Virtual Printer to Web Admin
Add a Celiveo Virtual Printer for Print-Direct
Deploy a Celiveo Shared Virtual Printer Package on a Print Server
Deploy a Celiveo Virtual Printer on a User's Work Station For Pull Printing
Deploy a Celiveo Virtual Printer on a User's Work Station For Direct IP Printing

Last modified: 29 September 2022

8.4.1. Antivirus False Positive cases

In some cases, the Windows Defender or Symantec Endpoint antivirus identifies Celiveo Virtual Printer as a threat.

We have submitted the file to Microsoft for a malware analysis who confirmed this was a **false positive** as proven by the reports below:



To avoid this problem, make sure that you add Celiveo to the antivirus exclusion list. To do so
- For Windows Defender, add the “C:\Program Files\Celiveo” folder to the exclusion list : https://support.microsoft.com/en-ie/help/4028485/windows-10-add-an-exclusion-to-windows-defender-antivirus.
- For Symantec Endpoint, follow the procedure described here.

Celiveo software executable files are verified virus/malware using eSET Nod32, then digitally signed, and therefore can’t be patched at a later stage by a virus without triggering a signature failure alert.
If you receive an invalid signature alert, do you run the application as it means a software has modified the binary file.

Recent versions of Windows Defender wrongly reports some clean obfuscated .Net assemblies as a threat, this is a false positive.
Would you face that issue, we strongly recommend you try other anti-virus to get a confirmation before considering that detection as accurate.

Paths used by Celiveo Virtual Printer:
C:\Program Files\Celiveo\Celiveo Server Services*
C:\Program Files\Celiveo\Celiveo Virtual Printer*
C:\ProgramData\Celiveo\Celiveo Virtual Printer*

Last modified: 29 September 2022

8.4.2. Add a Celiveo Virtual Printer to Web Admin

What is a Celiveo Virtual Printer (CVP)?

Print-Direct Enterprise Business

The CVP is a module that is deployed on a user's workstation, so that they can print to and release print jobs on Celiveo enabled-printers. On the Web Admin, you add a Celiveo Virtual Printer (CVP), set it up for serverless pull printing or server based pull printing, and generate a deployment package. Later on, you use the deployment package to install the CVP on a Workstation.

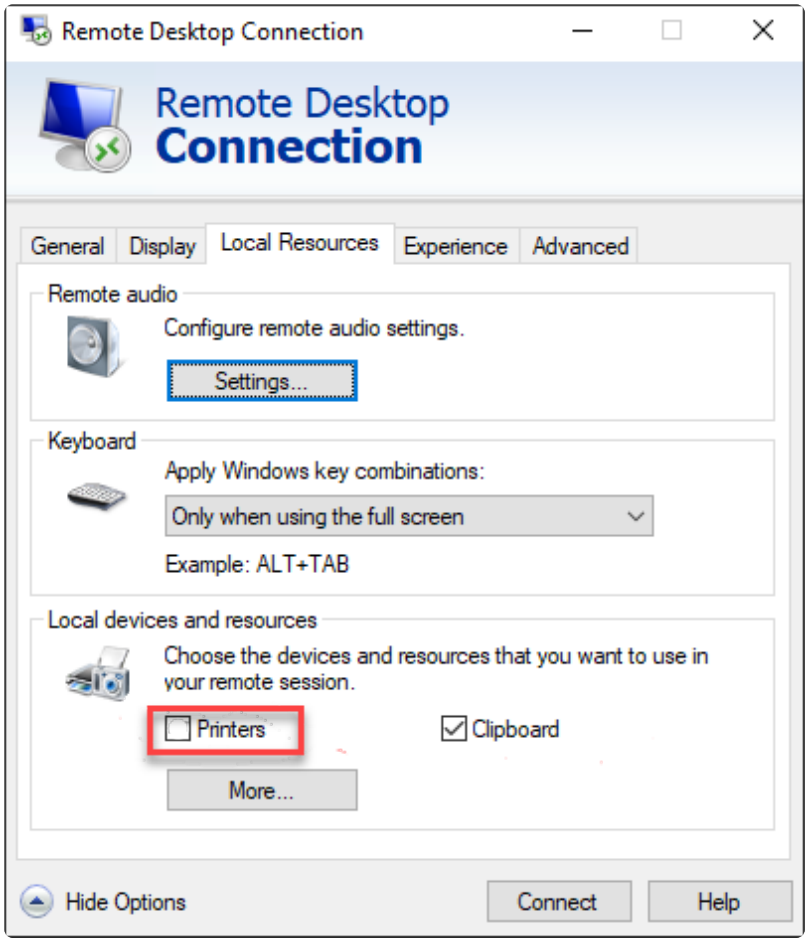
Before you begin…

Typically, a different printer driver is required for each printer. In order to make the most of pull printing, you need universal printer drivers that can support a fleet of printers. While adding the virtual printer, you may need to upload such a universal printer driver to the Celiveo Virtual Printer. The Add Printer wizard launches the Discovery Agent to enable you to import the driver from the workstation you are running the wizard on. So before you start, make sure that the workstation you are working on has the required printer drivers installed on it.

1. Start the Add Printer Wizard

1. At the Main menu, click .
2. At the Printer menu, click .
3. At the Add Printer menu, click . The Add Printer Wizard starts.

Important: If you are using a Remote Desktop Connection, in order for your Celiveo Virtual Printer to be the Default printer, make sure you uncheck the **Printers** option in the **Local Resources** tab of the Remote Desktop Connection settings.



2. Specify Virtual Printer Options

1. Specify a name for the CVP deployment package. After you add the Printer, you can download the deployment package and install it on a workstation.

> **Note**: Please use underscores instead of spaces in the name given to the virtual printer. Spaces cannot be used when printers are shared.

1. Click **[Next>]**. The next page displays.
2. Click **[Auto Update]** to enable automatic update of Virtual printer settings.

Auto Update

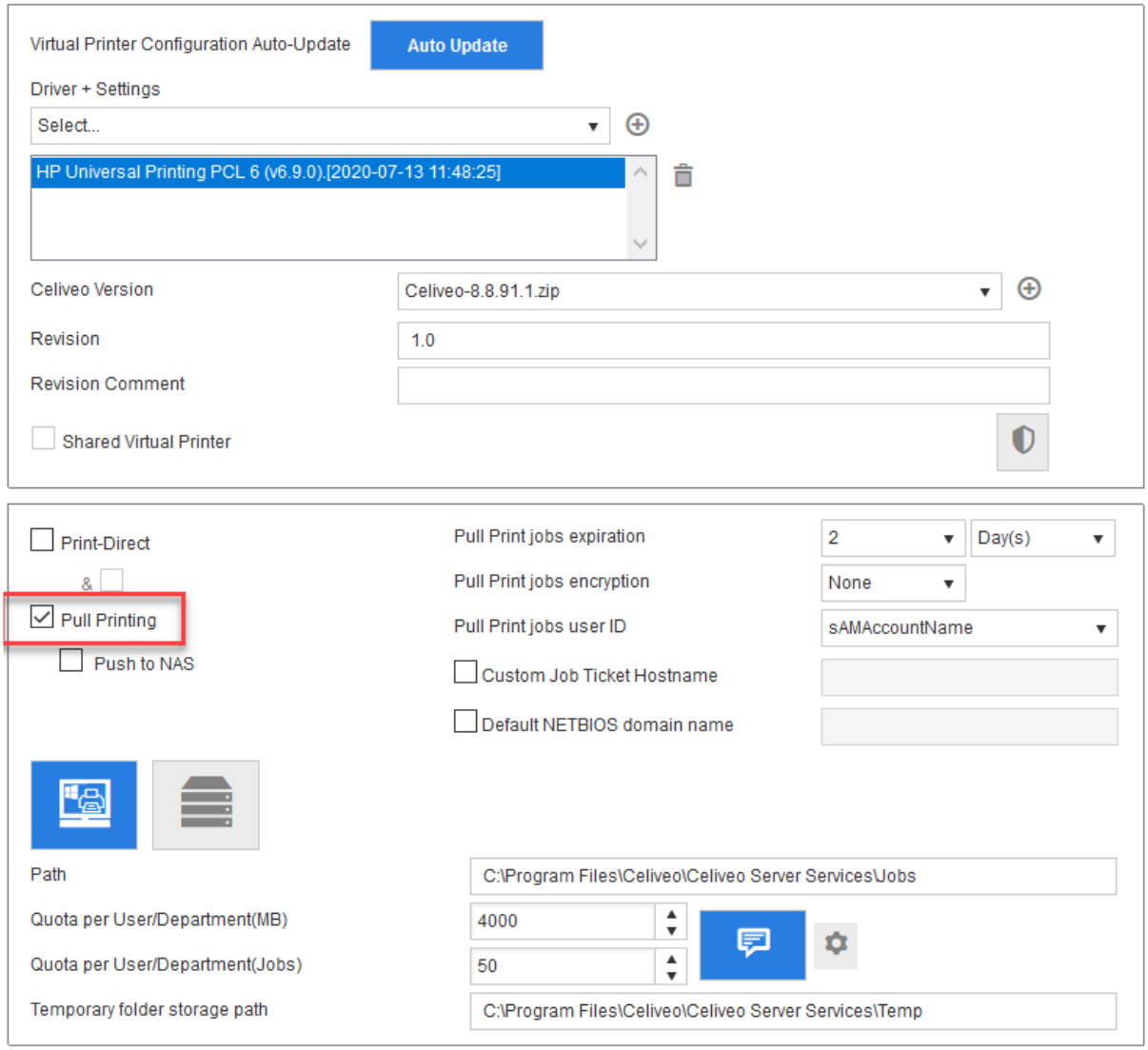
The table below describes which actions are performed when Auto Update is enabled and when it is not.

Nb	CVP Action	Auto-Update OFF	Auto-Update ON
1	If switch “-nodpq” is not in effect:		**X**
	Update the CSS settings		**X**
	Delete stall queues drivers and reinstall the current queues		**X**
2	Update Cost profile for each print queue		**X**

3	Get Groups and OU information of current user	X	X
4	If the database cannot be reached, try to update the primary connection string from Web Admin	X	X
5	If opening a connection to the primary database fails, monitor the connection and when it is available restart from step 3	X	X
6	Check the CVP configuration file and update it if needed	X	X
7	Get the tags and their names	X	X
8	Get the tags applying to this user (User tags, Groups tags, OU tags, IP tags)	X	X
9	Set CVP capabilities (Print-Direct, Pull Print or both)	X	X
10	Store CVP local settings	X	X
11	Store CSS settings to registry	X	X
12	Get the tags combination that will be used for the user based on priorities	X	X
13	Update primary and secondary DB connections strings for CVP and CSS if applicable	X	X
14	Get the tags available for the user	X	X
15	Load the local print drivers	X	X
16	If any queue needs to be installed and switch “-nodpq” is not in effect:		X
	Update the CSS settings		X
	Delete stall queues drivers and reinstall the current queues		X

Note: For a virtual printer (CVP), the update occurs for Print Queues, Cost Profile and Print Rules on Login event.

3. Select **[Pull Printing]** and clear **[Print-Direct]**.



4. **You can choose either the Local (HDD of user workstation) or Remote server to store the print jobs.**
5. Enter the default NETBIOS domain name.

2.1 To store print jobs on local drive:

1. Click icon to store print jobs on local (user workstation) hard disk.
2. **Path** – Enter the directory location in which the user jobs are to be stored, if you need to change the default storage location set.
3. **Quota per User/ Department (MB)** – indicates the quota for a user or department on the basis of print job size.
4. **Quota per User/ Department (Jobs)** – indicates the quota for a user or department on the basis of print job count.
5. The **Notifications** icon allows you to define the message to display when quotas are reached. To do so, click the **Configure** button.
6. **Temporary folder storage path** – Enter the directory location where the jobs are to be stored on a temporary basis.

Note: the maximum limit for **Quota per User/ Department (Jobs)** is 50.

> ! Please note that notifications need to be manually enabled so that users can see quota notifications.

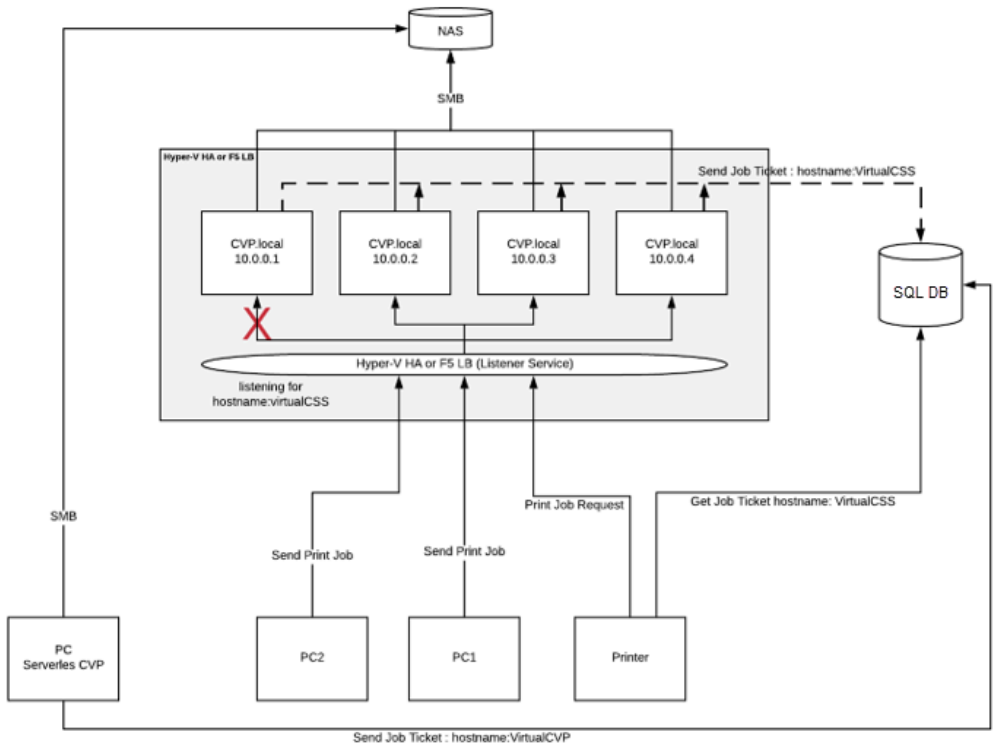
> ! **Warning**: if one of these quotas is reached, print jobs will be lost without any further notification.

2.2 To store print jobs on a network drive:

1. Click icon to store on remote server.
2. At **[Domain]**, enter the domain name of the network drive to store the print jobs.
3. At **[User name]** and **[Password]**, enter the login credentials to the network drive to store the print jobs.
4. At **[Retry Count]**, enter the number of attempts to reach the network drive to store the jobs.
5. At **[Retry timer]**, enter the time interval (seconds) between each attempt to reach the network drive.
6. **Path** -Enter the directory location in which the user jobs are to be stored. Ensure that the user has read/write access permissions on the shared network folder.

Custom Job Ticket Hostname

Custom Job Ticket Hostname allows the CVP to replace its own IP/Hostname with a custom CVP IP/Hostname to all the spooled jobs. This information is then stored on the SJPS DB Job Ticket. This configuration is useful when using Clusters/Load Balancers with Virtual IP/Hostname.



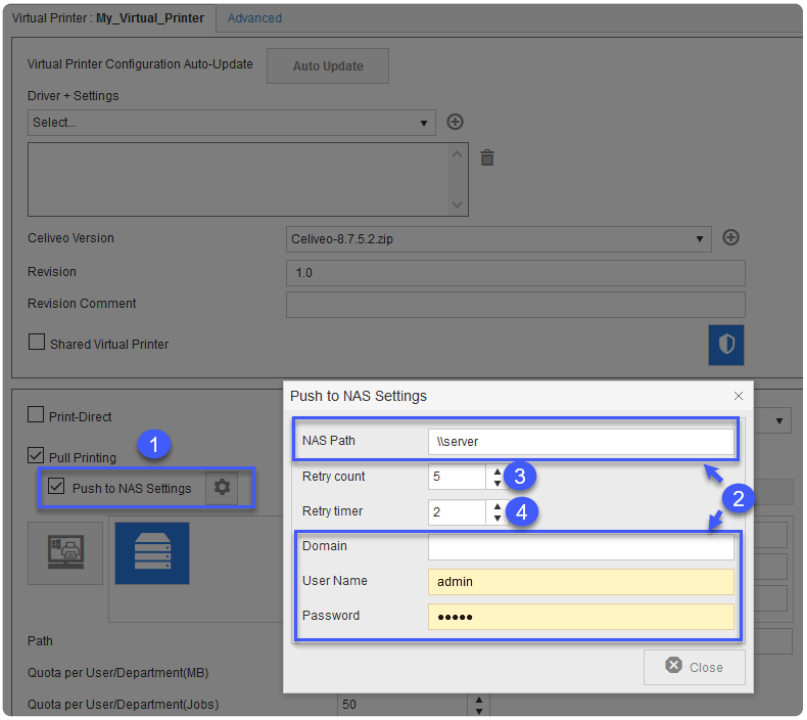
To enable Custom Job Ticket Hostname:

1. Tick the Custom Job Ticket Hostname.
2. Enter the Hostname in the corresponding field.

2.3 To store print jobs on Network Attached Storage (NAS) unit:

You can configure the print jobs to be transferred to a NAS unit connected in the same domain network. The Celiveo Virtual Printer pushes the print files to NAS unit when user initiates Shutdown of his/her PC. The Celiveo Virtual Printer can push the print files to a temporary storage (NAS unit) which is connected in the same domain network.

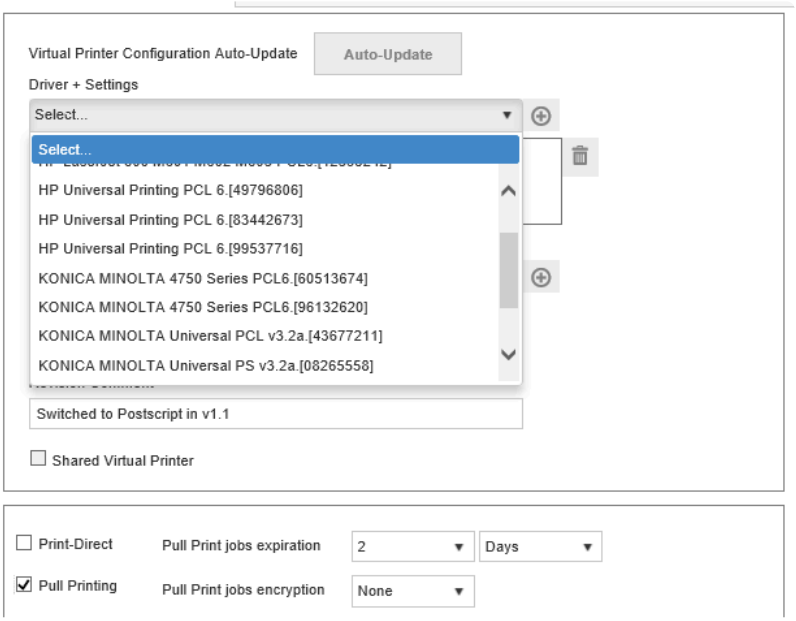
CVP (Client station mode) Configuration



1. Select the **[Push to NAS Settings]** option and click the ⚙ button.
2. Enter **[User name]**, **[Password]**, **[Domain]** and **[NAS Path]**.
3. At **[Retry count]**, enter the number of attempts to reach the NAS to store the jobs.
4. At **[Retry timer]**, enter the time interval (seconds) between each attempt to reach the NAS.

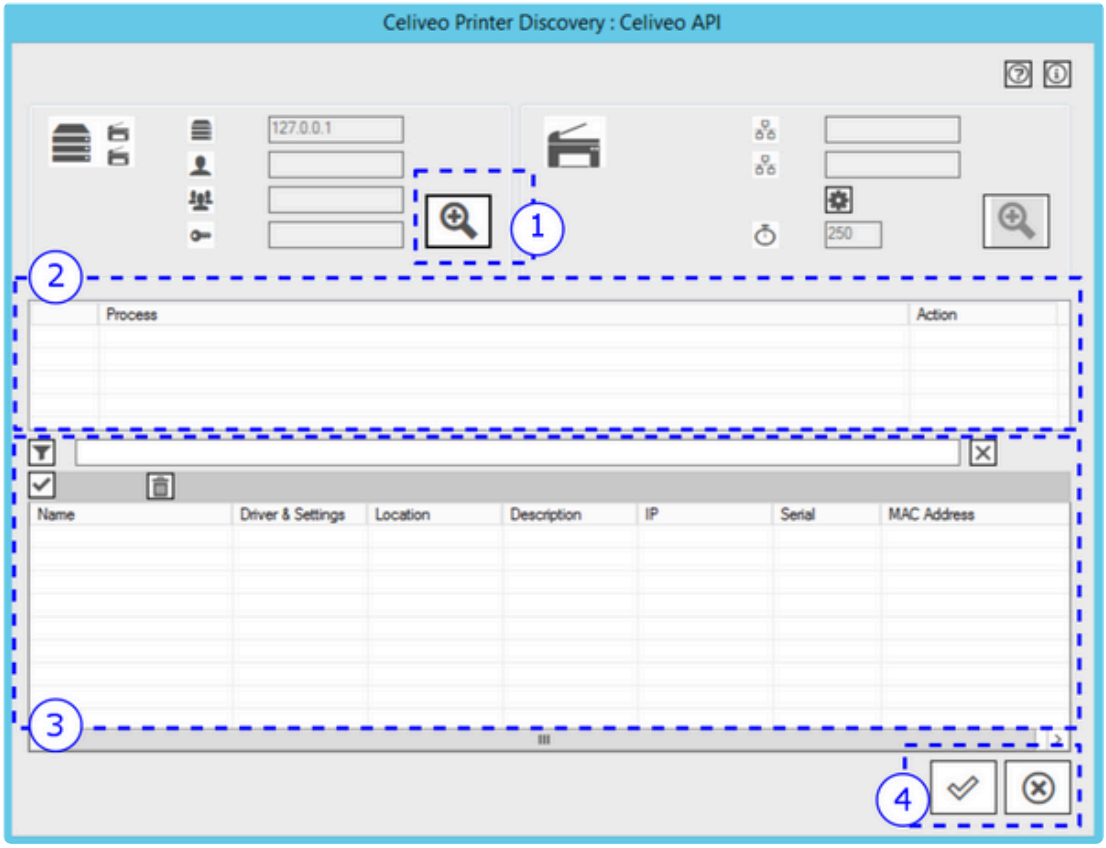
NOTE: When the NAS is not reachable upon Shutdown of the client PC, the print jobs are retained on client machine's default jobs location.

3. Import Printer Driver



From the **[Driver + Settings]** drop-down, select the printer driver to use for pull printing.
If the driver you want to use is not available on the list:

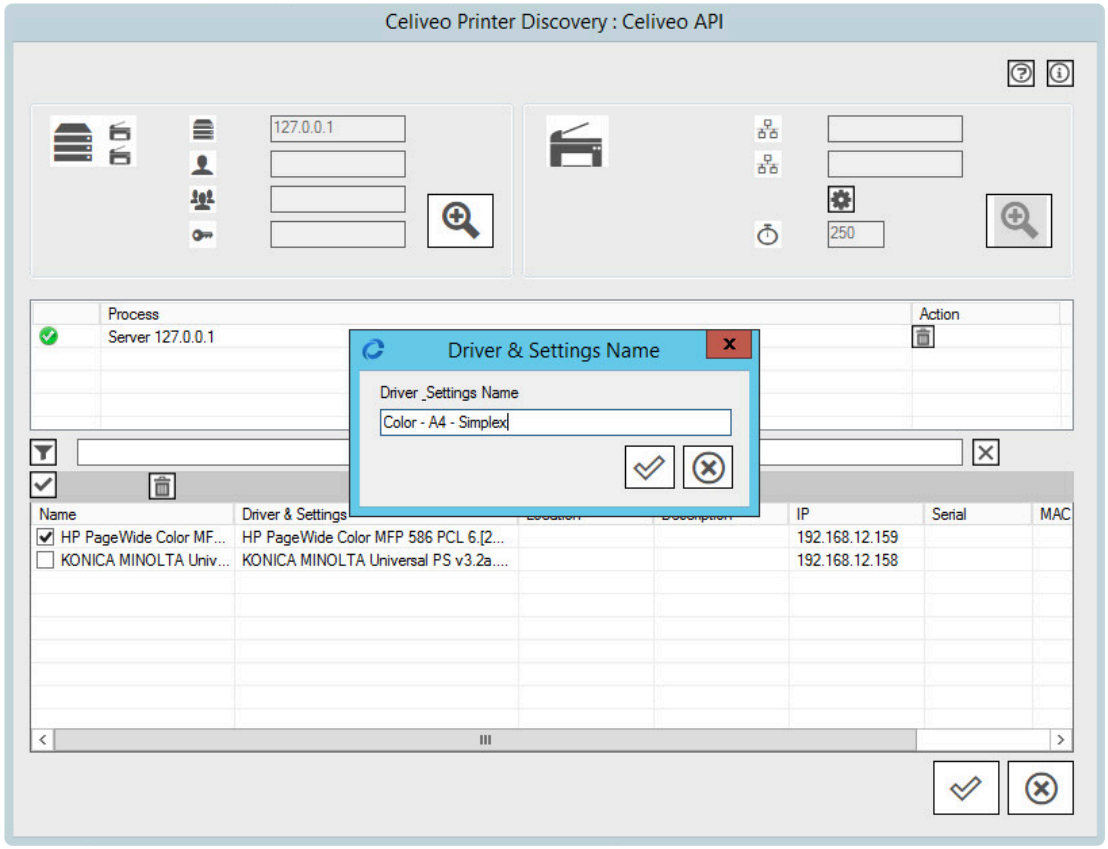
1. Click ⊕, next to the **[Driver + Settings]** drop-down. The Discovery Agent displays.



2. In the area marked 1, click on the Search icon (🔍).
   The Discovery Agent searches the workstation the Web Admin is running on for printer drivers.
   The printer drivers installed on the workstation are displayed in the area marked 3 in the illustration above.

Note: The Discovery Agent is unable to import class drivers.

3. Select the driver to import.
   When you import the driver, the default printing preferences are also imported with the driver. With Celiveo Enterprise, you can assign up to five drivers per printer. This translates into five print queues for the user. By renaming the driver+settings meaningfully, users can perceive each print queue as a preset for the same printer.
   To rename the driver+settings to something more meaningful:
   a. Double-click the row containing the driver.



   b. At [Driver+Settings Name], specify the new name.

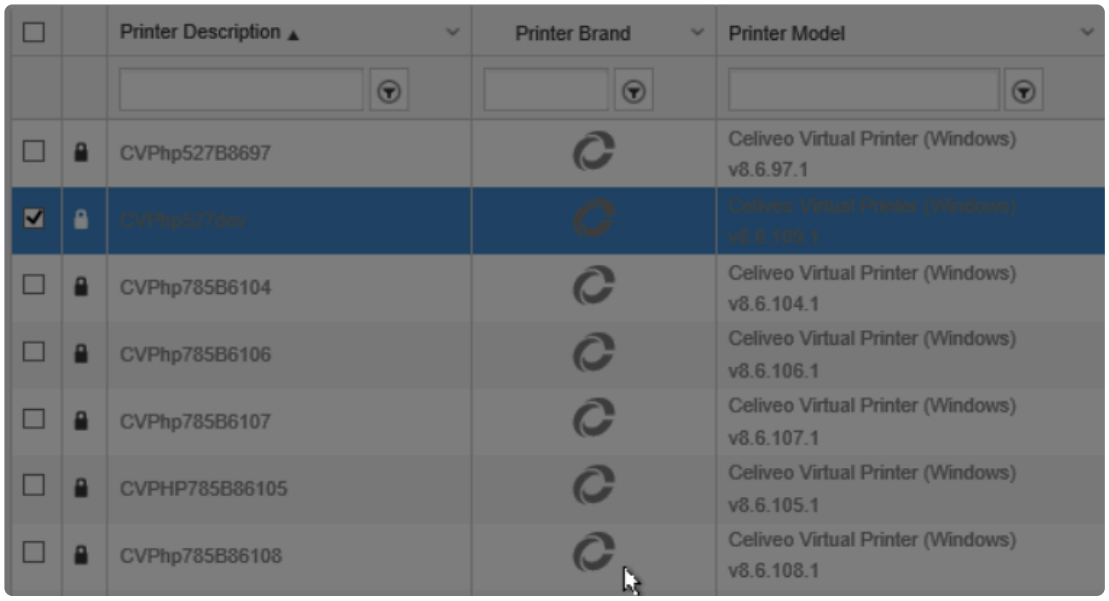
4. Click ✓ until all dialogs close.
5. From the **[Driver + Settings]** drop-down, select the printer driver you just added.
   You are returned to the Add Printer wizard.

2. Click **[Next]**.

4. Finalize

1. Accept the defaults for the next few steps and click **[Next>]** until the Save Confirmation dialog displays.
2. Ensure that the option for downloading the deployment package is selected, and click **[Save]**.
   Preserve the downloaded file so that you can expand it and deploy it on a target workstation.

Note: CVPs created by Admins can be unavailable for edition to other users. However, they can still be selected to be downloaded.



Last modified: 29 September 2022

8.4.3. Add a Celiveo Shared Virtual Printer to Web Admin

What is a Celiveo Shared Virtual Printer (CSVP)?

The CSVP is a module that is deployed and shared on a Print Server so that users can print to and release print jobs on Celiveo enabled-printers. On the Web Admin, you add a Celiveo Virtual Printer (CVP), set it up as a CSVP, and generate a deployment package. Later on, you use the deployment package to install the CSVP on a Print Server.

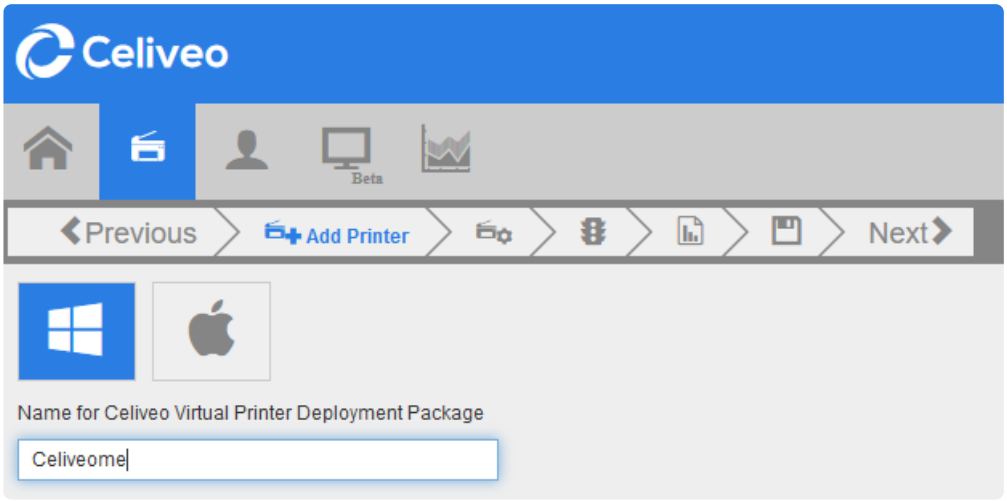
***Tip**: It is recommended to follow the Microsoft's Print Server Scalability and Capacity planning guide to dimension appropriately the Windows Print Server hosting the Celiveo Shared Virtual Printer (CSVP). The CSVP provides the Server-based Pull Print service and is equivalent to 50 physical printers in terms of resources. The actual number of physical printers in your setup that benefit from the pull print service is irrelevant when defining the Print server specifications.*

Before you begin…

Typically, a different printer driver is required for each printer. In order to make the most of pull printing, you need universal printer drivers that can support a fleet of printers. While adding the virtual printer, you may need to upload such a universal printer driver to the Celiveo Virtual Printer. The Add Printer wizard launches the Discovery Agent to enable you to import the driver from the workstation you are running the wizard on. So before you start, make sure that the workstation you are working on has the required printer drivers installed on it.

1. Start the Add Printer Wizard

1. At the Main menu, click .
2. At the Printer menu, click . The Add Printer Wizard starts.

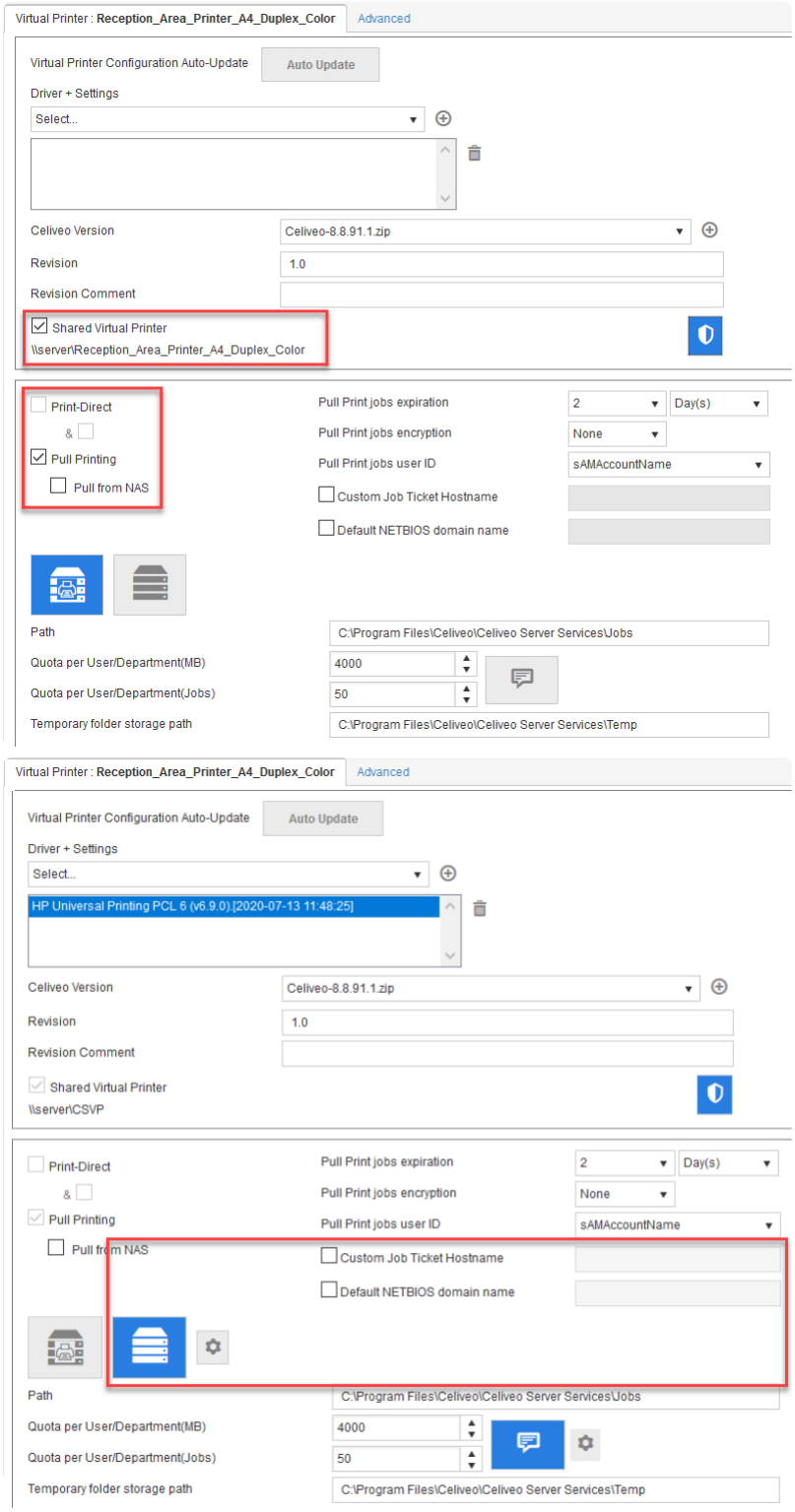


2. Specify Virtual Printer Options

1. Specify a name for the CSVP deployment package. After you add the Printer, you can download the deployment package and install it on a Print Server.

> **Note**: Make sure you use underscores instead of spaces in the name given to the virtual printer.

2. Click **[Next>]**. The next page displays.



3. Select **[Shared Virtual Printer]**.
4. Verify that **[Pull Printing]** is selected. **[Print-Direct]** is disabled when you select **[Shared Virtual Printer]** option. Additional options are enabled for configuration, when you select **[Pull Printing]** option.

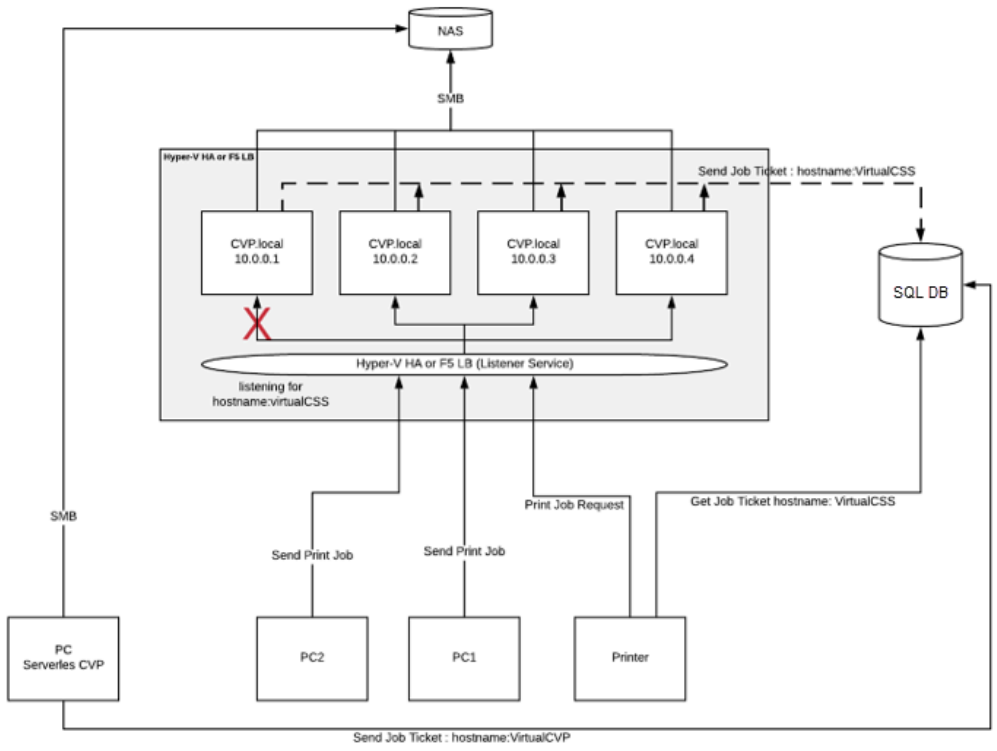
2.1 Options

- **Stealth Mode** – Enabling this option for the virtual printer encrypts the user data (user login name and print job information) on both shared and non-shared print queues. The document name will be replaced with asterisks symbols prefixed and suffixed respectively with first and last character of the original document name, in the Tracking Reports.

> **NOTE**: Stealth mode feature is available only on Optional connectors with active license.

- **Custom Job Ticket Hostname**

Custom Job Ticket Hostname allows the CVP to replace its own IP/Hostname with a custom CVP IP/ Hostname to all the spooled jobs. This information is then stored on the SJPS DB Job Ticket. This configuration is useful when using Clusters/Load Balancers with Virtual IP/Hostname.



To enable Custom Job Ticket Hostname:

1. In the Domain, User Name and Password fields, enter the information of the service account that has access to the remote storage/share.
2. In the Path and Temp fields, enter the share location: eg \\servername\sharename.

NOTE: This feature is available only for Pull Printing. The custom server should also have a CVP/CSVP installed.

- **Pull Print jobs expiration** – indicates the number of days/ hours after which the print jobs shall expire.
- **Pull Print jobs encryption** – indicates the encryption to be used on print jobs.

You can choose either the *Local* (HDD of the Print-Server where CSVP is installed) or *Remote* server to store the print jobs.

2.2 To store print jobs on local server

1. Click icon icon to store print jobs on hard disk.
2. **Path** – Enter the directory location in which the user jobs are to be stored. For custom server (Custom Job Ticket Hostname), enter the directory location to the custom server.
3. **Quota per User/ Department (MB)** – indicates the quota for a user or department on the basis of print job size.
4. **Quota per User/ Department (Jobs)** – indicates the quota for a user or department on the basis of print job count.
5. **Temporary folder storage path** – Enter the directory location where the jobs are to be stored on a temporary basis.

Note: The maximum limit for **Quota per User/ Department (Jobs)** is 150.

2.3 To store print jobs on a network drive:

1. Click to store on remote server.
2. At **[Domain]**, enter the domain name of the network drive to store the print jobs.
3. At **[User name]** and **[Password]**, enter the login credentials to the network drive to store the print jobs.
4. At **[Retry Count]**, enter the number of attempts to reach the network drive to store the jobs.
5. At **[Retry timer]**, enter the time interval (Seconds) between each attempt to reach the network drive.
6. Enter the directory location in which the user jobs are to be stored. Ensure that the user has read/ write access permissions on the shared network folder.
7. Define the quota to be set for the user/ department.
8. Enter the directory location where the jobs are to be stored on a temporary basis.

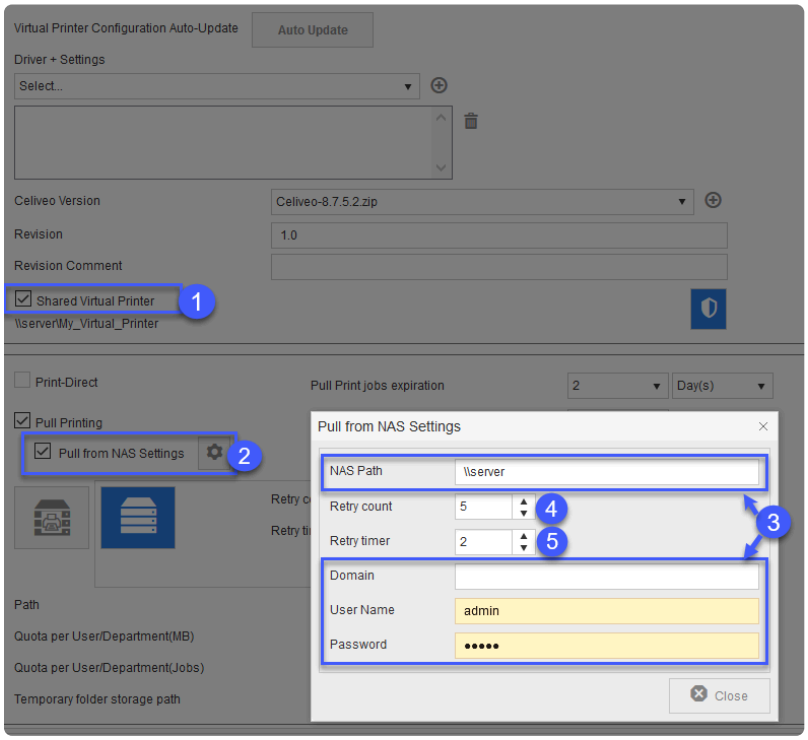
Note: If the **Custom Job Ticket Hostname** option is selected, the Domain, Path and login credentials should be configured for the custom server.

2.4 To store print jobs on Network Attached Storage (NAS) unit:

You can configure the print jobs to be transferred to a NAS unit connected in the same domain network.

The Celiveo Virtual Printer pushes the print files to NAS unit when user initiates Shutdown of his/her PC.

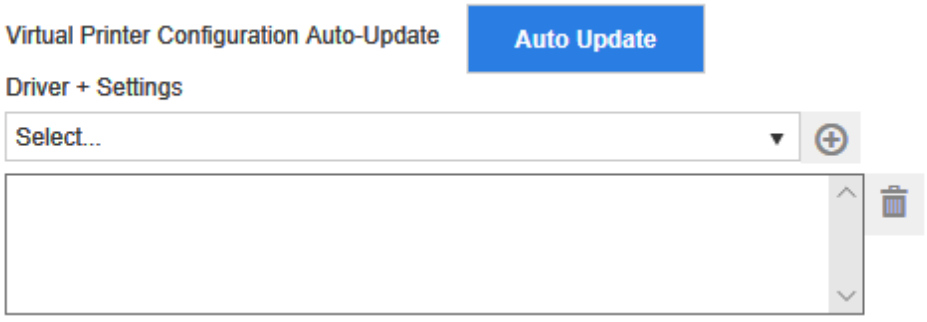
CSVP (Server mode) Configuration



1. Select the **[Shared Virtual Printer]** option.
2. Select the **[Pull from NAS Settings]** option and click the ⚙ button.
3. Enter **[User name]**, **[Password]**, **[Domain]** and **[NAS Path]**.
4. At **[Retry count]**, enter the number of attempts to reach the NAS to store the jobs.
5. At **[Retry timer]**, enter the time interval (Seconds) between each attempt to reach the NAS.

NOTE: When the NAS is not reachable upon Shutdown of the client PC, the print jobs are retained on client machine's default jobs location. Learn more about pushing print jobs to NAS.

3. Import Printer Driver



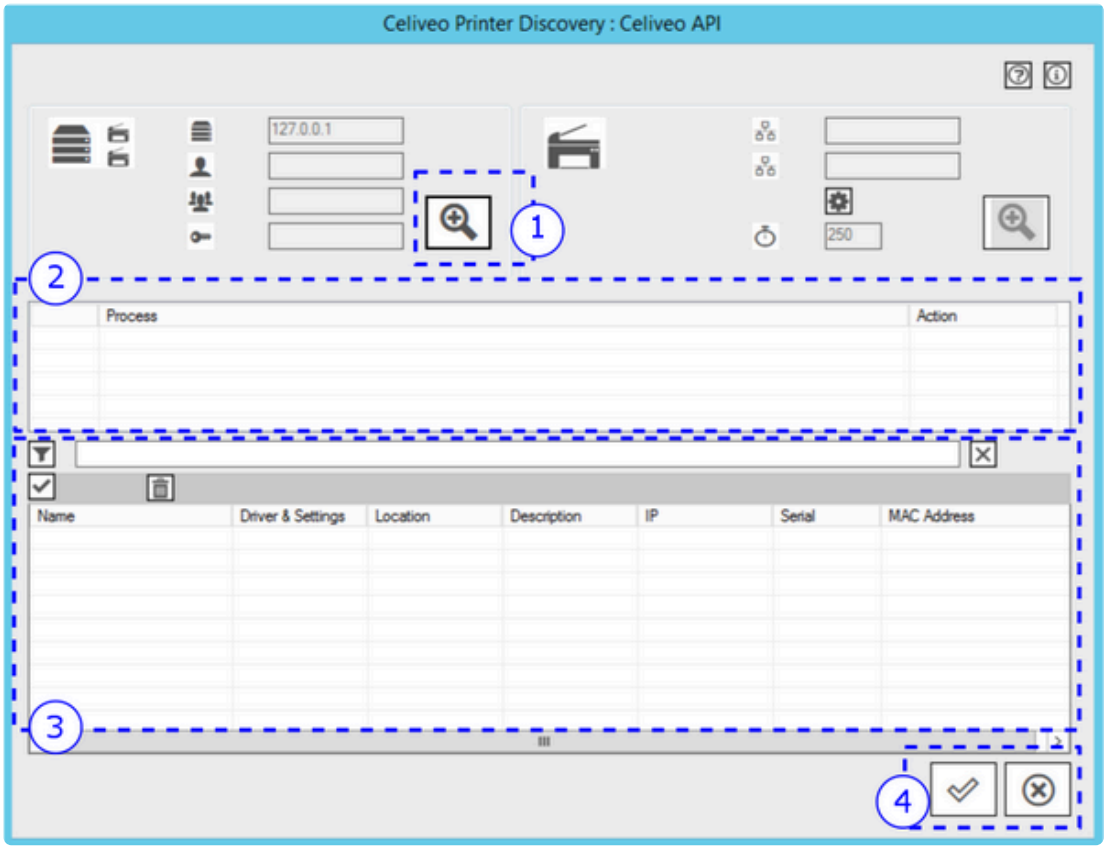
1. Click **[Auto Update]** to enable automatic update of Virtual printer settings. This will synchronize the Driver, Cost Definition Profile, and Access and Rules Profile settings for the virtual printer. For example, if a printer driver was already installed in the workstation by Celiveo Virtual Printer,

then the **[Auto-update]** option updates the driver settings configuration (if it had been modified); rather than downloading and installing the driver again.

> **Note**:
> For a virtual printer (CVP), the update occurs for Print Queues, Cost Profile and Print Rules on Login event.
> For shared virtual printer (CSVP), the update is scheduled to occur every night at 01:00 AM.

2. From the **[Driver + Settings]** drop-down, select the printer driver to use for pull printing.
   If the driver you want to use is not available on the list:

1. Click ⊕, next to the **[Driver + Settings]** drop-down. The Discovery Agent displays.



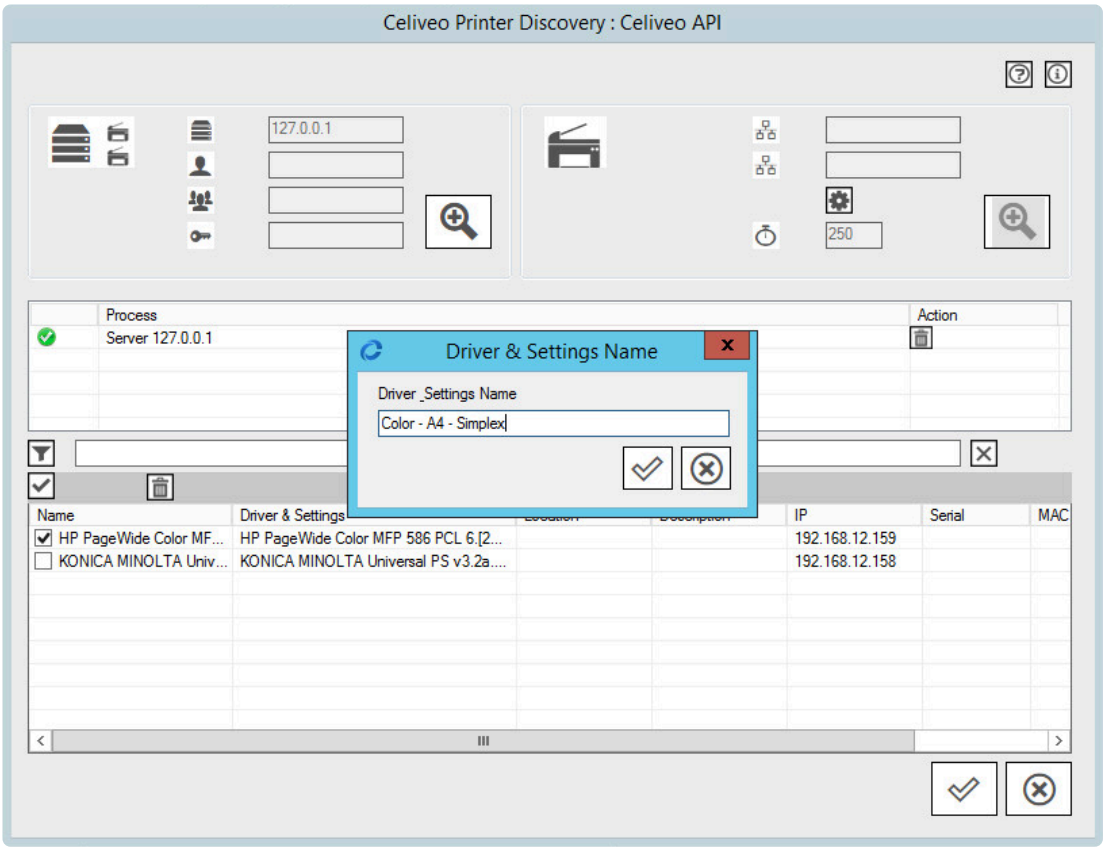
2. In the area marked 1, click on the Search icon (🔍).
   The Discovery Agent searches the workstation the Web Admin is running on for printer drivers. The printer drivers installed on the workstation are displayed in the area marked 3 in the illustration above.

> **Note**: The Discovery Agent is unable to import class drivers.

3. Select the driver to import.
   When you import the driver, the default printing preferences are also imported with the driver. With Celiveo Enterprise, you can assign up to five drivers per printer. Thereby, you can have five different sets of printing preferences for the same driver, which translate into five print queues for the user. By renaming the driver+settings meaningfully, users can perceive each print queue as a

preset for the same printer.
To rename the driver+settings to something more meaningful:

a. Double-click the row containing the driver.



b. At **[Driver+Settings Name]**, specify the new name.

4. Click ✔✔ until all dialogs close.
5. From the **[Driver + Settings]** drop-down, select the printer driver you just added.
   You are returned to the Add Printer wizard.

3. Click **[Next]**.

IMPORTANT: Rules for a Celiveo Shared Virtual Printer must not have **USER OU** as a criteria.

4. Finalize

1. Accept the defaults for the next few steps and click **[Next>]** until the Save Confirmation dialog displays.
2. Ensure that the option for downloading the deployment package is selected, and click **[Save]**.
   Preserve the downloaded file so that you can expand it and deploy it on a Print Server.

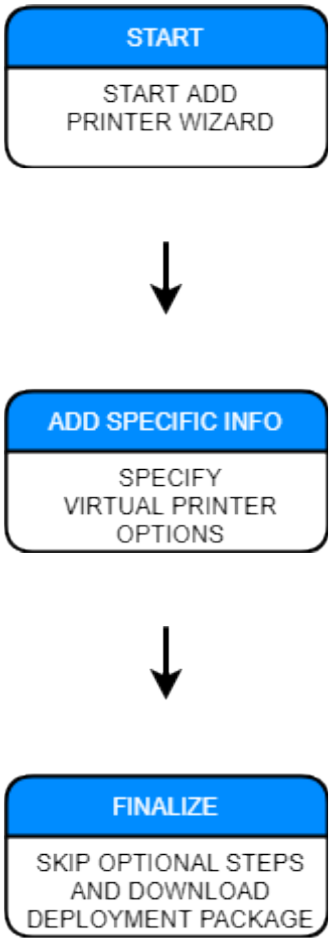
Last modified: 29 September 2022

8.4.4. Add a Celiveo Virtual Printer for Print-Direct

What is a Celiveo Virtual Printer (CVP)?

The CVP is a module that is deployed on a user's workstation, which enables a user to print directly to a printer, subject to rules based printing and usage reporting. On the Web Admin, you add a Celiveo Virtual Printer (CVP), and generate a deployment package. Later on, you install deployment package on the user's workstation.

Workflow



Start the Add Printer Wizard

1. At the Main menu, click .
2. At the Printer menu, click .
3. At the Add Printer menu, click . The Add Printer Wizard starts.

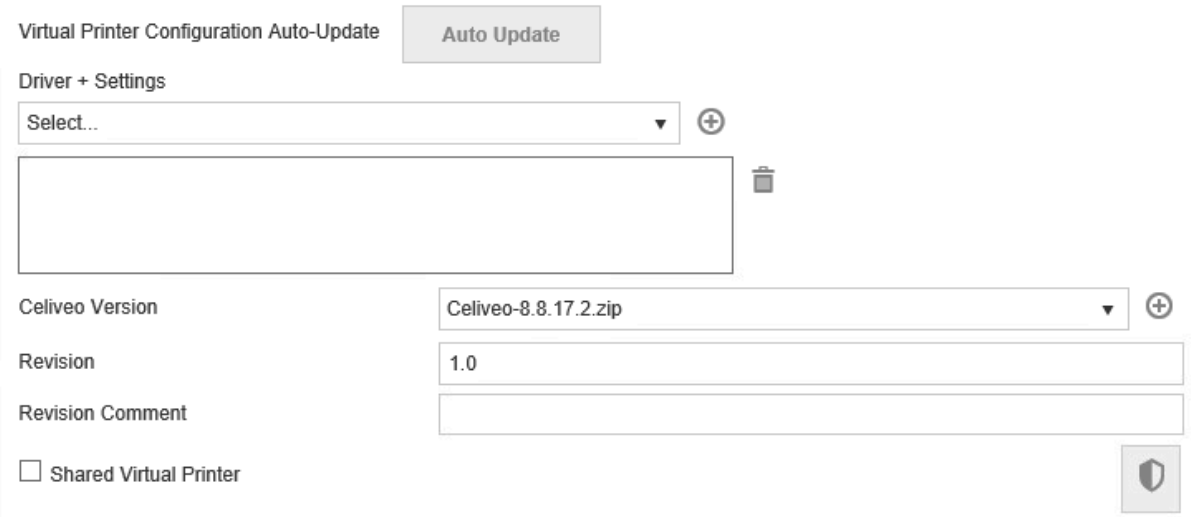
Specify Virtual Printer Options

1. Specify a name for the CVP deployment package.

During the final stage, the Add Printer wizard generates and downloads a deployment package using the name you provide. Subsequently, you can install the deployment package on a user's workstation.

Note: Please use underscores instead of spaces in the name given to the virtual printer. Spaces cannot be used when printers are shared.

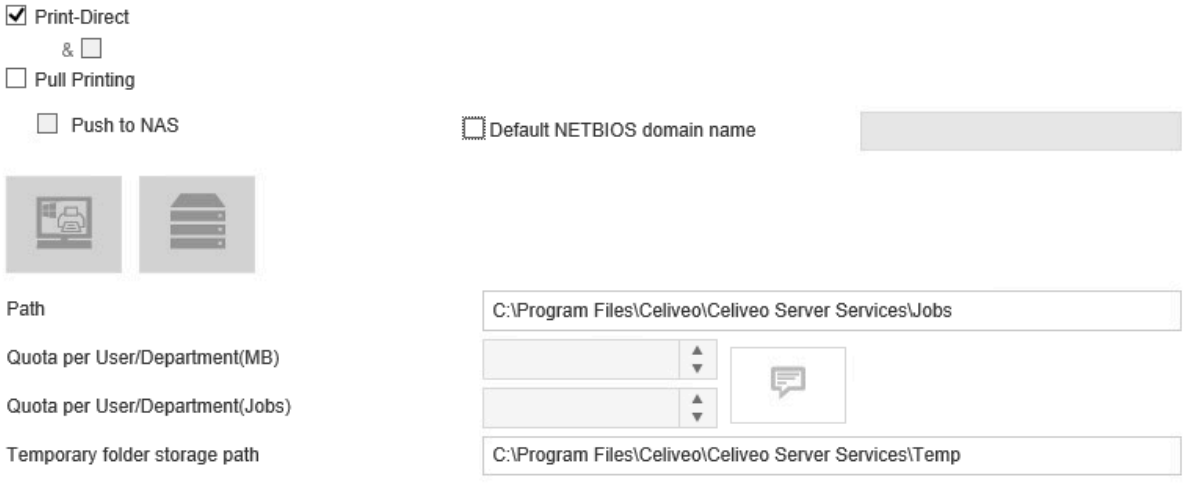
2. Click **[Next>]**. The next page displays.



3. Click **[Auto Update]** to enable automatic update of Virtual printer settings. This will synchronize the Driver, Cost Definition Profile, and Access and Rules Profile settings for the virtual printer. For example, if a printer driver was already installed in the workstation by Celiveo Virtual Printer, then the **[Auto-update]** option updates the driver settings configuration (if it had been modified); rather than downloading and installing the driver again.

For a virtual printer (CVP), the update occurs for Print Queues, Cost Profile and Print Rules on Login event.

4. Choose the Celiveo Version. The latest version will be the listed first by default.
5. Select **[Print-Direct]** and clear **[Pull Printing]**.



6. Click **[Next>]**

Finalize

1. Accept the defaults for the next few steps and click **[Next>]** until the Save Confirmation dialog displays.
2. Ensure that the option for downloading the deployment package is selected, and click [Save]. Preserve the downloaded file so that you can expand it and deploy it on a Print Server.
3. **Please Logout/Login or reboot the machine to complete the installation.**

Tip: You can download the deployment package later, by selecting the CVP in Web Admin, and clicking .

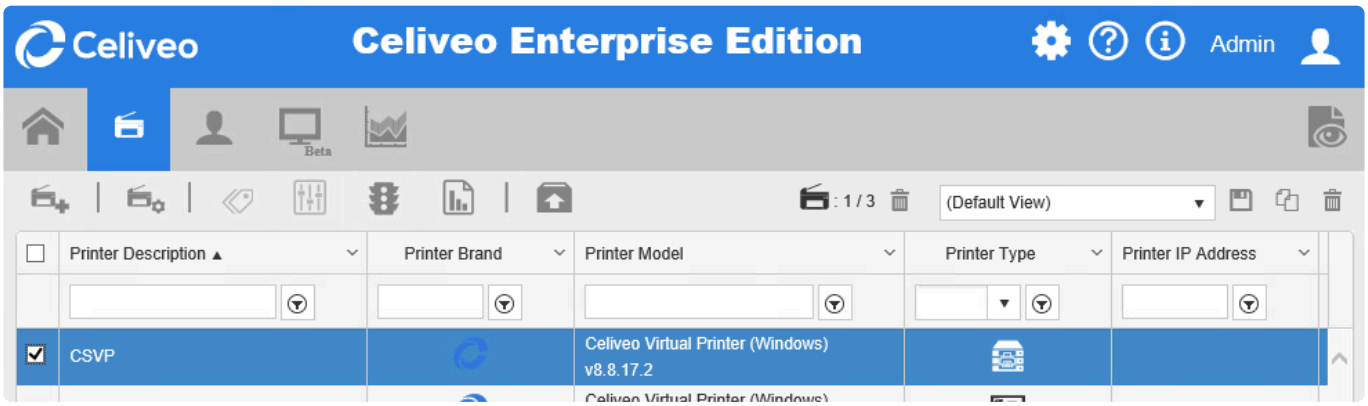
Last modified: 29 September 2022

8.4.5. Deploy a Celiveo Shared Virtual Printer Package on a Print Server

Follow the steps listed below to deploy a Celiveo Shared Virtual Printer (CSVP) on a Print Server:

1. Download the Deployment Package
2. Install the CSVP on Print Server
3. Verify CSVP on Print Server
4. Connect to a CSVP from a User's Workstation

1. Download the Deployment Package

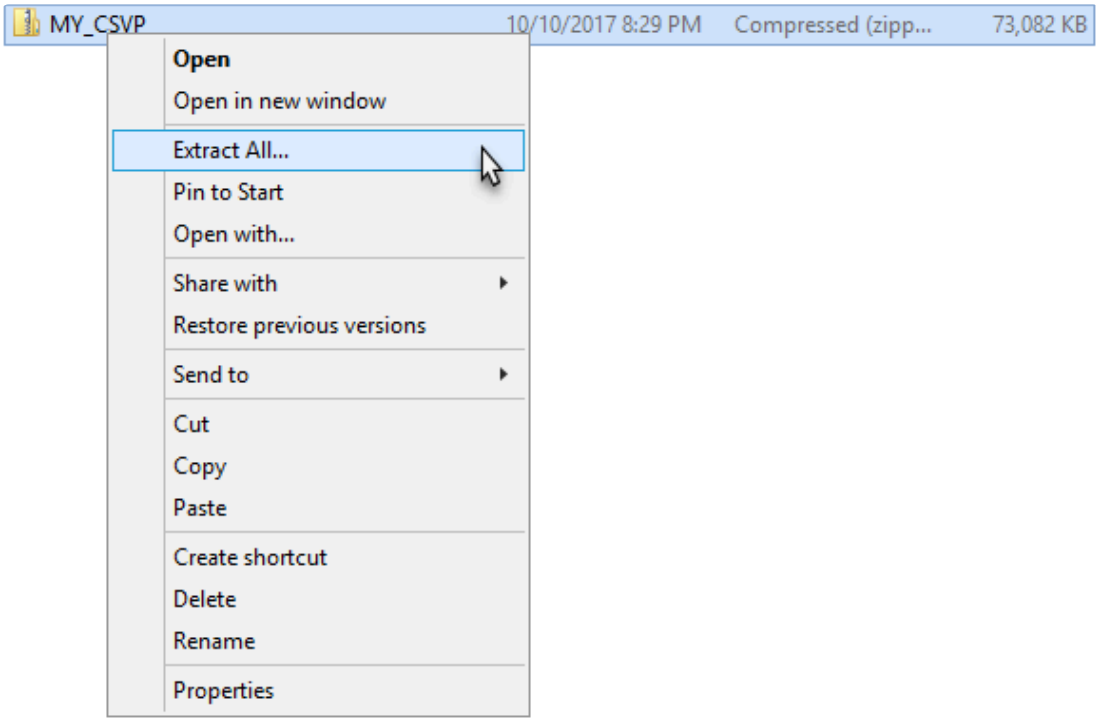


1. In the Web Admin, select the CSVP.
2. Click .
   The Shared Virtual Printer Deployment Package downloads.

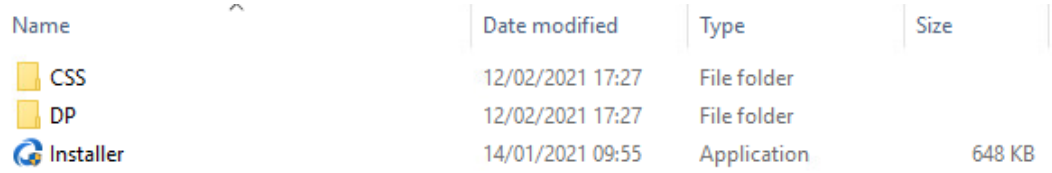
Note: For Non-Super admins, multiple selections of CVPs are only allowed for download, edit and delete are disabled.

2. Install the CSVP on Print Server

1. Log in to the server as its administrator.
2. Copy the Virtual Printer Deployment Package to a temporary folder on the print server.
3. Right-click the Deployment Package. A menu displays.



4. Click **[Extract All]**.
5. Select a temporary folder to extract the files to, and click **[Extract]**.



}!

6. Double-click **[Installer]** and start the installation. Upon installation, a Celiveo Virtual Printer icon ( ) is placed on the Desktop and the System Tray.

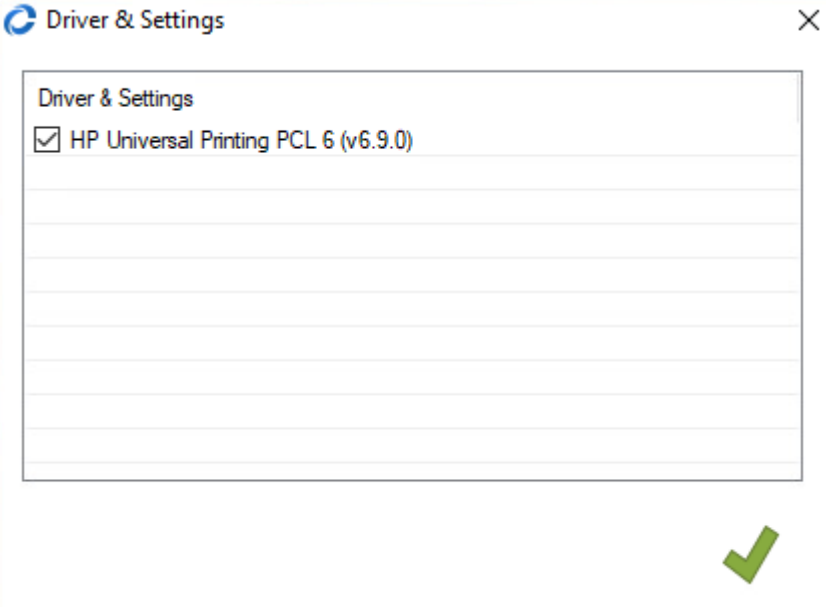
The table below lists the possible codes returned by the installer:

Code	Message
0	Success
1001	Invalid argument for custom installation directory
1002	Custom installation directory could not be created
1003	Administrator rights are required
1004	.NET Framework 3.5 is not installed
1005	Unable to uninstall Celiveo Server Services via UninstallUtility while trying to upgrade to a new version
1006	Unable to uninstall Celiveo Virtual Printer
1007	Unable to uninstall Celiveo Server Services
1008	Unable to uninstall Celiveo Virtual Printer while trying to upgrade to a new version
1009	Unable to install Celiveo Virtual Printer MSI

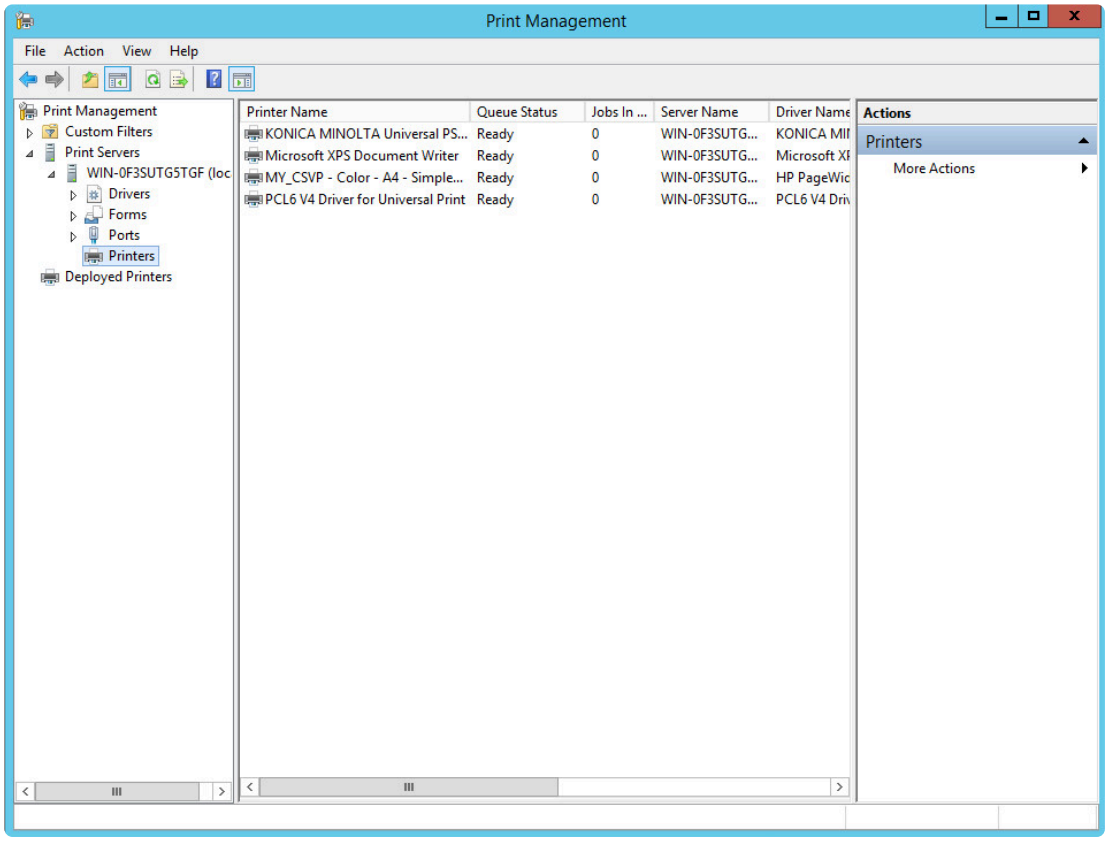
1010	Unable to install Celiveo Server Services MSI
1011	Unexpected error, see installation logs for details
1012	Invalid argument for the custom CSS port
1013	Invalid argument for the custom CSS port, port specified is out of range
1014	Unable to uninstall Celiveo Mobile Extension Agent
1015	Unable to install Celiveo Mobile Extension Agent MSI
1016	Invalid argument for the Celiveo Mobile Extension Agent certificates password
1017	Celiveo Mobile Extension Agent requires its certificates to be installed
1018	Invalid argument for the Celiveo Mobile Extension Agent custom print queue name
1019	Unable to install Celiveo Mobile Extension Agent certificates, see installation logs for details
1020	Unable to configure Celiveo Mobile Extension Agent, see installation logs for details

3. Verify CSVP on Print Server

1. Right-click on the system tray. A menu displays.
2. Click **[Celiveo Pull Printing]**. The Driver and Settings screen displays.



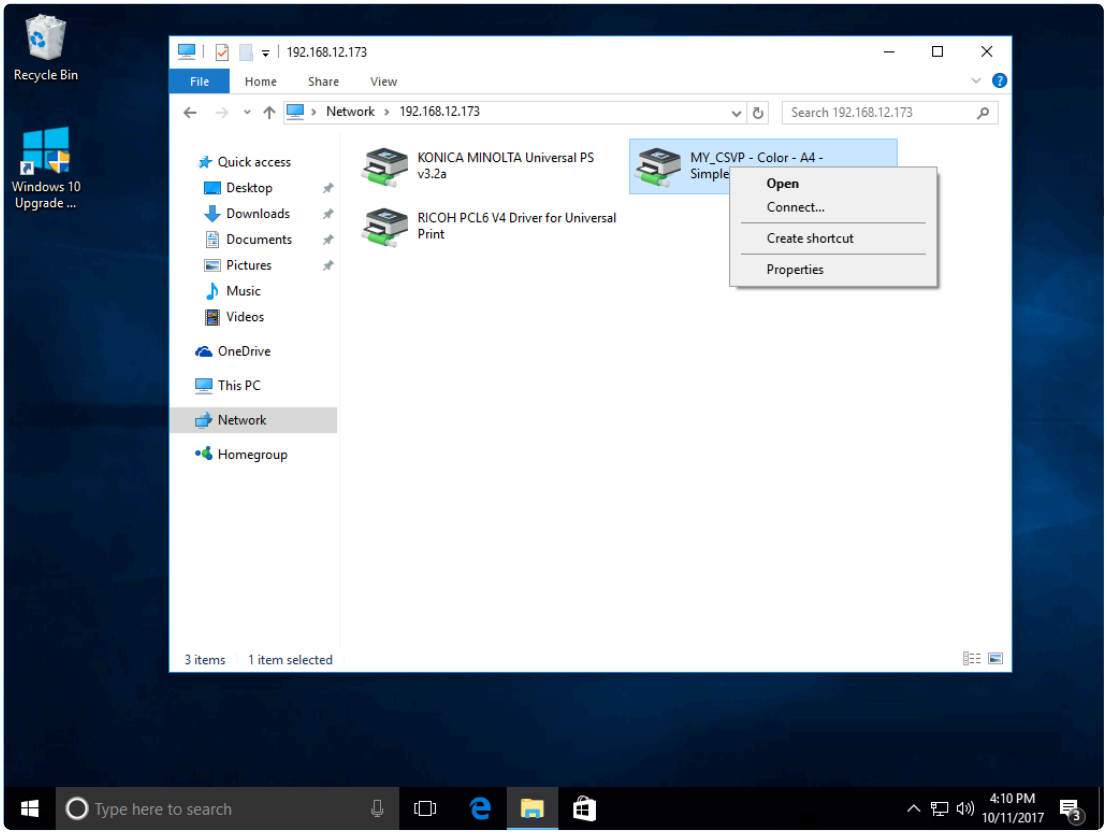
3. Select the printers to use and click .
   A vertical yellow bar starts running on the Celiveo Virtual Printer system tray icon while the printer drivers are installed.
4. Verify that the Celiveo Shared Virtual Printer is added to the Print Server
   a. In Server Manager, click **Tools > Print Management**. The Print Management console displays.
   b. In the left pane, click **Print Management > Print Servers > *Your_Server_Name* > Printers**.



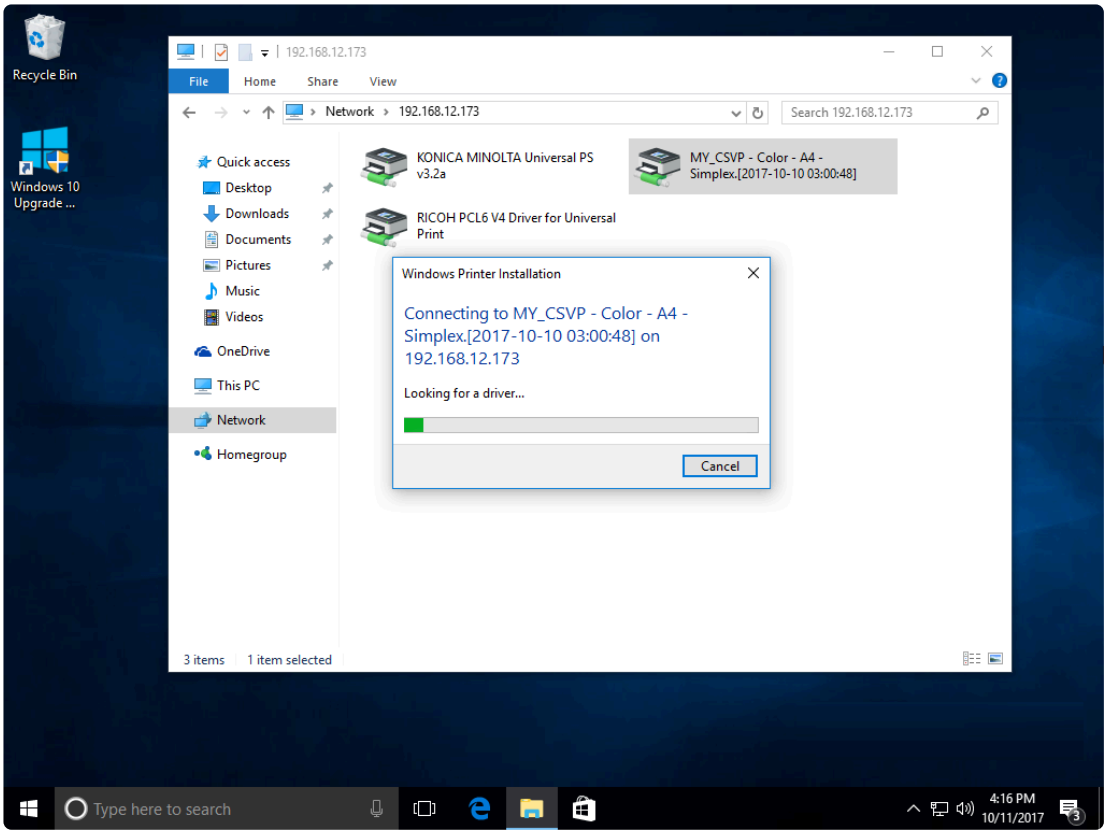
c. Verify that the Celiveo Shared Virtual Printer is listed.

4. Connect to a CSVP from a User's Workstation

1. From the Workstation, use Windows Explorer to Navigate to the print server.



2. Right-click the Celiveo Shared Virtual Printer and select **[Connect]**. The printer installation starts.



3. In Devices and Printers, verify that the Celiveo Shared Virtual Printer was installed.

Last modified: 10 October 2022

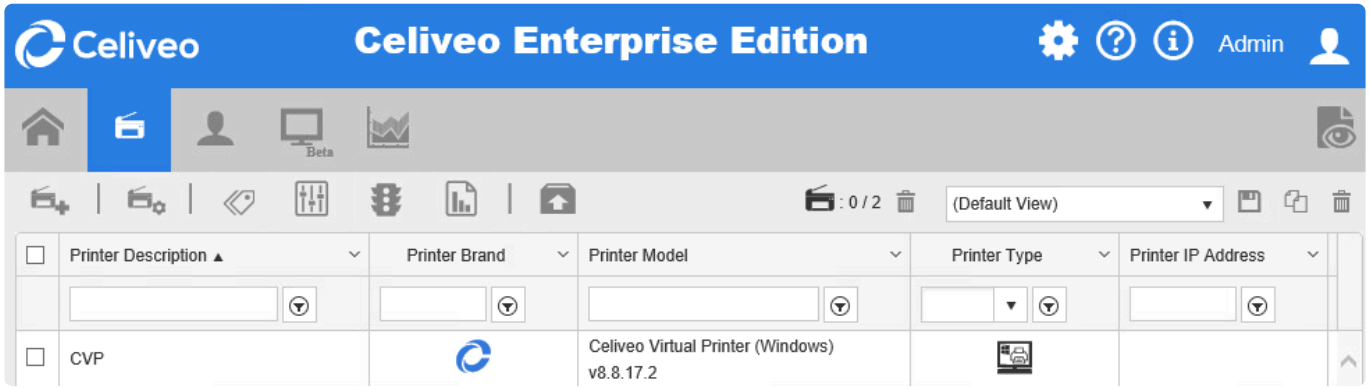
8.4.6. Deploy a Celiveo Virtual Printer on a User's Work Station (For Pull Printing)

Follow the steps below to deploy a Celiveo Virtual Printer on a user's workstation:

Print-Direct Enterprise Business

1. Download the Virtual Printer deployment package.
2. Install the Virtual Printer on a user's workstation.
   - Silent installation
   - Uninstallation
3. Install Printer Queues for pull printing.
4. Multi-SQL Configuration.

1. Download Virtual Printer Deployment Package



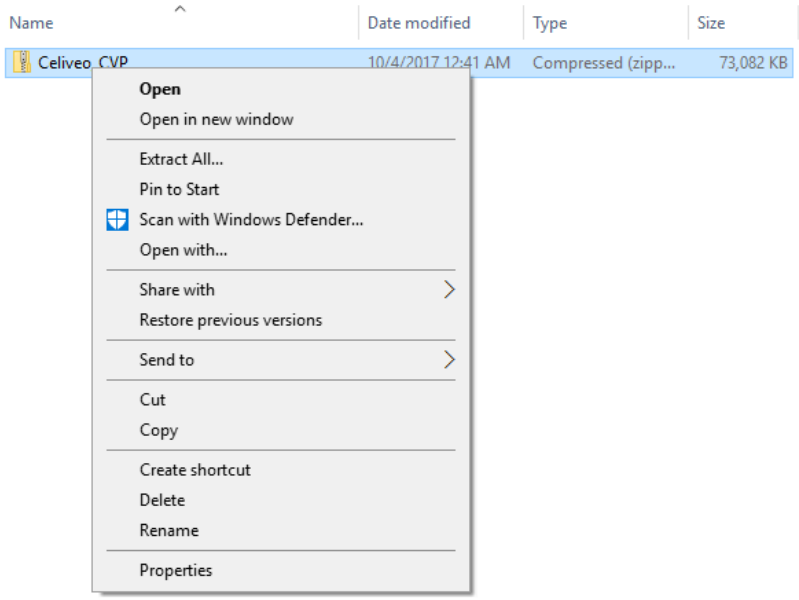
1. In the Web Admin, select the Celiveo Virtual Printer.
2. Click .
   The Virtual Printer Deployment Package downloads.

> **Note**: For Non-Super admins, multiple selections of CVPs are only allowed for download, edit and delete are disabled.

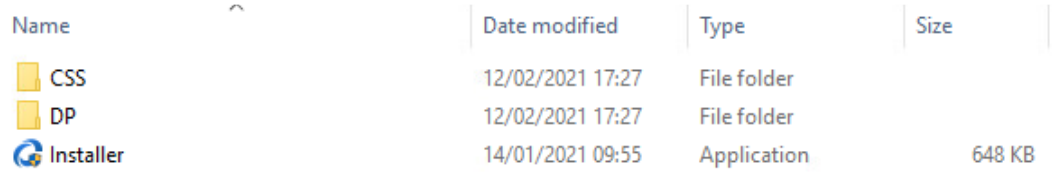
2. Install Virtual Printer on User's Workstation.

> **Note**: Before installing the Virtual Printer, make sure that .Net Framework 3.5 is installed on the workstation.

1. Copy the Virtual Printer Deployment Package to a temporary folder on the user's workstation.
2. Right-click the Deployment Package. A menu displays.



3. Click **[Extract All]**.
4. Select a temporary folder to extract the files to, and click **[Extract]**.



5. Right-click the **[Installer]** and select **[Run as administrator]** to start the installation.
6. Upon installation, a Celiveo Virtual Printer icon is placed on the Desktop and the System Tray.

NOTE 1: Users need to log out and log in again in order to have all rules and quotas applied.
NOTE 2: Please ensure that set the appropriate Permission according to your company policy for all the EXE/DLL in the Celiveo Virtual Printers installation folders which, by default are **C:\Program Files\Celiveo\Celiveo Virtual Printer** for the application files and **C:\ProgramData\Celiveo\Celiveo virtual Printer** for data files. There is no need to have Write permission for those EXE/DLL. You may refer the Security Recommendation (login is required)

2.a. Silent Installation

Silent installation:

This option is useful, to silently install Celiveo Virtual Printer on user workstation without requesting any user interaction.
To do this:

1. Launch the command prompt dialog as Administrator.
2. Run the following command: **installer.exe -s**

Define a custom path:

You can also define a custom path to extract the files and install Celiveo Virtual Printer. To do this:

1. Enter the following command: **installer.exe -t"[folder path]"**.
   E.g: *installer -t"D:\Program Files\Celiveo"*

Upon installation, a Celiveo Virtual Printer icon is placed on the Desktop and the System Tray.

Desktop shortcut:

If you do not wish to create a shortcut on the Desktop, run the following command: **installer.exe -nosc**

With additional storage support (NAS):

You can install Celiveo Virtual Printer with an option to push print job tickets to a Network Attached Storage (NAS). This increases accessibility to the print jobs when CVP is offline (user workstation is shutdown).
To enable this feature during installation, run the following command: **installer.exe -ccp -s**

Note: -s prevents display of any notification popups to users during silent installation.

Install the CSS with a specific port:

If you wish to install the CSS using a specific port, use the following command: **installer.exe -p xxxx (xxxx being the port number)**.

2.b. Silent Uninstallation

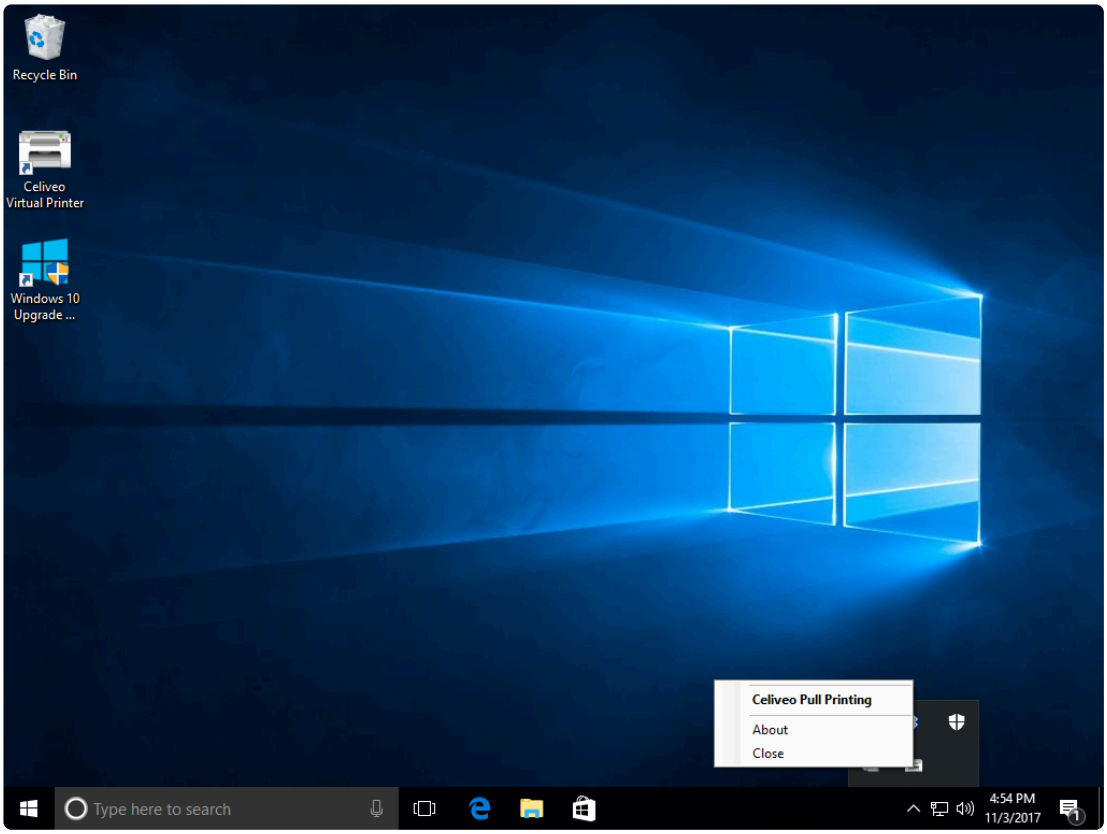
Celiveo Virtual Printer can also removed from user workstations without requesting any user interaction.

1. Launch the command prompt dialog as Administrator.
2. Run the following command: **installer.exe -u**

All binaries are removed from the Install folder.

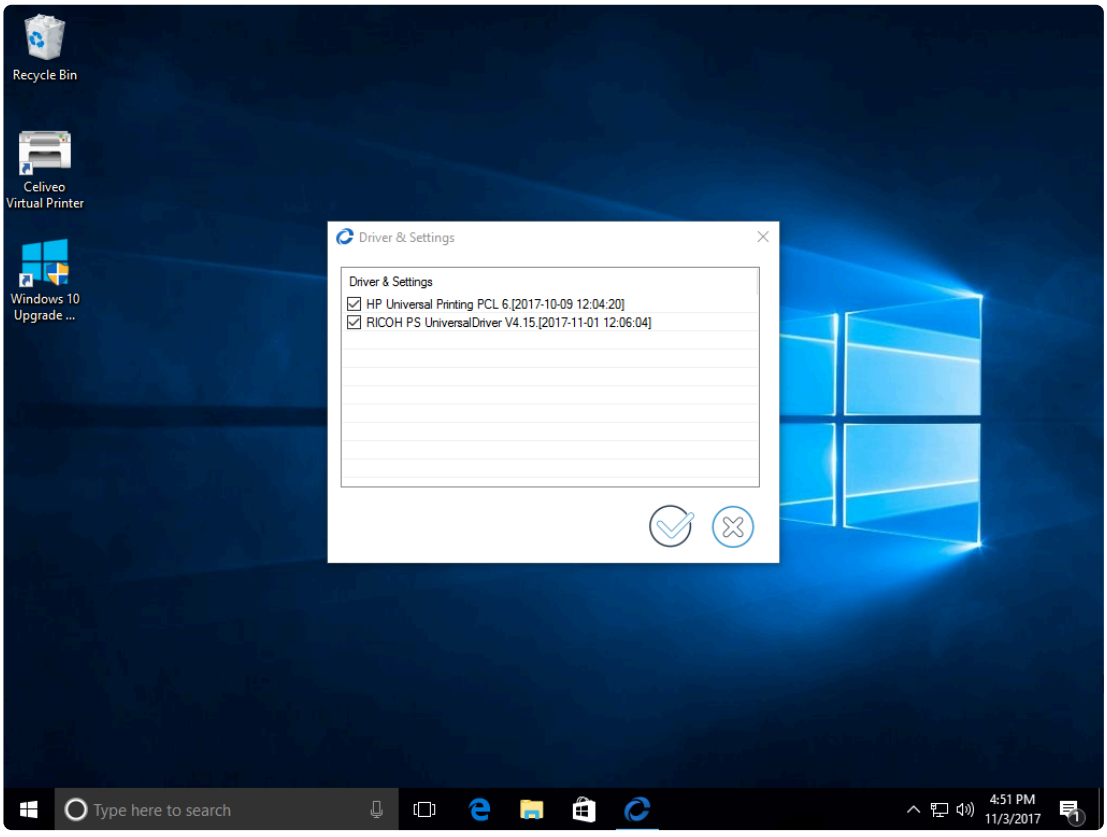
3. Install Printer Queues for Pull Printing

1. Right-click on the system tray. A menu displays.
2. Click **[Celiveo Pull Printing]**.



The Driver and Settings dialog displays.

3. Select the print queues you want to to use on this workstation, and click .



Note: The default name + time-date suffix can be edited in the WebAdmin.

A vertical yellow bar starts running on the Celiveo Virtual Printer system tray icon while the printer is

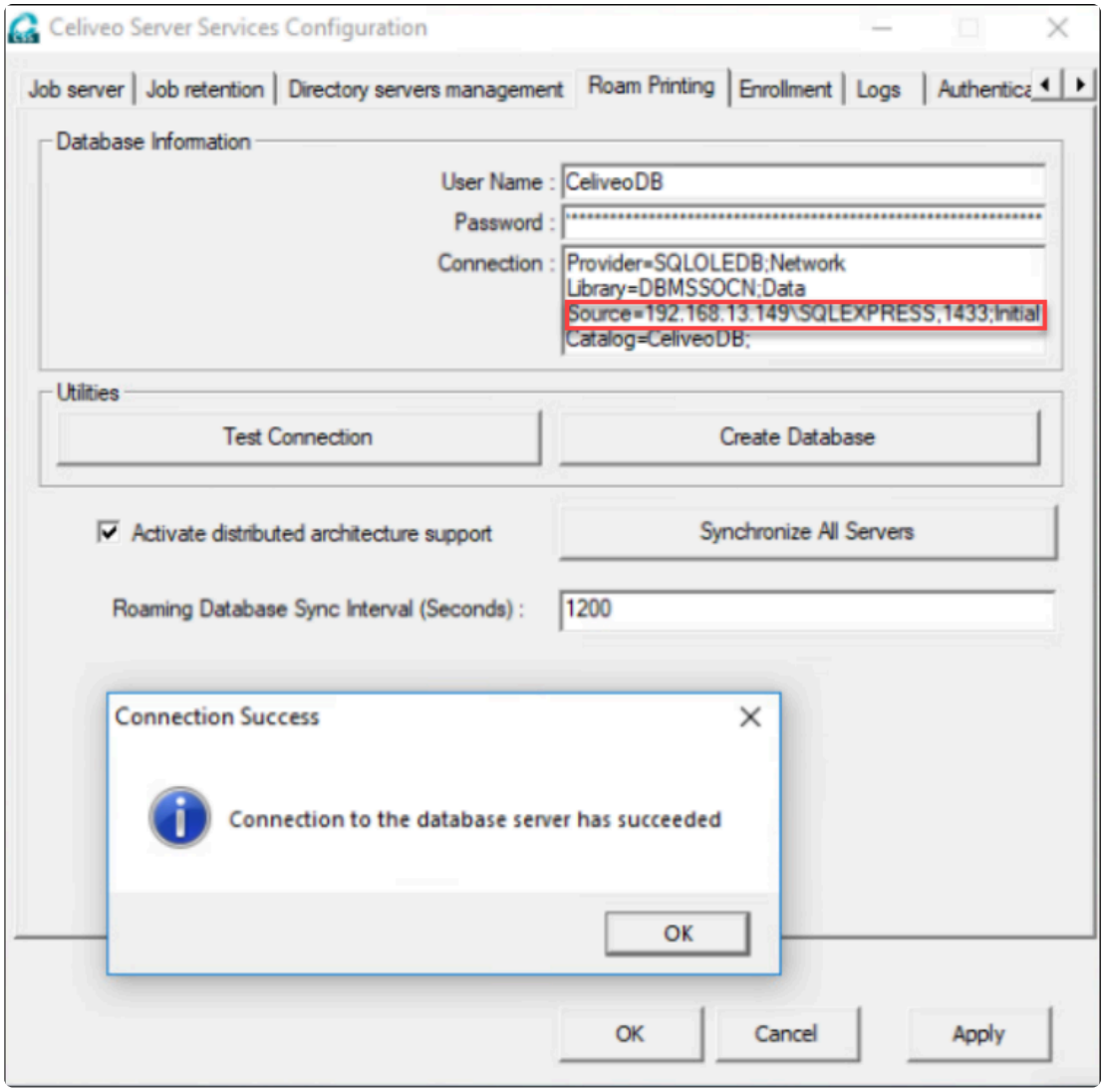
installed on the workstation. The drivers are installed on your workstation. Now when you attempt to print, the print queues are available for selection.

4. Multi-SQL Configuration

If you are intending to use additional SQL databases, make sure that the CVP is using the same Database IP address or hostname as the one set up in the Web Admin, with valid credentials.

This can be verified in the CSS configuration tool. To do so:

1. Go to CSS directory and then launch the configuration UI (Run as administrator)
2. In the **Roam Printing** tab, in the **Database Information** section, check the **Source** field.
3. Test the connection to the Database by clicking the **Test Connection** button.



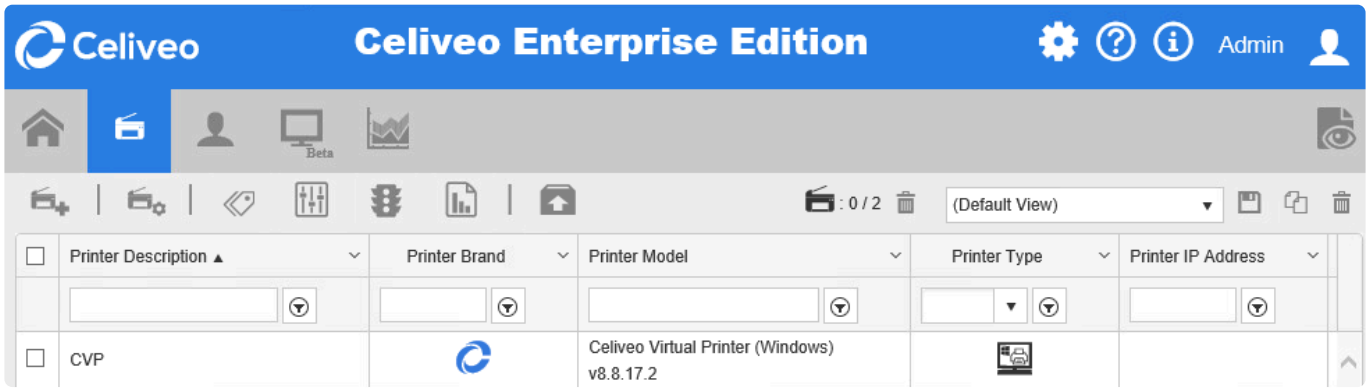
Last modified: 29 September 2022

8.4.7. Deploy a Celiveo Virtual Printer on a User's Work Station (For Direct IP Printing)

Follow the steps below to deploy a Celiveo Virtual Printer on a user's workstation:

1. Download the Virtual Printer deployment package.
2. Install the Virtual Printer on a user's workstation.
   - Silent installation
   - Uninstallation
3. Install Physical Printers for direct print.

1. Download Virtual Printer Deployment Package



1. In the Web Admin, select the Celiveo Virtual Printer.
2. Click .
   The Virtual Printer Deployment Package downloads.

> **Note**: For Non-Super admins, multiple selections of CVPs are only allowed for download, edit and delete are disabled.

BEFORE YOU INSTALL CELIVEO VIRTUAL PRINTER:

In some cases, the Windows Defender antivirus identifies Celiveo Virtual Printer as a threat.

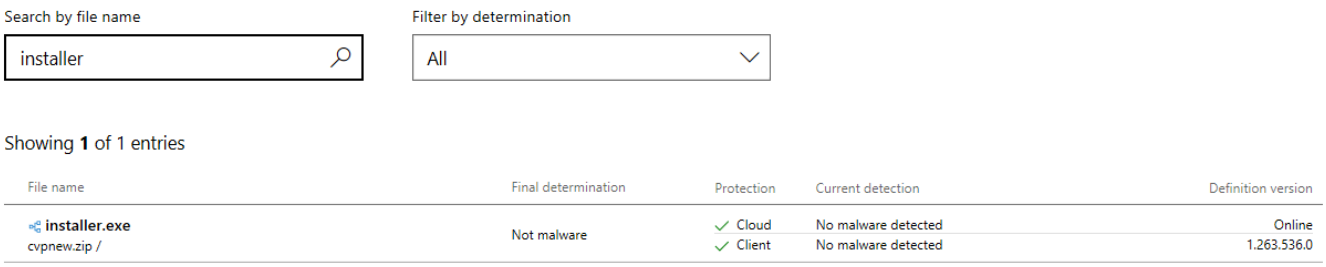
We have submitted the file to Microsoft for a malware analysis who confirmed this was a **false positive** as proven by the reports below:

Search by file name: virtual

Filter by determination: All

Showing **2** of 2 entries

File name	Final determination	Protection	Current detection	Definition version
dp_x86_celiveo virtual printer_setup.msi cvpnew.zip /	Not malware	Cloud Client	No malware detected No malware detected	Online 1.263.536.0
dp_x64_celiveo virtual printer_setup.msi cvpnew.zip /	Not malware	Cloud Client	Trojan:Win32/Critet.BS No malware detected	Online 1.263.536.0



To avoid this problem, make sure that you add Celiveo to the Windows Defender antivirus exclusion list. To do so, add the “C:\Program Files\Celiveo” folder to the exclusion list : https://support.microsoft.com/en-ie/help/4028485/windows-10-add-an-exclusion-to-windows-defender-antivirus.

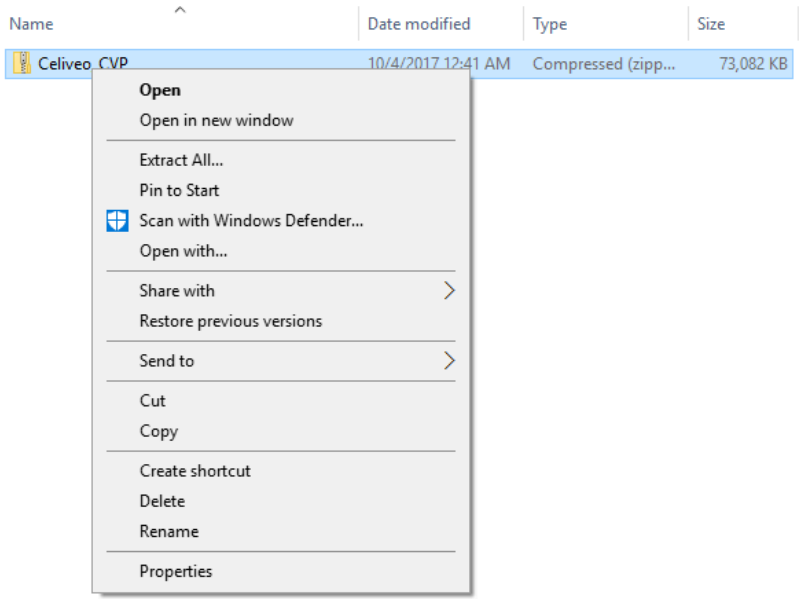
Celiveo software executable files are verified virus/malware using eSET Nod32, then digitally signed, and therefore can’t be patched at a later stage by a virus without triggering a signature failure alert.

If you receive an invalid signature alert, do not run the application as it means software has modified the binary file.

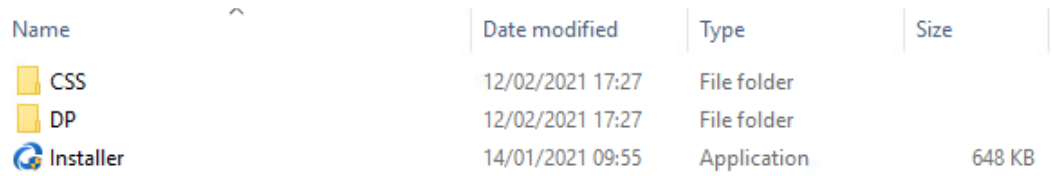
Recent versions of Windows Defender wrongly report some clean obfuscated .Net assemblies as a threat, this is a false positive.
Would you face that issue, we strongly recommend you try another anti-virus to get a confirmation before considering that detection as accurate.

2. Install Virtual Printer on User’s Workstation.

1. Copy the Virtual Printer Deployment Package to a temporary folder on the user’s workstation.
2. Right-click the Deployment Package. A menu displays.



3. Click **[Extract All]**.
4. Select a temporary folder to extract the files to and click **[Extract]**.



Name	Date modified	Type	Size
CSS	12/02/2021 17:27	File folder	
DP	12/02/2021 17:27	File folder	
Installer	14/01/2021 09:55	Application	648 KB

5. Right-click **[Installer]** and Run as Administrator to start the installation.

2.a. Silent Installation

This option is useful, to silently install Celiveo Virtual Printer on the user workstation without requesting any user interaction.

To do this:

1. Launch the command prompt dialog as Administrator.
2. Run the following command: **installer.exe -s**

Define a custom path:

You can also define a custom path to extract the files and install Celiveo Virtual Printer. To do this:

1. Enter the following command: **installer.exe -t"[folder path]"**.
   E.g: *installer -t"D:\Program Files\Celiveo"*

Upon installation, a Celiveo Virtual Printer icon is placed on the Desktop and the System Tray.

Desktop shortcut:

If you do not wish to create a shortcut on the Desktop, run the following command: **installer.exe -nosc**

Alternate Option for Silent Installation:

You can also define a custom path to extract the files and install Celiveo Virtual Printer. To do this:

1. Run the command prompt.
2. Enter the following command:

   installer -t"[folder path]". For e.g: installer -t"D:\Program Files\Celiveo"

- Upon installation, a Celiveo Virtual Printer icon is placed on the Desktop and the System Tray.

> **NOTE**: Users need to log out and log in again in order to have all rules and quotas applied.

2.b. Silent Uninstallation

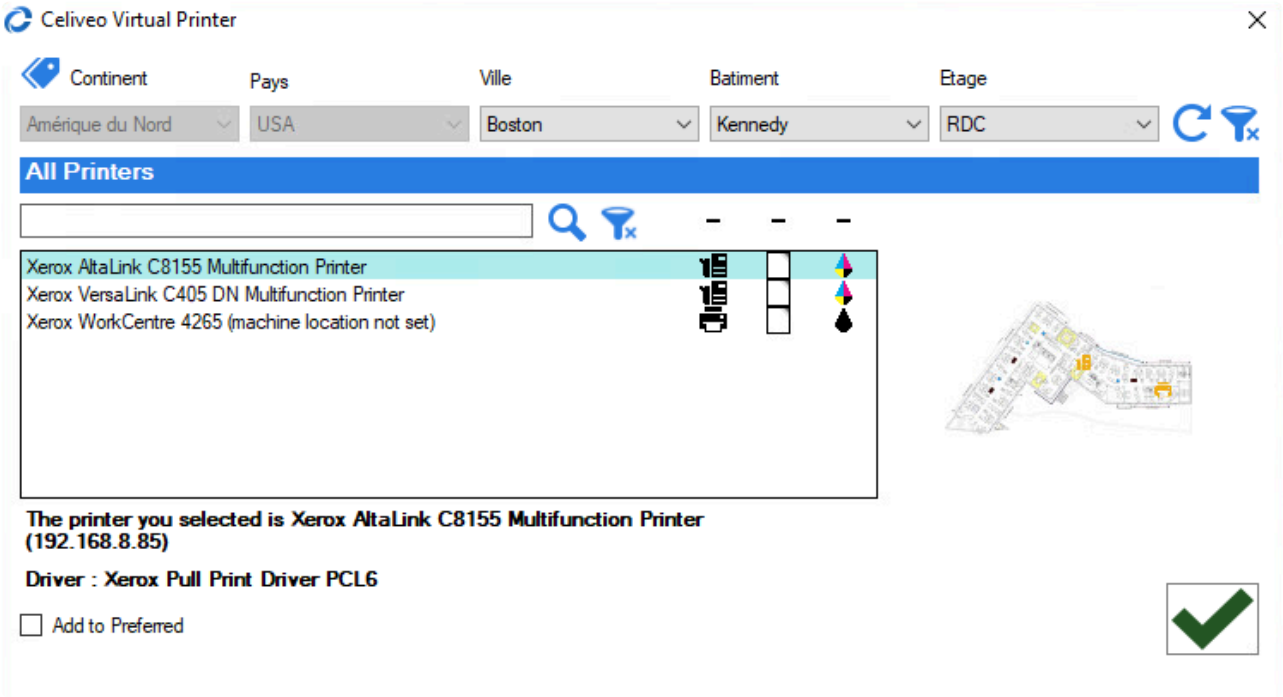
Celiveo Virtual Printer can also be removed from user workstations without requesting any user interaction.

1. Launch the command prompt dialog as Administrator.
2. Run the following command: **installer.exe -u**

All binaries are removed from the Install folder.

3. Install Physical Printers for Direct Print

1. Right-click on the system tray. A menu displays.
2. Click **[Choose another printer]**. The Celiveo Virtual Printer screen displays.
   !(zoom){IMAGE-LINK+



   }!

3. Select the printer to use on this workstation, and click .
   A vertical yellow bar starts running on the Celiveo Virtual Printer system tray icon while the printer is installed on the workstation.
4. Repeat steps 1 – 3 until you have added all the printers you need.

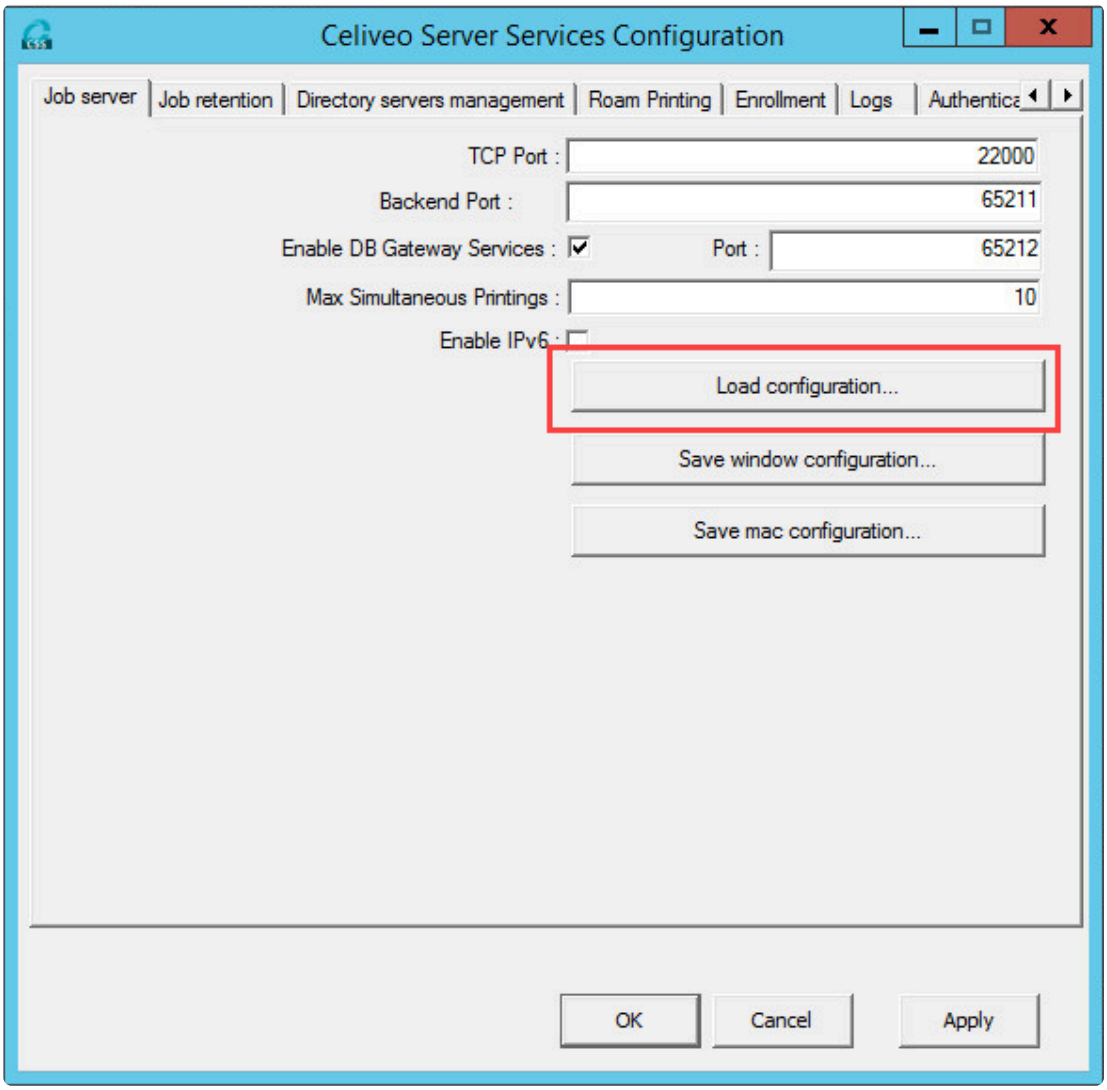
Last modified: 29 September 2022

8.4.8. Upgrade Celiveo Server Services for Windows

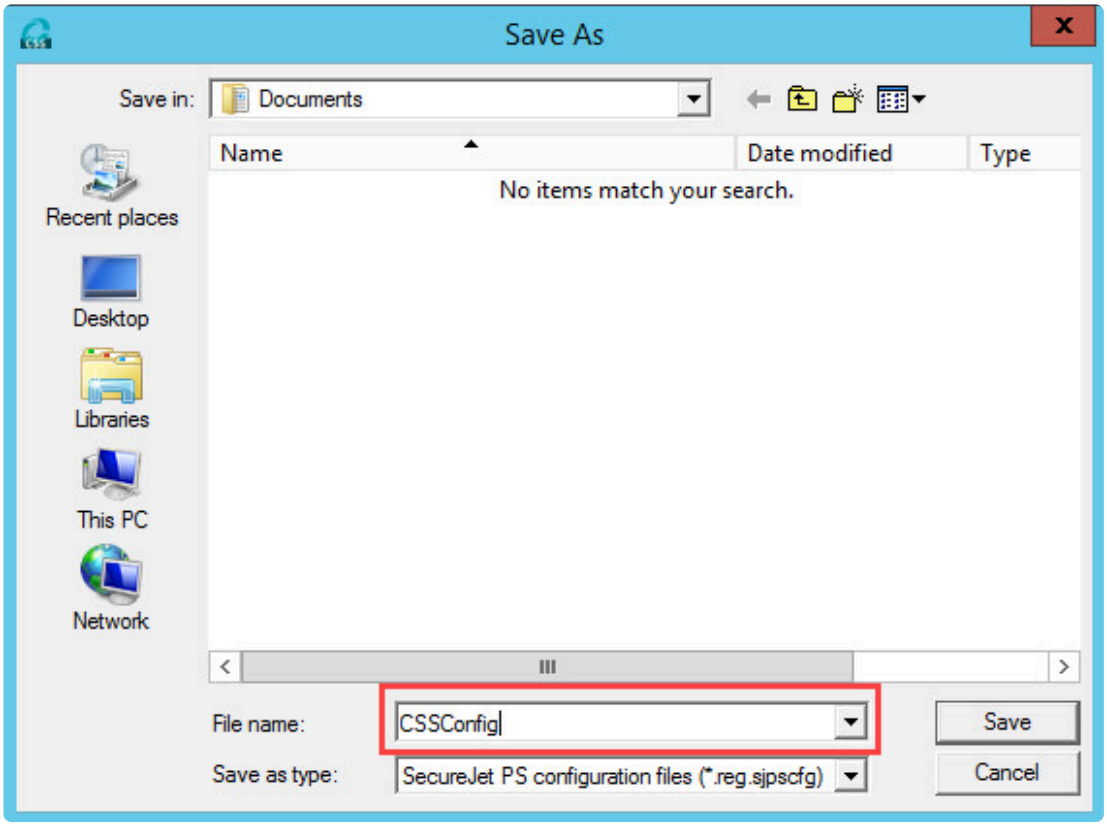
Before you begin…

Before migrating your database to a new version of Celiveo Server Services, you need to save the existing CSS configuration.

1. On the Server, go to the install directory of your existing version of Celiveo Server Services
2. Click **[Celiveo Print-PS Configuration]** to open the Celiveo Server Services configuration UI.
3. On the **Job Server** tab, click the **Save configuration** button.



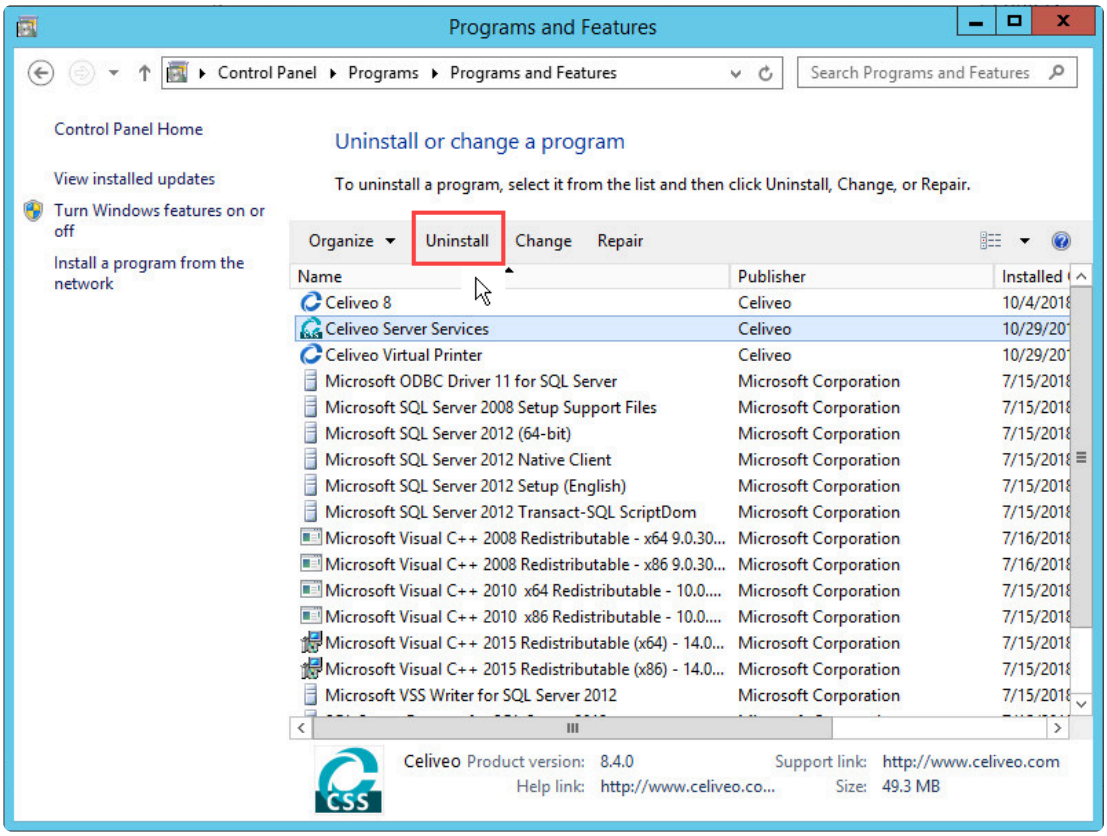
4. Save the configuration file at the location of your choice.



Uninstalling the previous version

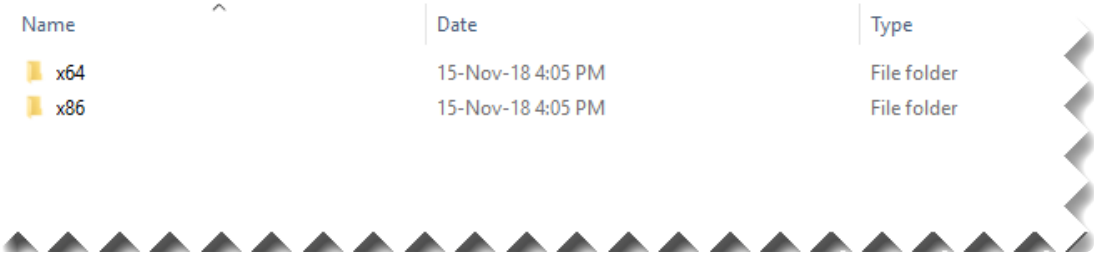
Use the Windows Server Control Panel to uninstall your current version of Celiveo Server Services

1. Go to **Control Panel > Programs and Features > Uninstall or change a program.**
2. Select **Celiveo Server Services** and click **[Uninstall]**.
3. When prompted, select **Yes**.

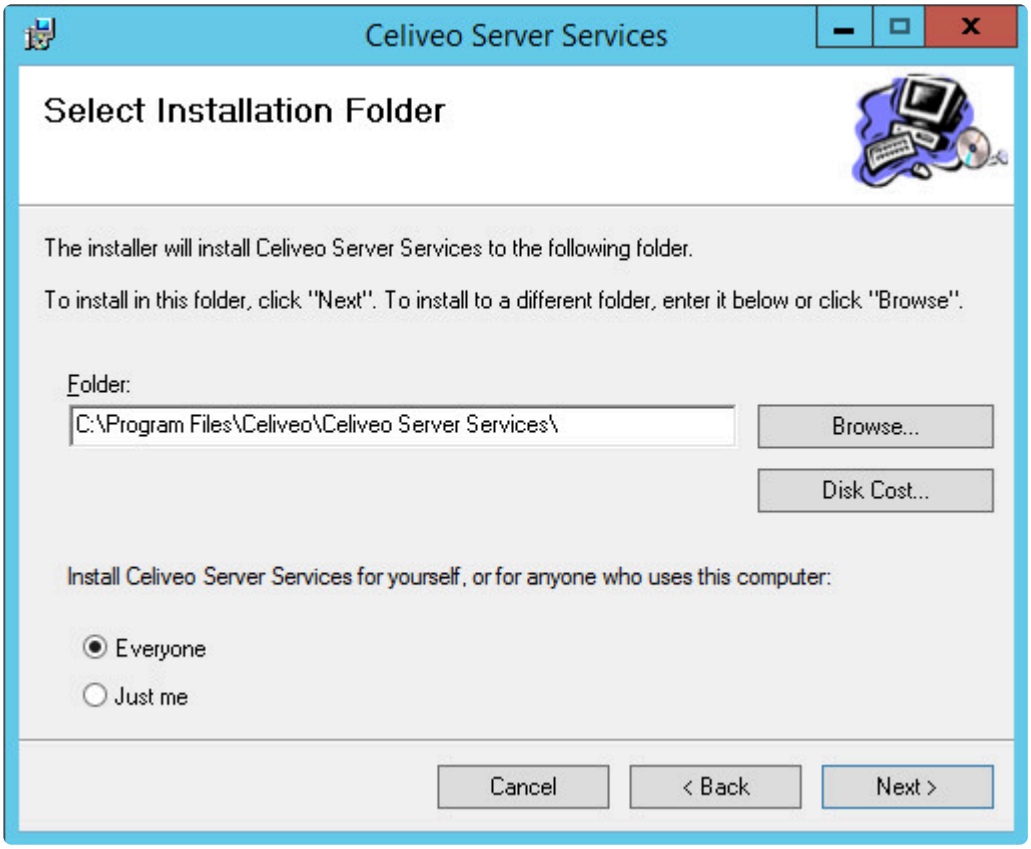


Installing the new version

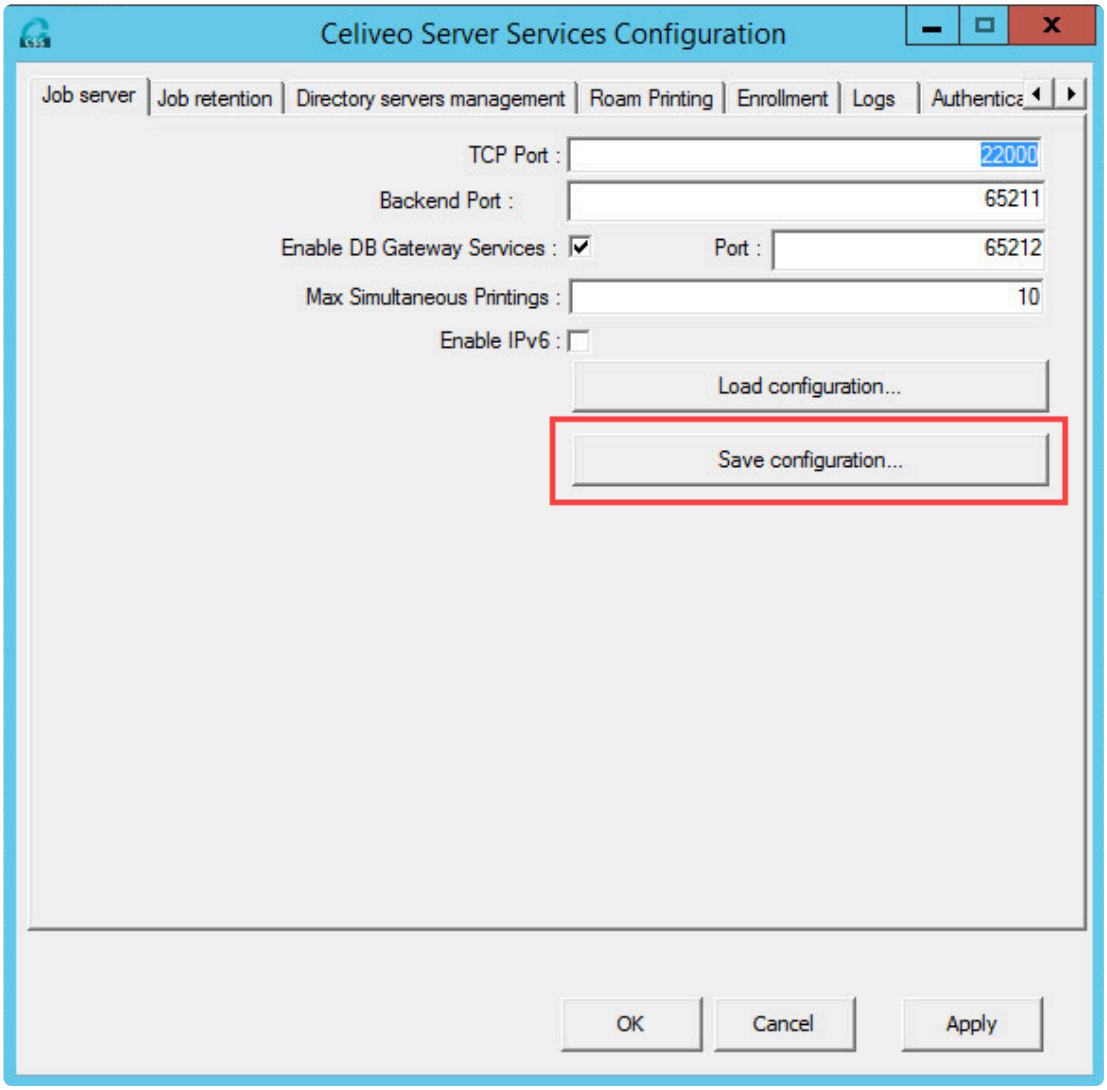
1. The latest CSS deployment package can be downloaded from here.
2. Download the deployment package and extract the files to a temporary folder.
3. Double-click the CSS directory.
4. Choose the installer based on the OS version of Windows running on the Server.



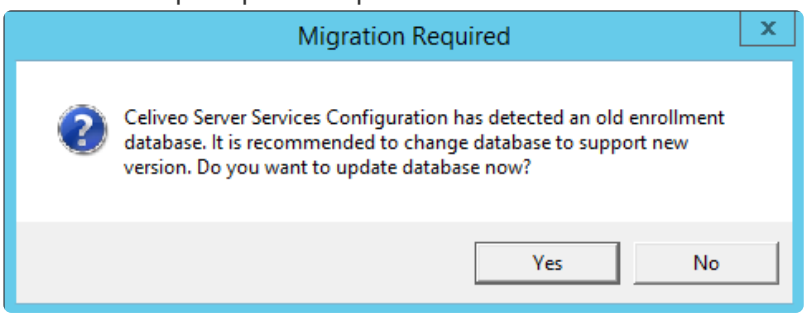
5. The Celiveo Server Services Installation Wizard opens. Click **Next** and accept the License Agreement.
6. Select the Installation Folder and the users for whom you wish to install the program and click **Next**.



7. When the *Installation Successful* message displays, click **Close**.
8. Open the Celiveo Server Services configuration tool.
9. On the **Job Server** tab, click the **Load configuration** button.

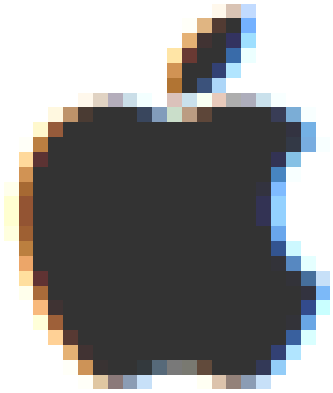


10. Select the configuration file you had previously saved and click **Open**.
11. You are now prompted to update the database. Select **Yes**.



Last modified: 29 September 2022

8.5. Celiveo Virtual Printer for macOS



The Celiveo solution is also available on macOS!

Install Celiveo Virtual Printer on multiple macOS workstations – Silent Install Procedure
Add a Celiveo Virtual Printer on macOS machine – Interactive Install Procedure
Connect to a Windows Celiveo Shared Virtual Printer from macOS machine
Upgrade Celiveo Secure Services for macOS
Configure Celiveo macOS NAS Job Transfer with Job Delegation
Upgrade Celiveo Server Services for Windows

Last modified: 29 September 2022

8.5.1. Install Celiveo Virtual Printer on multiple macOS workstations – Silent Install Procedure

Before you begin…

1. Pre-installation requirements

On the macOS client machine, make sure the minimum system requirements for installation are met.

2. Export the settings configuration file

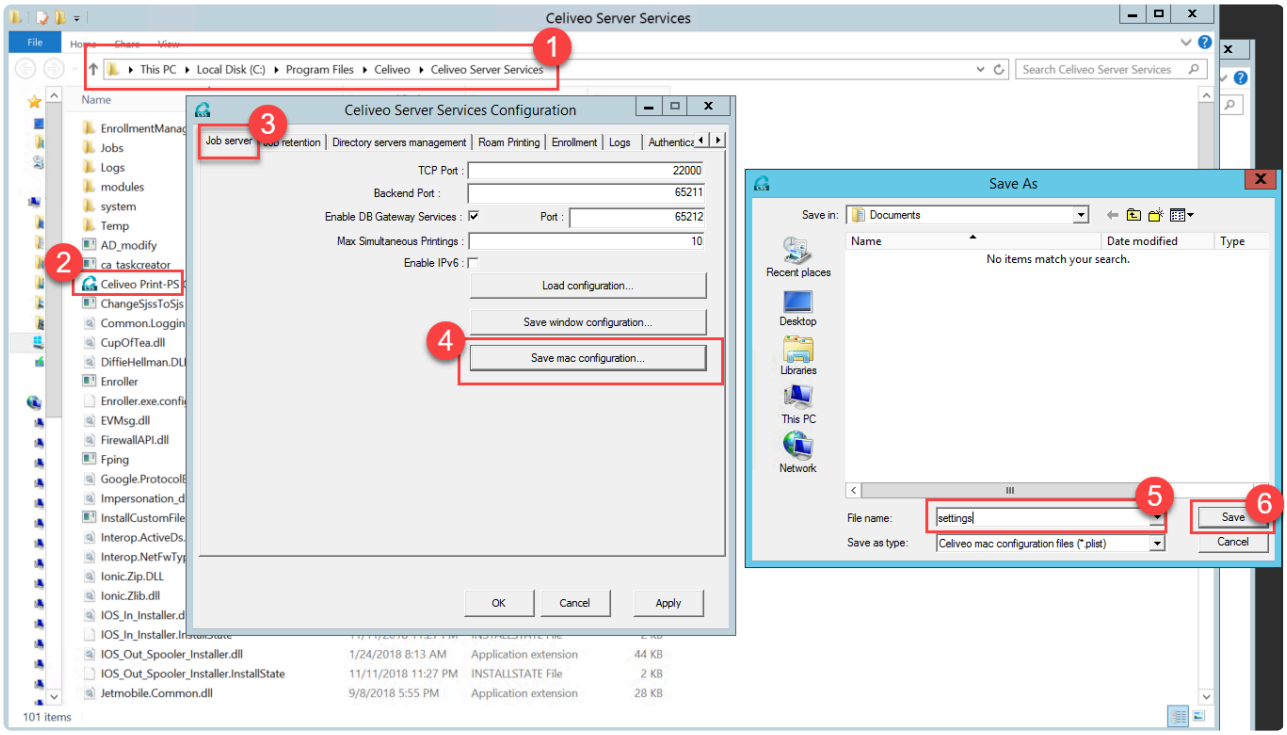
The CVP Installer package for macOS contains the following folder and files:

- *Printer Setup – Folder containing configuration files and Print Queue creation scripts*
- *Celiveo Server Services-8.4.pkg – Install file*
- *Celiveo Server Services-8.4-uninstall.pkg – Uninstall file*
- *installer.sh – Silent install script*
- *settings.plist – Configuration file for logging and database*

Before you install the Celiveo Virtual Printer on the macOS machine, the database and other configuration details have to be setup in the Settings file present in the deployment package. You have to generate a Settings file which will automatically retrieve the database configuration, and then export this file onto the deployment package.

Prerequisite: Make sure you have the latest CSS – Celiveo Server Services – installed on the Server. You can refer to this article on how to upgrade CSS.

1. Log into Windows Server.
2. Go to Celiveo Server Services directory and then launch the configuration UI (Run as administrator).
3. On the **[Job Server]** tab, click **[Save mac configuration]** button.
4. A popup appears for saving the configuration file. Type file name as “settings” and click **[Save]**. This retrieves the database configuration automatically and creates **settings.plist** file on the given path.



5. Export this Settings file onto the macOS machine, where the CVP is to be installed.
6. Replace with the existing “settings.plist” file in the deployment package.

3. Additional configuration

Two settings need to be configured before starting the install process:

1. In the **Printer Setup** folder, open the PrinterConfig.ini file and define a Print Queue name.

> ***Note**: Do not use any space for the Print Queue name*

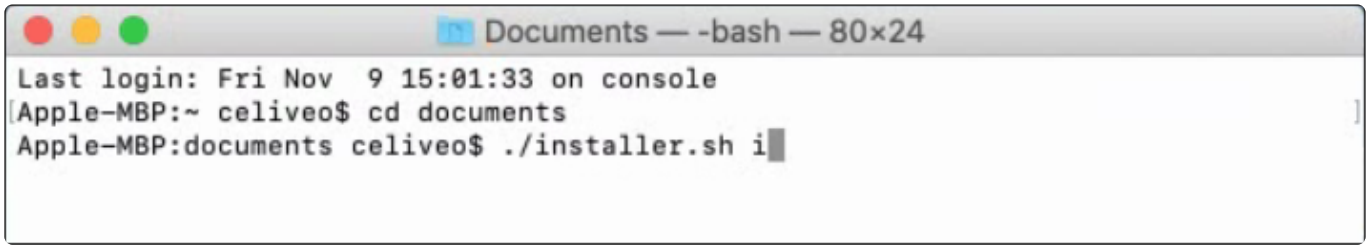
2. In the same file, indicate the path to the folder containing the driver to use.

> ***Note**: By default, the script uses the macOS generic PostScript driver. In case a different driver is required: Download and install it prior to this step, and then indicate its location (file with .pdd extension) in the ini file.*

Launching Silent Install Process

1. On the admin machine, launch the command prompt dialog.
2. Call the silent installer by typing the following command: **./installer.sh i**

> ***Note**: First make sure you are in the right folder. To do so, type **cd < path to the folder >***



A Pull Print queue is automatically created.

Uninstalling a Celiveo Virtual Printer silently

Celiveo Virtual Printer can also be removed silently from macOS machine, ie without requesting any user interaction.

1. On the admin machine, launch the command prompt dialog.
2. Call the silent uninstaller by typing the following command: **./installer.sh u**

All binaries are removed from the Install folder.

> ***Note**: Although the solution files have been removed, Print jobs remain for migration purposes.*

Last modified: 29 September 2022

8.5.2. Add a Celiveo Virtual Printer on macOS machine – Interactive Install Procedure

The Celiveo macOS CVP is an independent module used to deploy on a user machine using MacOS X that enables the user to print on a Celiveo-enabled printer. This stand-alone deployment package comprises of:

- Install executable file
- Uninstall executable file
- Settings configuration file
- Printer Setup directory (configuration to create pull-print queue name and retrieve printer driver path – this is applicable while performing Silent installation. See this article for instructions on silent installation procedure.)
- Silent Installation script (applicable for silent installation)

IMPORTANT NOTE: The CVP installable is applicable ONLY for Celiveo 8.

Before you begin…

On the macOS client machine, make sure the minimum system requirements for installation are met.

Follow the steps below to deploy a Celiveo Virtual Printer on macOS machine.

1. Export the settings configuration file.
2. Manually install the CVP on macOS machine.
3. Create a pull print queue on macOS machine.

1. Export the settings configuration file

Before you install the Celiveo Virtual Printer on the macOS (client) machine, the database and other configuration details have to be setup in the Settings file present in the deployment package. You have to generate a Settings file which will automatically retrieve the database configuration, and then export this file onto the deployment package.

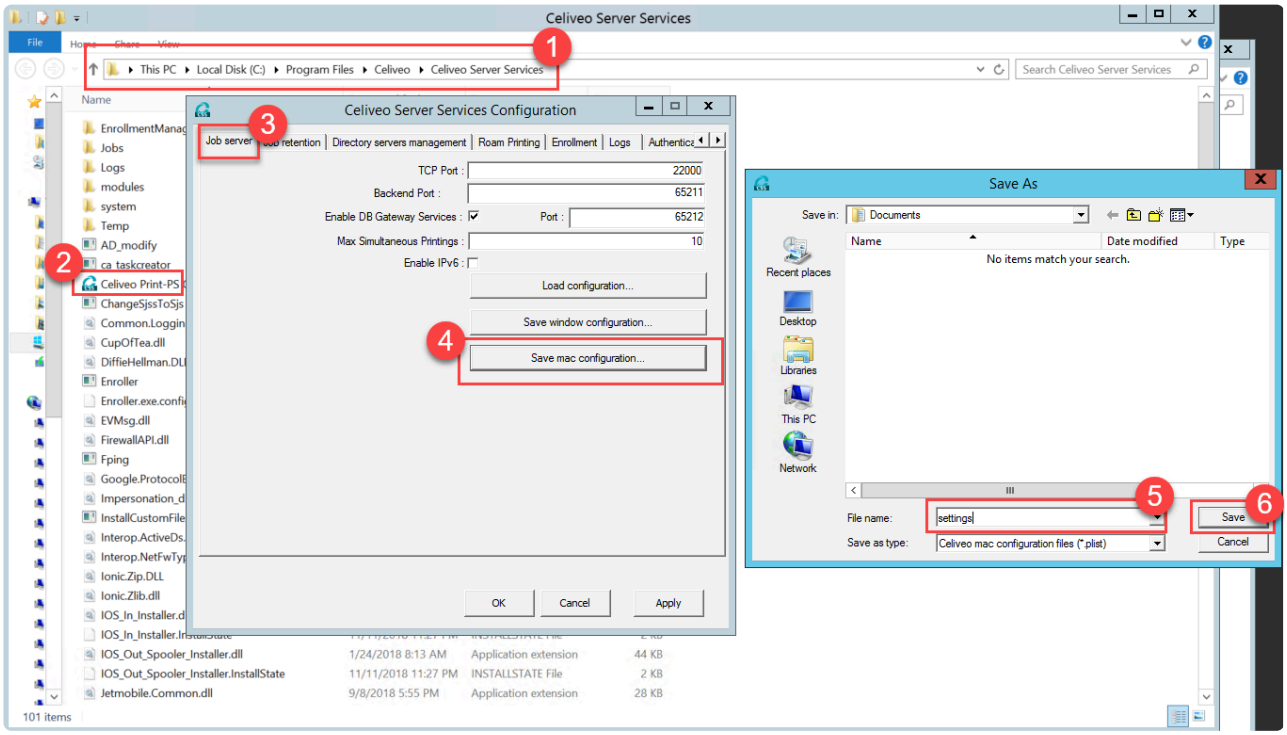
The Setting file can be generated by following these steps:

Step 1: In Web Admin (Celiveo 8.0.1/ 8.0.2)

1. Install the latest version of Celiveo Server Services (CSS). You can refer to this article on how to upgrade CSS.
2. Once successfully installed, go to Web Admin application.
3. Select the new CSS in the Web Admin and synchronize.
4. Now, go to the new CSS Configuration Console and export the macOS settings file.

Step 2 : In Windows CSS/CVP on Client or Server:

1. Log into the target machine with Celiveo CSS/CVP.
2. Go to CSS directory and then launch the configuration UI (Run as administrator).
3. On the **[Job Server]** tab, click **[Save mac configuration]** button.
4. Validate that Roam Printing contains SQL information, Server connection string, Username/ Password (This is the information that will be exported to the file **settings.plist** that is then used by the macOS CVP installer).
5. A popup appears for saving the configuration file. Type file name as “settings” and click **[Save]**. This retrieves the database configuration automatically and creates **settings.plist** file on the given path.

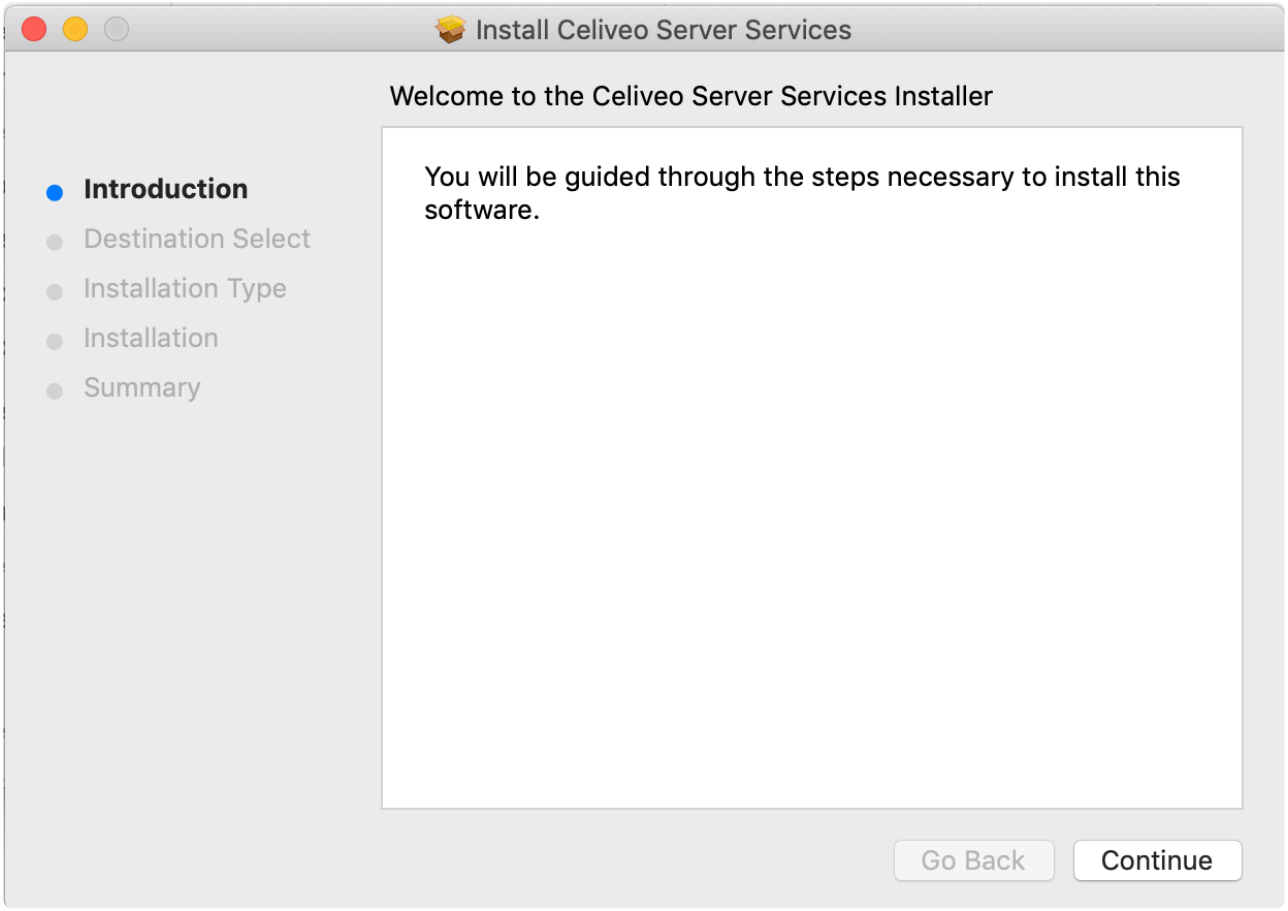


6. Export this Settings file onto the macOS machine, where the CVP is to be installed.
7. Replace with the existing “settings.plist” file in the deployment package.

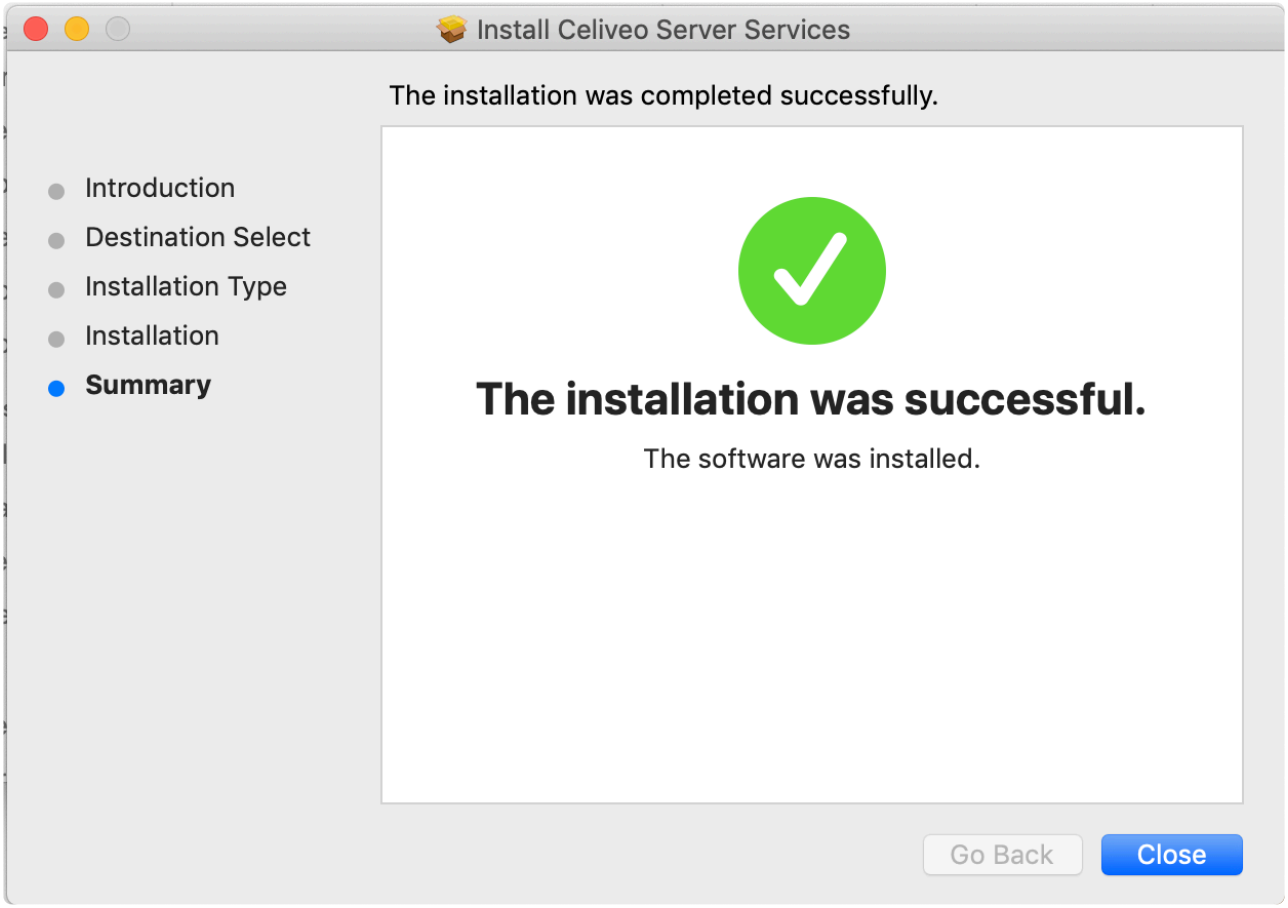
2. Manually install the Virtual Printer on macOS machine

To install :

1. Copy the Celiveo Virtual Printer Deployment Package to a temporary folder on the user’s machine.
2. Right-click the Deployment Package. A menu displays.
3. Click **[Extract All]**.
4. Select a temporary folder to extract the files to, and click **[Extract]**.
5. Replace the existing Settings file with the exported one onto this folder.
6. Double-click **[Installer]** to start the installation wizard.



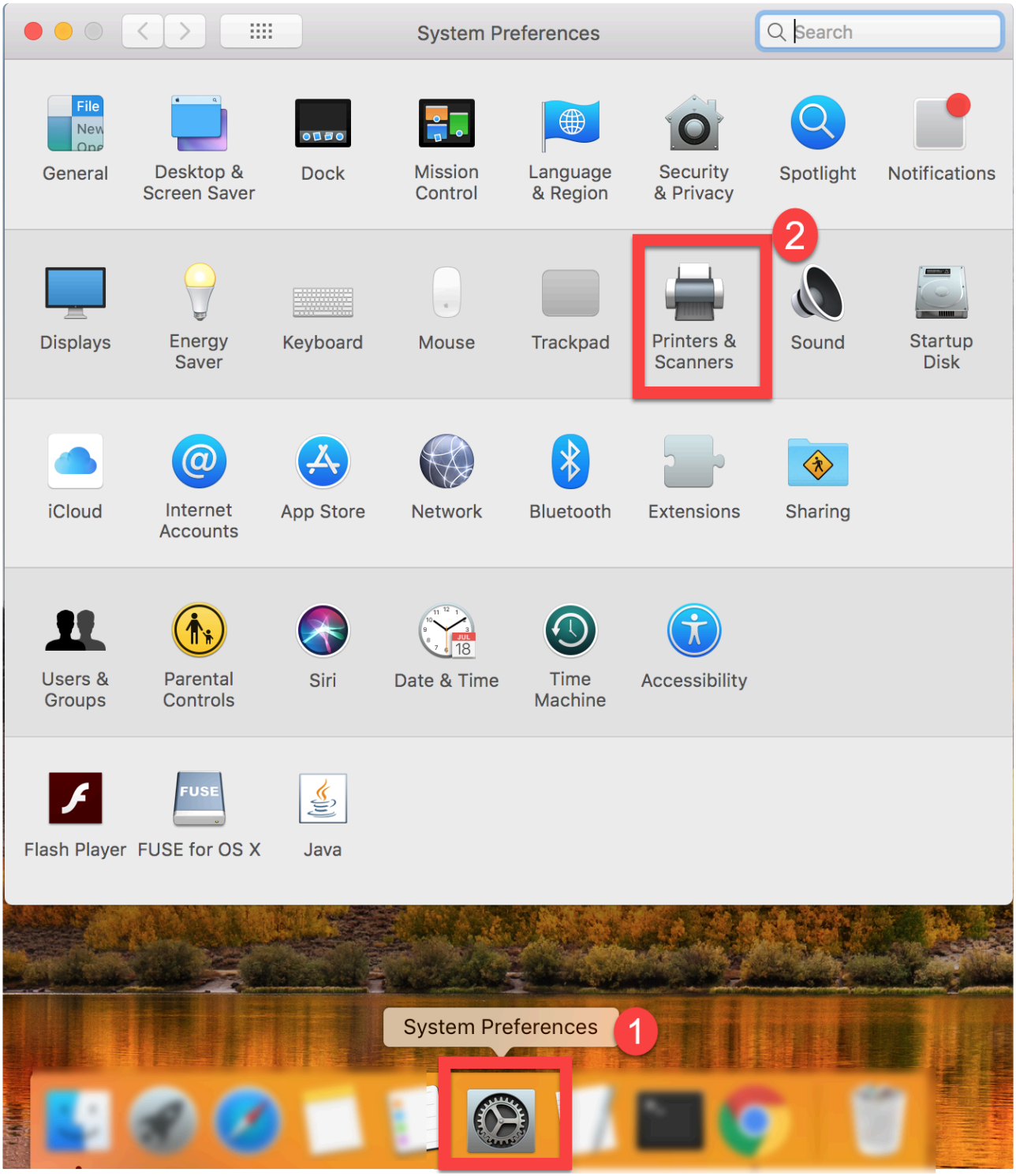
7. Continue with the instructions given on the installation wizard till the installation is successful.



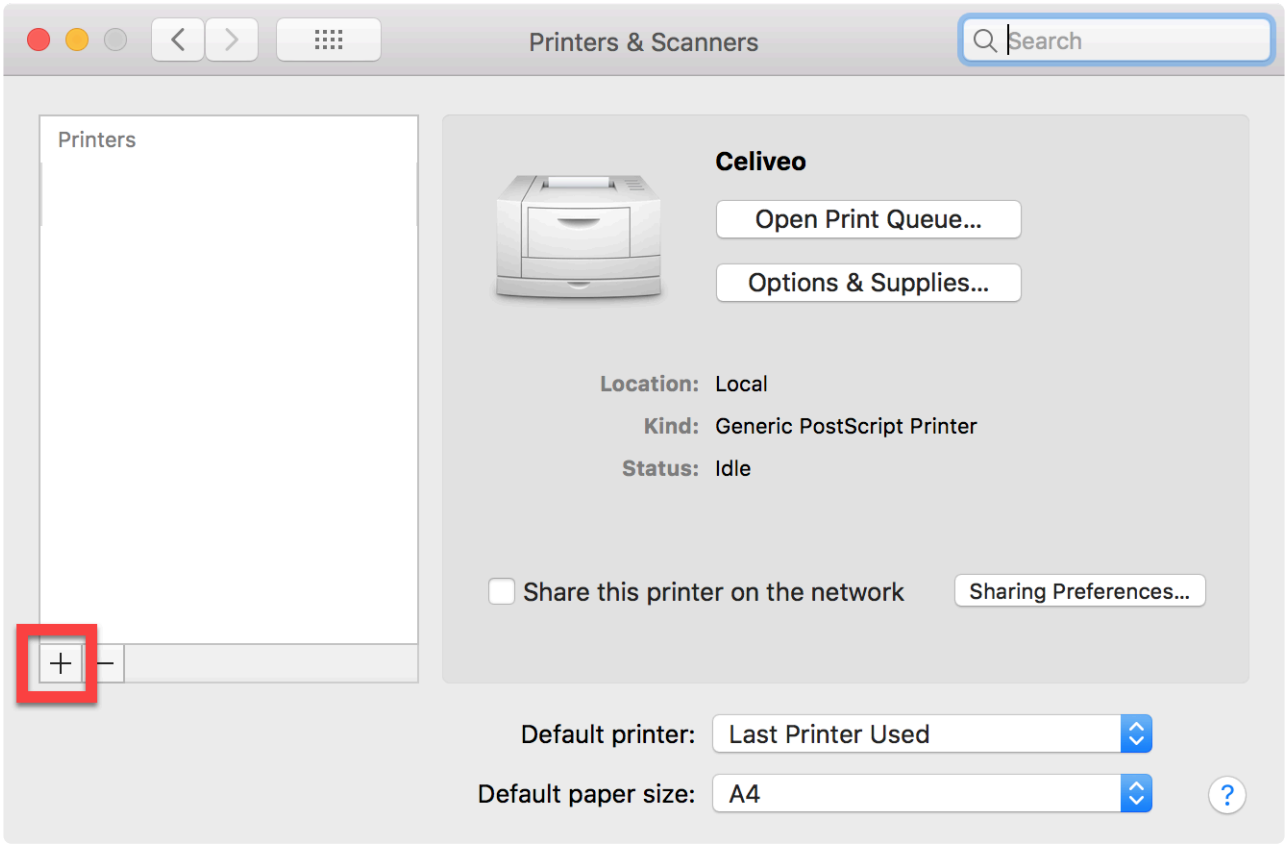
3. Create a pull print queue on macOS machine

Follow the below steps to add a print queue to macOS machine:

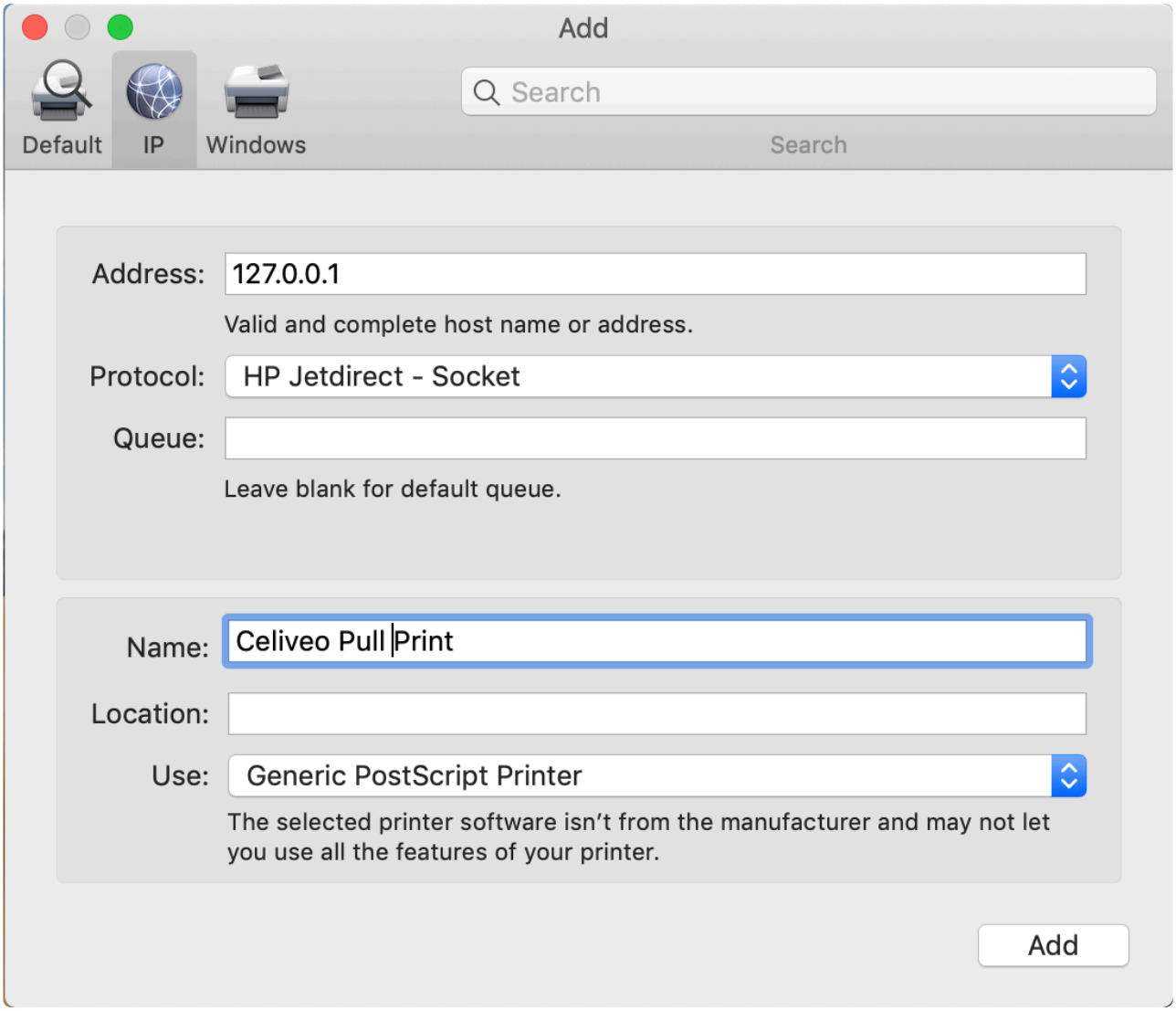
1. In your Mac machine, go to **System Preference**.
2. Click **Printers and Scanners**.



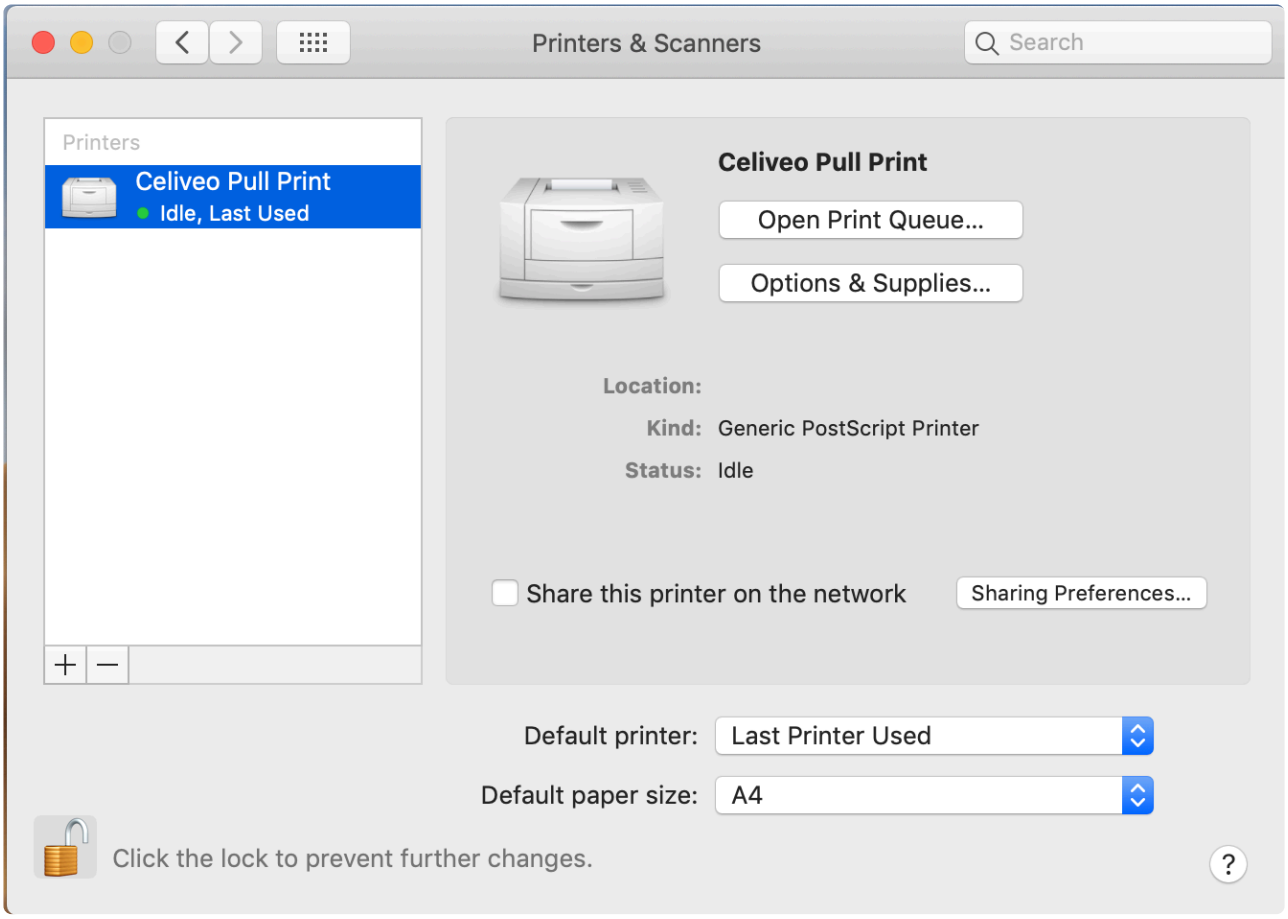
3. Click the [+] sign to add new printer.



4. Go to **IP** tab and fill the settings as shown in the screenshot below.



5. Then, click **Add**.
6. The Celiveo pull print queue is now added.



> We recommend to use the printer drivers supplied by the printer vendors instead of genetic drivers, as otherwise some printer capabilities may be missing or not working as expected.

Uninstall the Celiveo Virtual Printer from macOS machine

Celiveo Virtual Printer can be removed using the Uninstall executable file provided in the deployment package.

1. On the user machine, launch the **[Uninstall]**. The installation wizard opens up.
2. Continue with the instructions given on the installation wizard till the un-installation is successful.

All binaries will be removed from the Install folder.

> **Note**: Although the solution files are removed, Print jobs remain for migration purposes.

Last modified: 29 September 2022

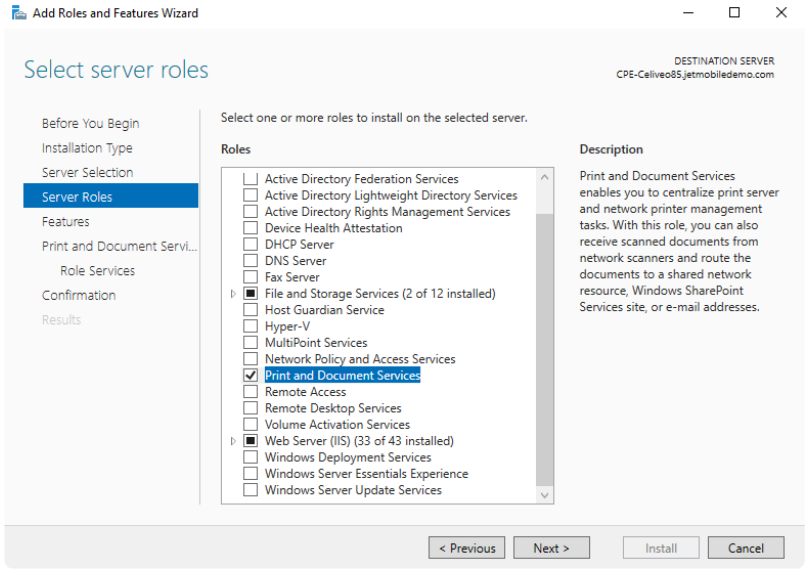
8.5.3. Connect to a Windows Celiveo Shared Virtual Printer from macOS machine

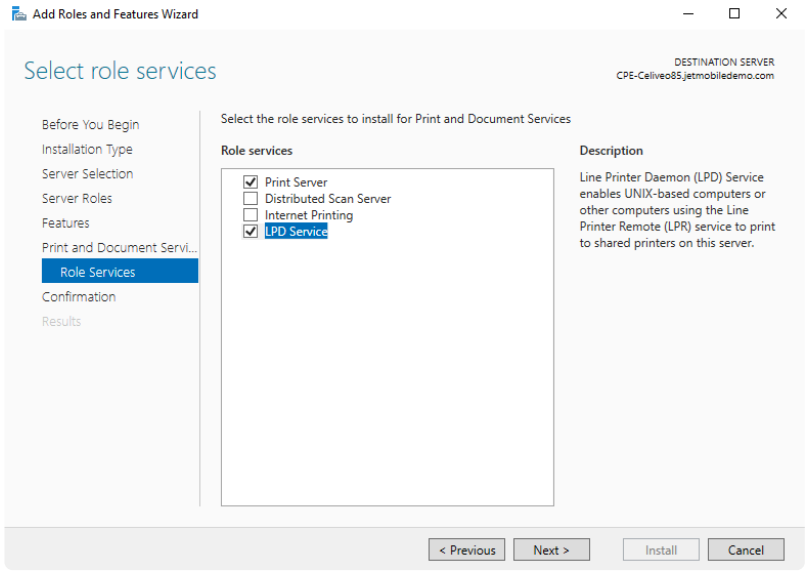
Creating a Celiveo Shared Virtual Printer (server based pull printing) follows a different procedure for macOS with respect to Windows OS.

Before you begin…

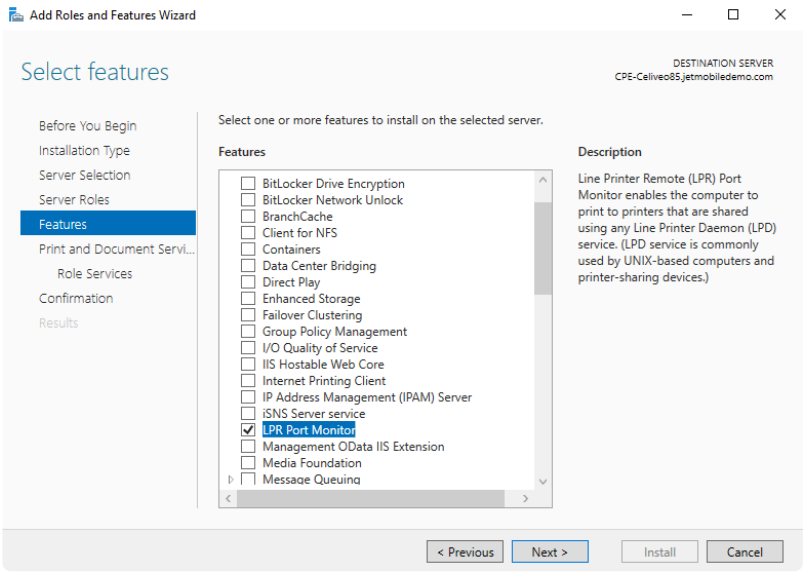
The shared print queue must be created in the Windows Print Server to support macOS printing. For this setting, the print queue on the server must have the pre-processing filter configured.

1. On the Print Server, enable **LPD Service and LPR Port Monitor**. (Enabling these features allows printing to shared printers on this server).
2. To do this:
   a. Go to **Add Roles and Features > Server Roles**
   b. Locate and select the **Print and Document Services** checkbox. Click to display **Role Services** sub menu.
   c. Select **LPD Service** checkbox.

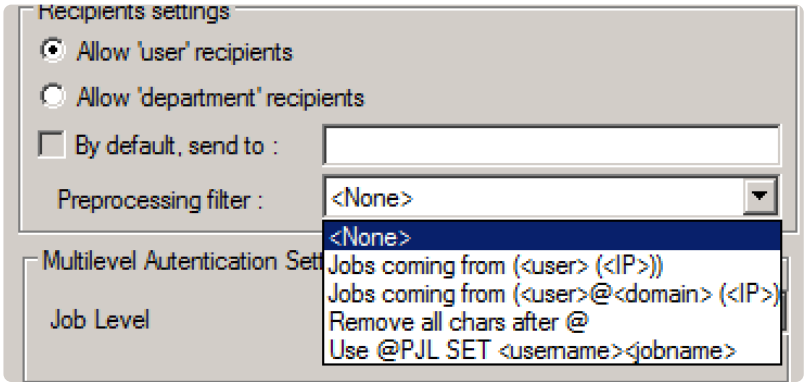




d. Click **Next**. Select **LPR Port Monitor** under **Features**.



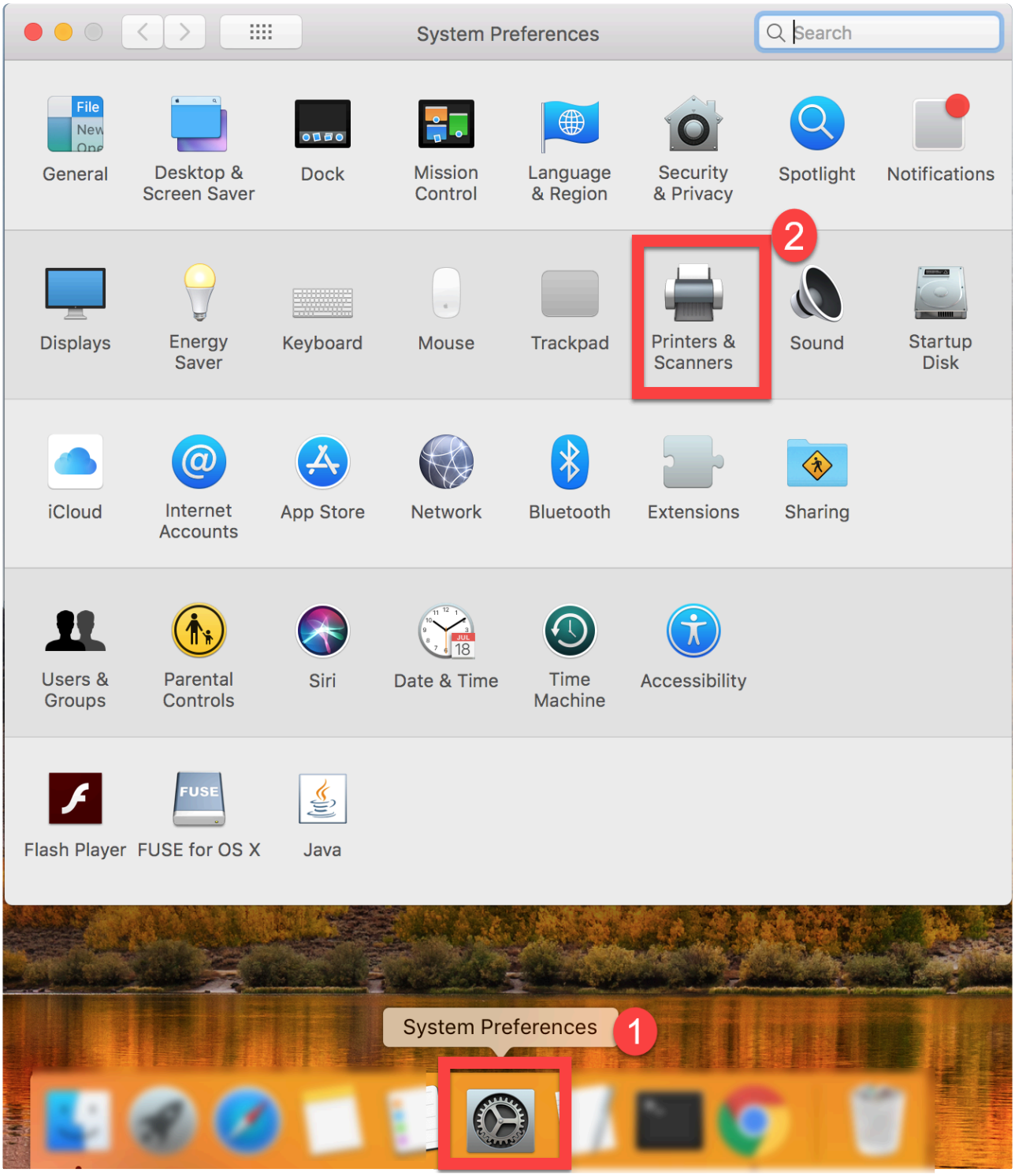
3. Create a Celiveo Shared Virtual Printer (CSVP) on the Print Server. Refer to the article here on how to deploy and create CSVP on Print Server.
4. Go to Printer Properties option of the CSVP.
5. Under **Celiveo Pull Printing** tab, set the **Preprocessing filter** depending on the Username format sent by the host machine.



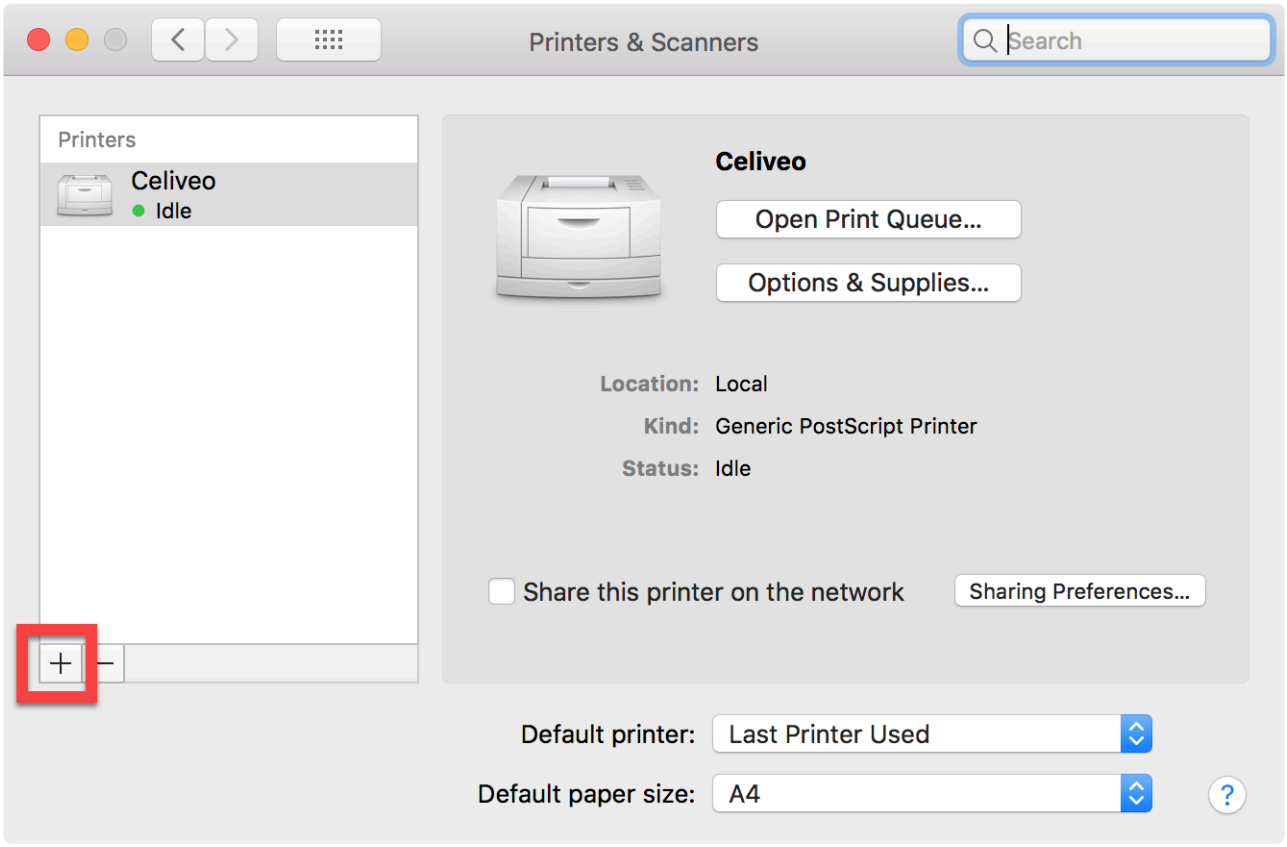
Connect to CSVP from macOS machine

Follow the below steps to add a server based Celiveo print queue on macOS machine:

1. In your macOS device, go to **System Preference**.
2. Click **Printers and Scanners**.

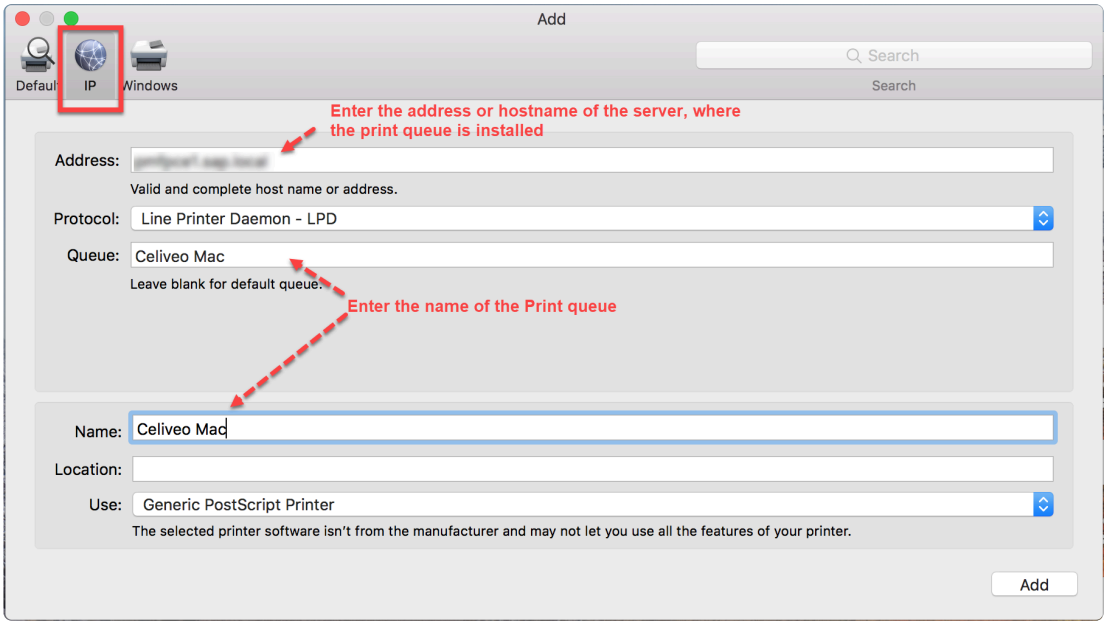


3. Click the [+] sign to add new printer.

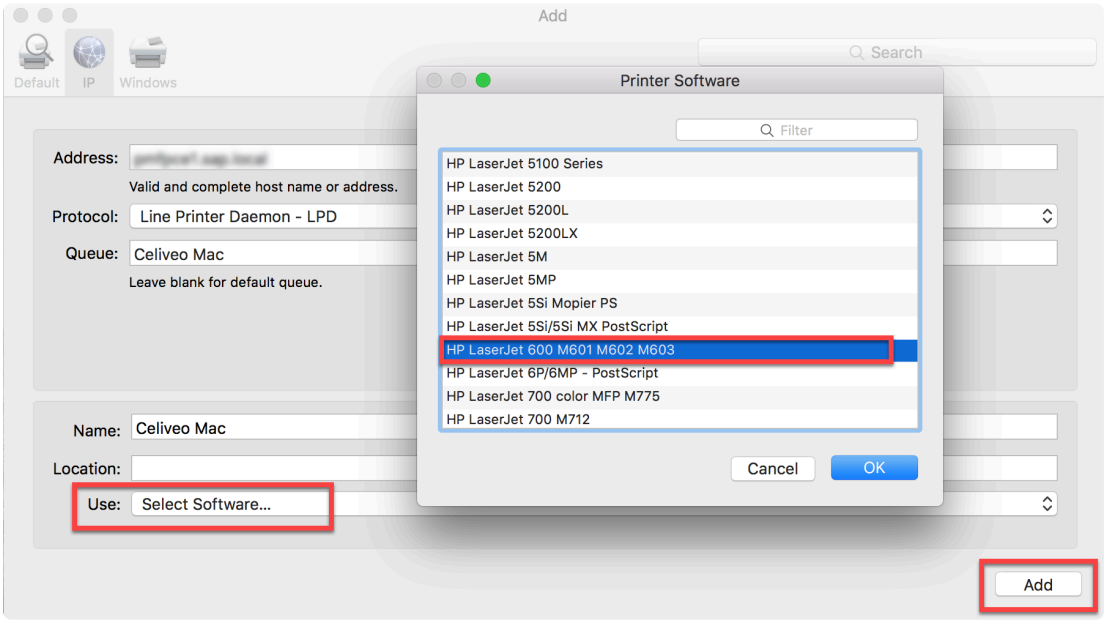


Using IP tab:

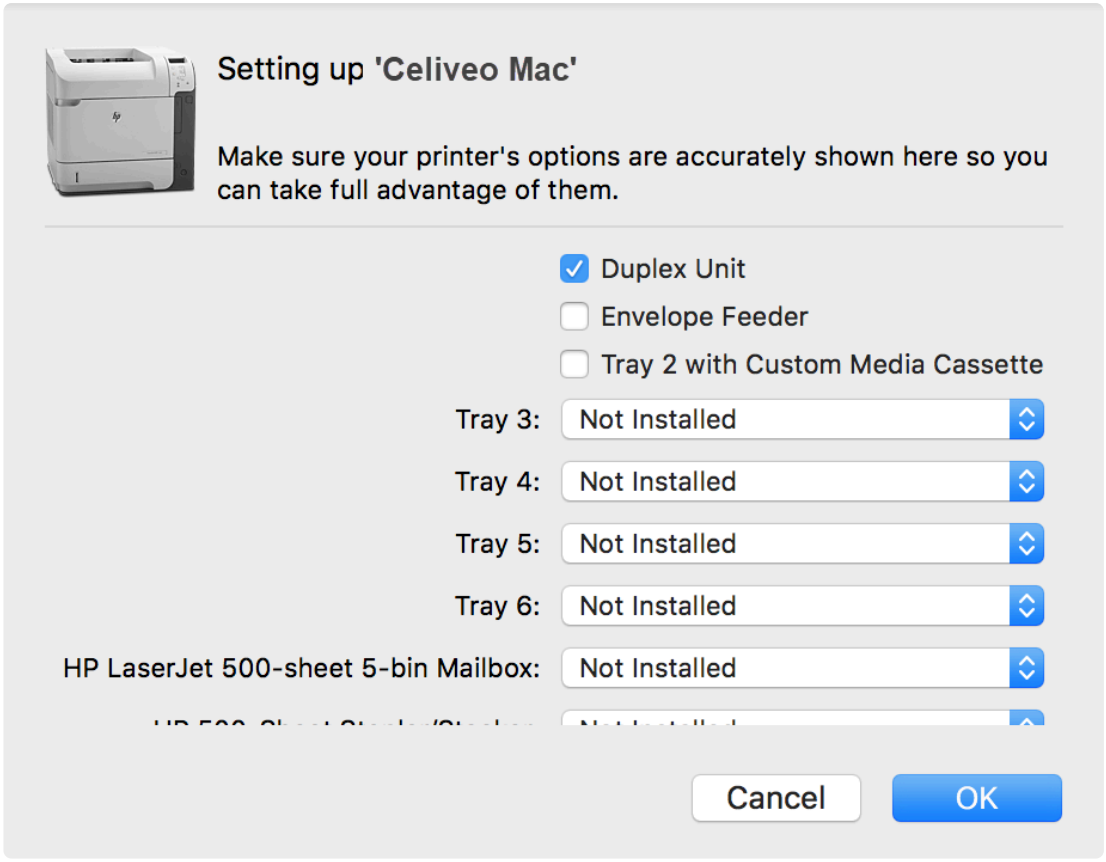
1. Go to **IP** tab and fill the settings as mentioned in the screenshot below.



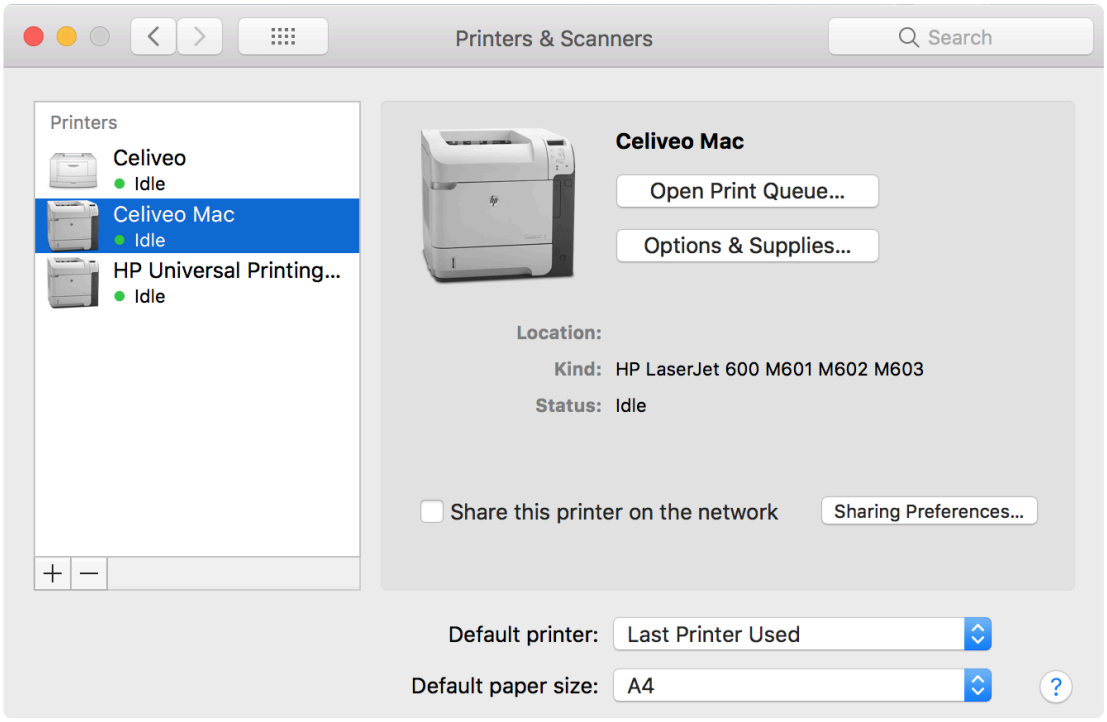
2. Click **Use** and choose **Select Software**.
3. Choose the desired printer driver, and click **OK**.
4. Then, click **Add**.



5. Check the Duplex Unit and any Trays if one or more printers have additional trays.
6. Click **OK**.

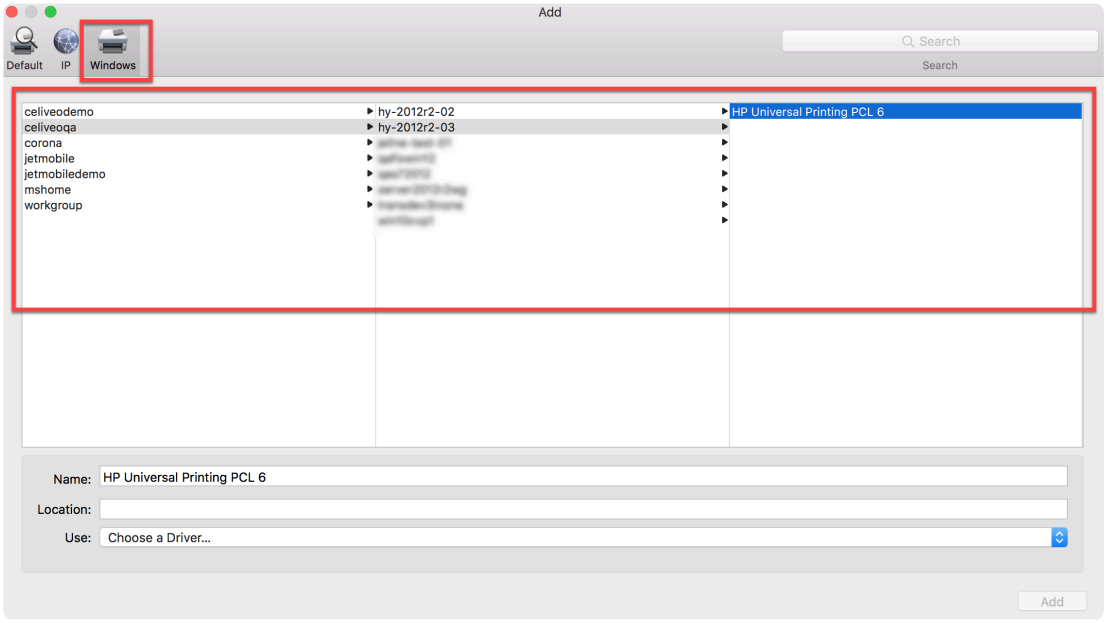


The Celiveo print queue is now added.

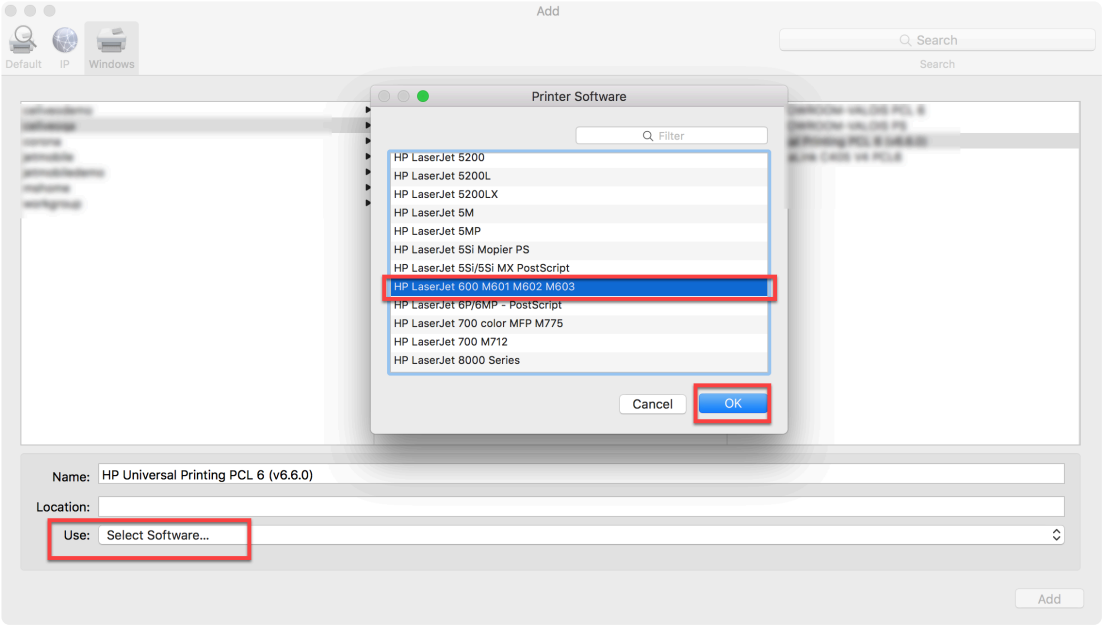


Using Windows tab:

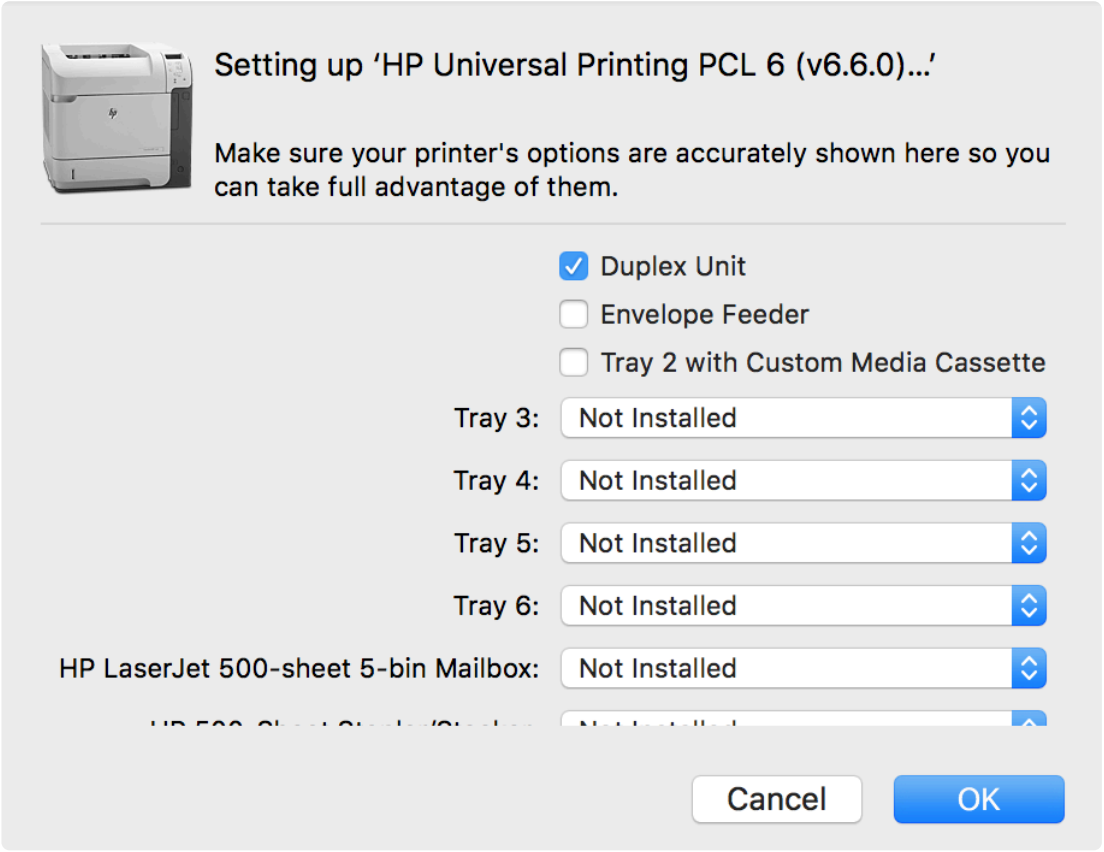
1. Select **Windows** tab.



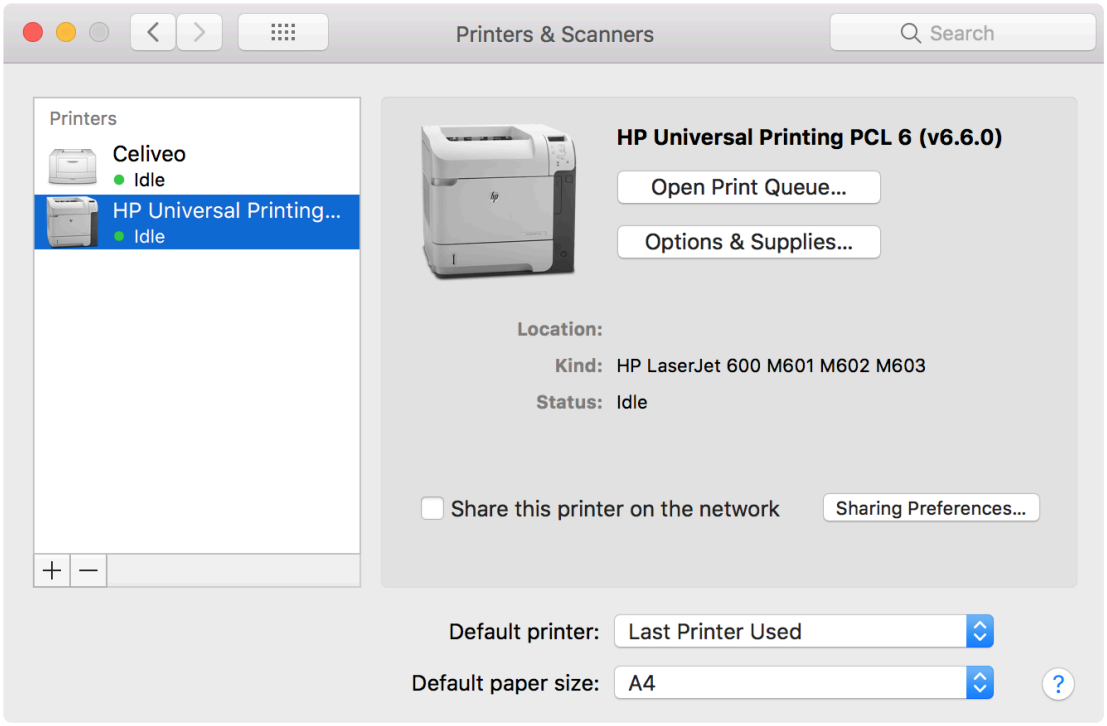
2. Select the **Domain name > Print Server name > Celiveo Shared Virtual Printer** as shown in the screen above.
3. Click **Use** and choose **Select Software**.
4. Select the desired Printer Driver and click **OK**.



5. Then, click **Add**.
6. Check Duplex Unit and any Trays if one or more printers have additional trays.
7. Click **OK**.



The Celiveo pull print queue is now added.

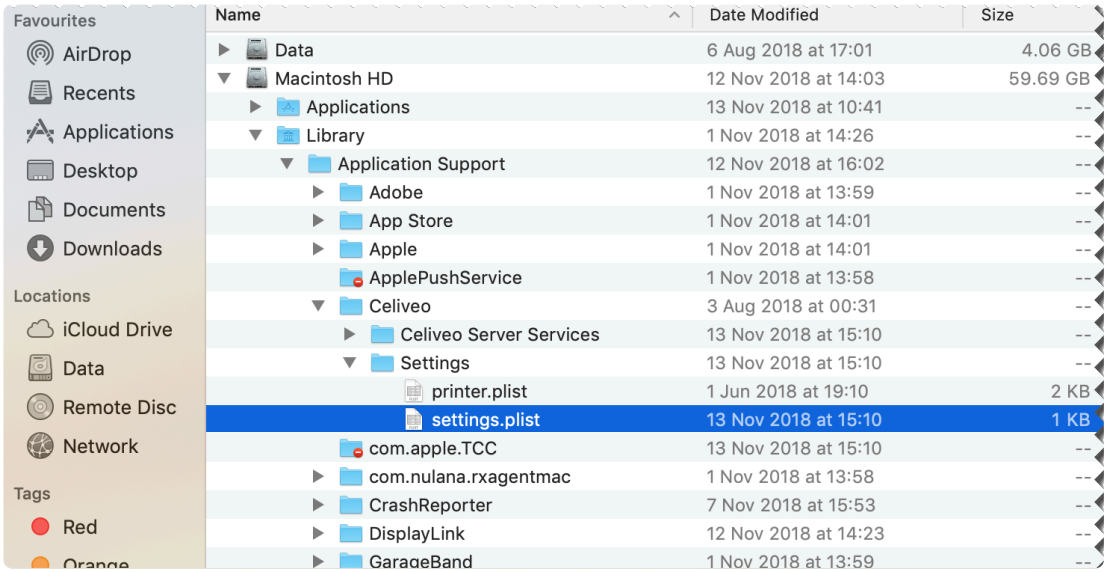


Last modified: 29 September 2022

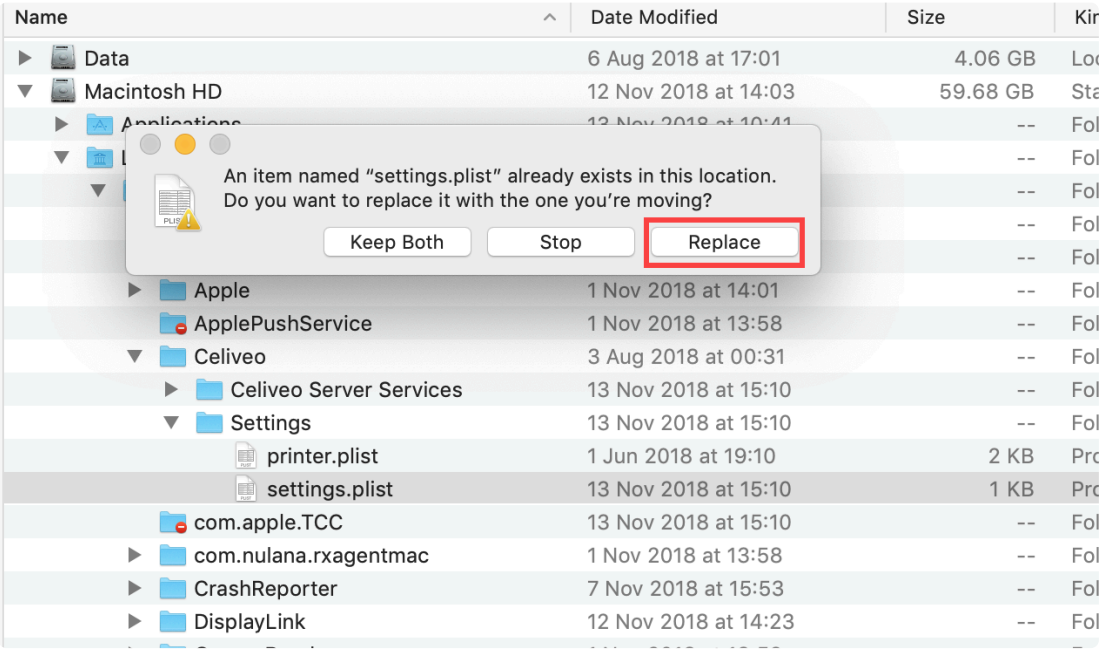
8.5.4. Upgrade Celiveo Secure Services for macOS

On the macOS machine:

1. Make a backup of the *settings.plist* file located in **Library/Application Support/Celiveo/settings/**.



2. Uninstall the existing CSS version using either the interactive or silent uninstall method.
3. Copy the *settings.plist* previously saved into the new macOS CSS install package, then run the install process following the interactive or silent procedure.

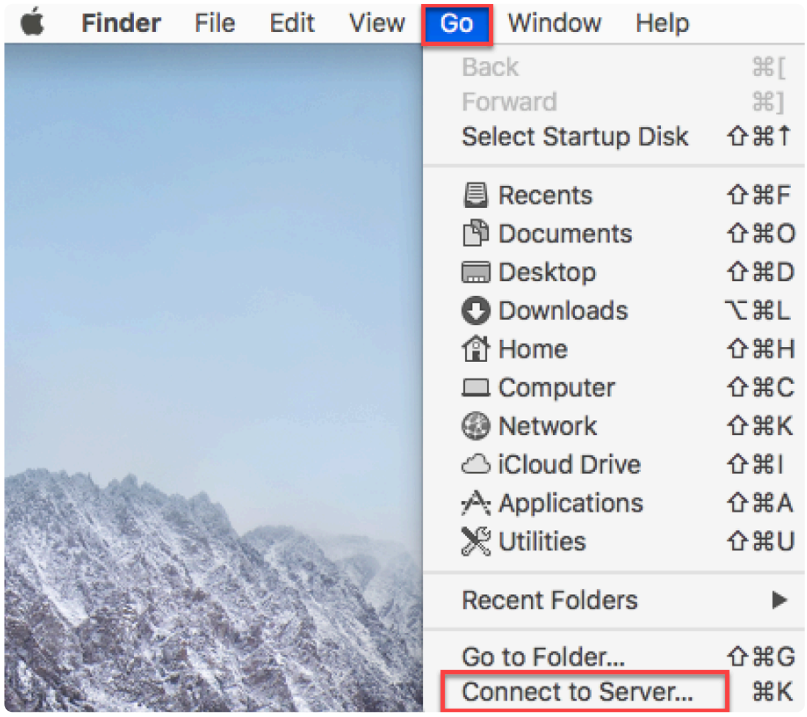


Last modified: 29 September 2022

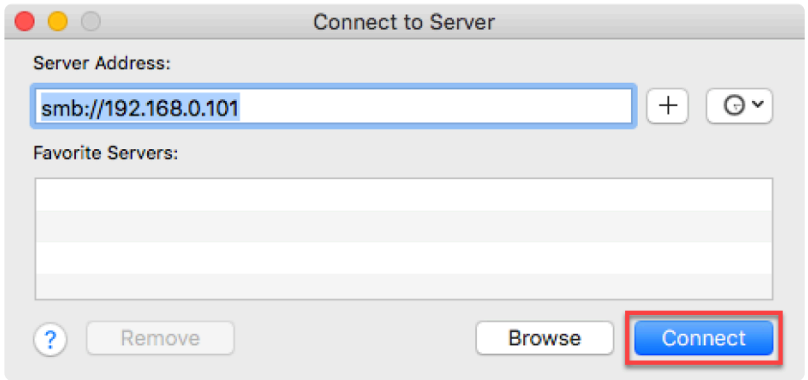
8.5.5. Configure Celiveo macOS NAS Job Transfer with Job Delegation

Configure the Windows NAS location on your Mac client workstation.

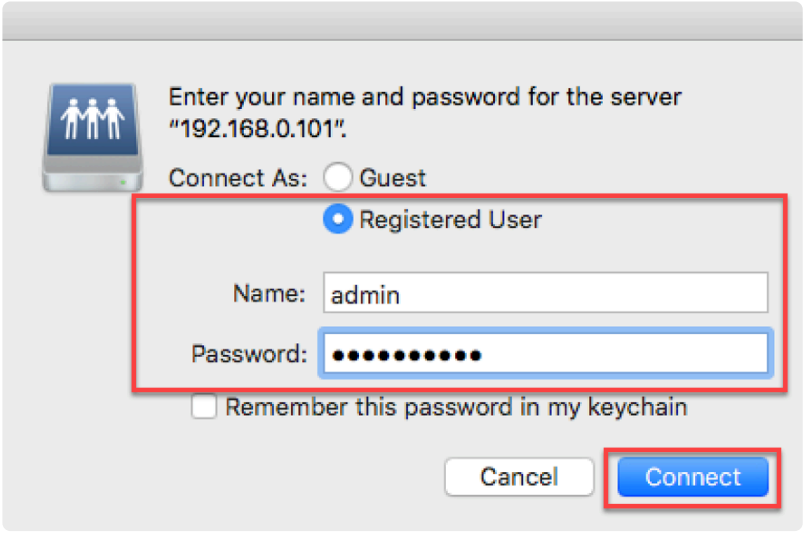
In the Finder, click the **Go** option and select **Connect to server**.



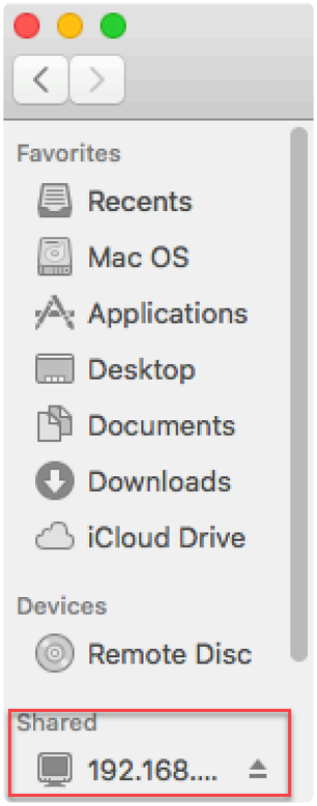
Provide the Windows NAS address and click the **Connect** button.



Provide the credentials to connect to the NAS location and click the **Connect** button.



The NAS folder is now available in your location list.



You can locate the actual location using the following command prompt:

```
Admins-MacBook-Pro:Jobs admin$ pwd
/Volumes/Users/Administrator/Desktop/Jobs
Admins-MacBook-Pro:Jobs admin$
```

Please note that the connection to the NAS location is lost every time the computer is restarted. To avoid having to reconnect it manually, follow one of the procedures below:

Method 1*

1. Open **System Preferences** and click on **Users & Groups**.
2. Select your user name from the list and then click the **Login Items** tab.

3. Drag & drop a mounted network drive into the login items list.
4. *Optional*: check the **Hide** box to keep the drives window from opening on each login and boot. This can be used to automatically connect to and mount drives to share files with a Windows PC, though it is necessary to enable SAMBA beforehand within **File Sharing** preferences.

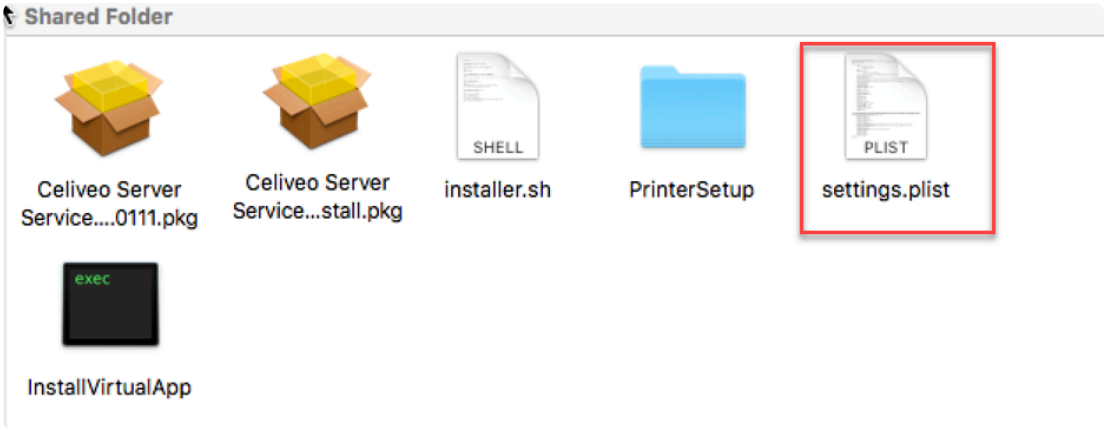
Method 2*

1. Launch Automator in OS X and create a new **Application**.
2. Drag **Get Specified Server** into the workflow, click **Add** and place the network drive network location address into the field.
3. Drag **Connect to Server** into the workflow.
4. Click on **Run** then log in to the network drive as usual to verify that it works, choosing to save the login credentials.
5. Save the Automator application.

*Source: http://osxdaily.com/2012/05/04/automatically-connect-to-network-drive-mac-os-x/

Configure the NAS location and Default user in the Mac package before installation

In the Mac package, open the settings.plist file.



Update the string corresponding to the NAS location as indicated on the picture below.

```
        <key>ProcessDLL_FileName</key>
        <string>/Library/Application Support/Celiveo/Celiveo Server Services/Logs/
_jobProcess.log</string>
        <key>NASLocation</key>
        <string>/Volumes/Users/Administrator/desktop/jobs</string>
        <key>DbDatabase</key>
        <string>SJPS</string>
```

You can also define the predefined Active Directory user in the settings.plist file.

```
        <key>ADuser</key>
        <string></string>
        <key>DelegateTo</key>
        <string></string>
```

***Note**: database details also have to be updated in the settings.plist file.*

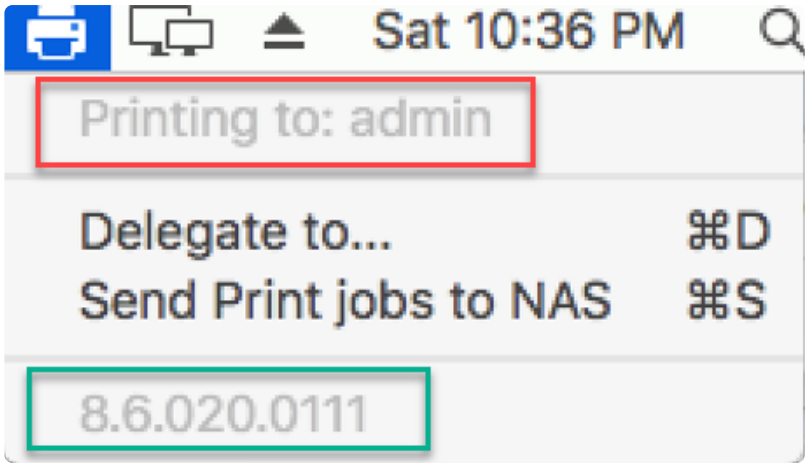
Install the Mac Package

Install the package using the command line as shown below.

```
Admins-MacBook-Pro:installer admin$ ./installer.sh i
Password:
installer: Package name is Celiveo Server Services
installer: Installing at base path /
installer: The install was successful.
driver ppd file path  = /System/Library/Frameworks/ApplicationServices.framework
/Versions/A/Frameworks/PrintCore.framework/Versions/A/Resources/Generic.ppd and
Queue name = Celiveo
Admins-MacBook-Pro:installer admin$
```

For more information on the installation process, please refer to this article.

After installation, the application UI is available in the Mac tray:

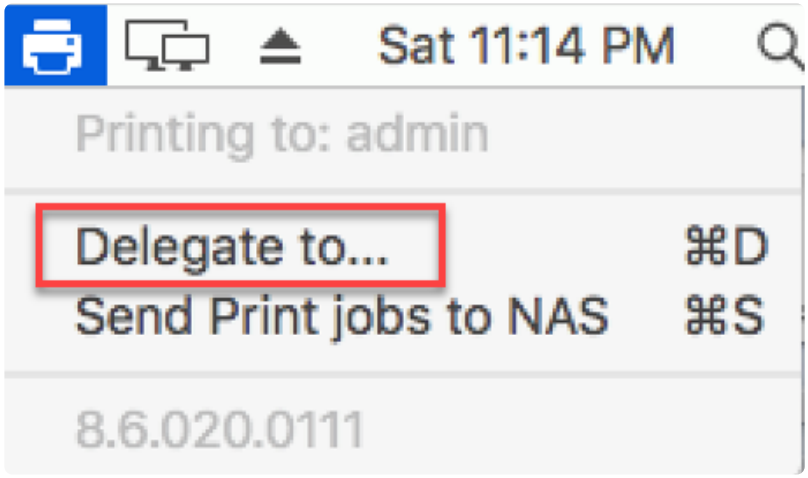


The section highlighted in red displays the Celiveo Pull Print User Name and the one highlighted in green indicates the version of the CVP.

User Delegation

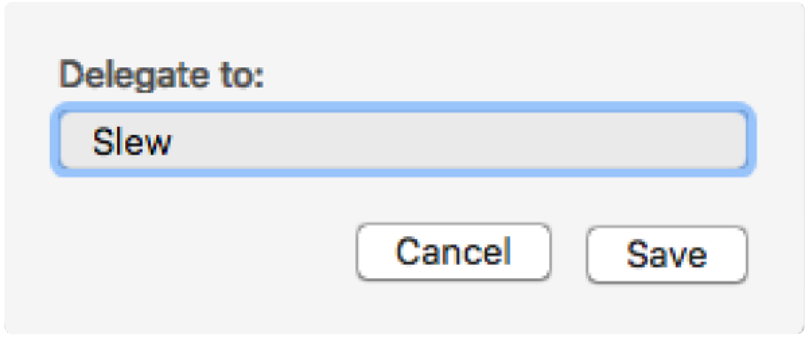
By default, Pull Print jobs are generated for the logged-in user and they are stored under the CSS jobs directory. However, it is possible to delegate jobs to another user.

Click on **Delegate to** choose the user to delegate to.

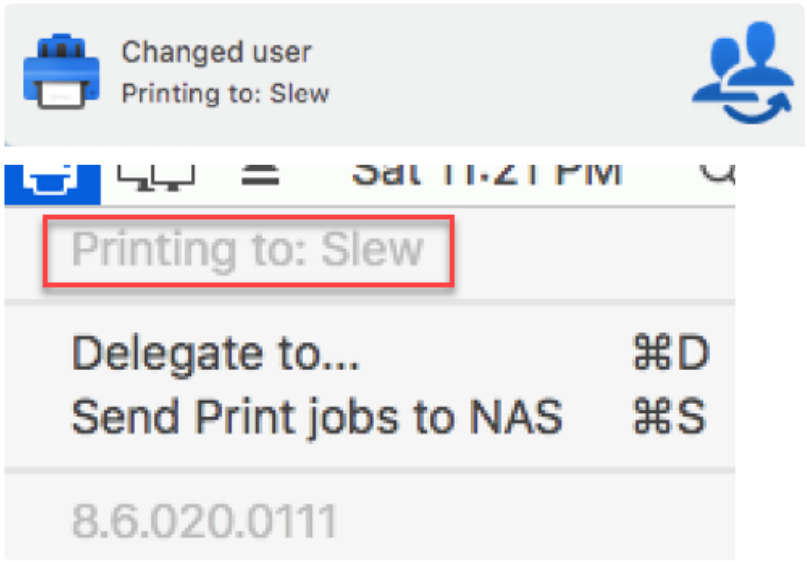


Enter the user you wish to delegate to and click **Save**.

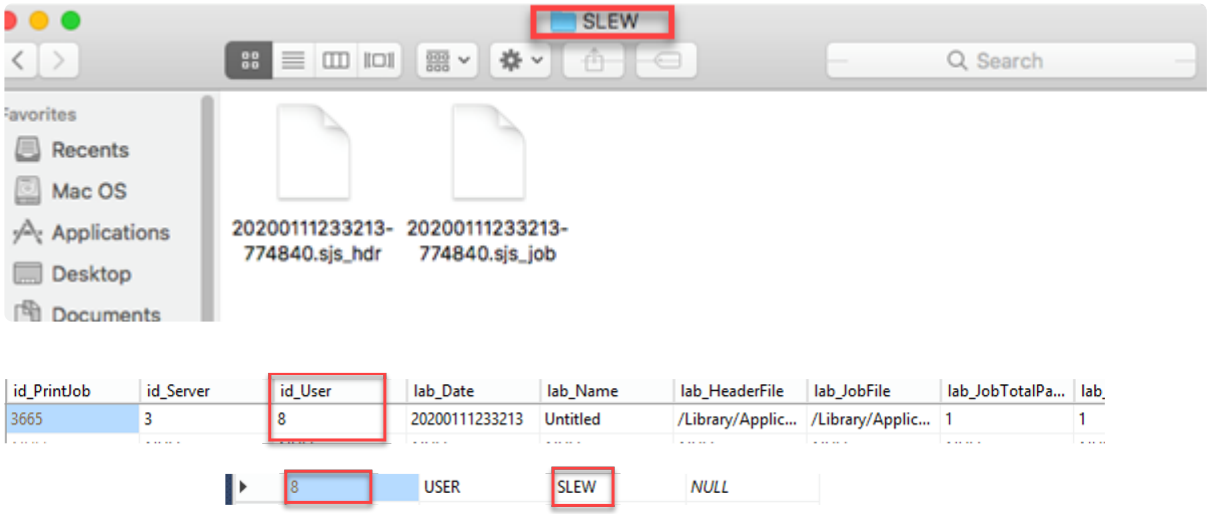
Note: Only the following special characters are allowed in the **Delegate to** field: ~ ` ! # $ % ^ & ( ) – _ { } ‘ .



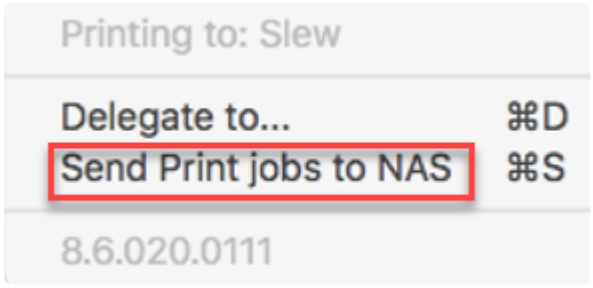
A notification is displayed and the status of the virtual printer in the tray is updated:



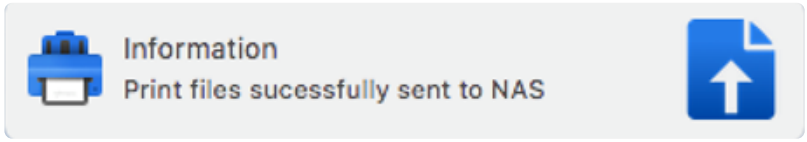
Pull Print jobs are now released for the delegated user. Jobs will be stored in the delegated user folder after print and appear in the database under the delegated user ID.



Pull Print can now be transferred to the configured NAS location by selecting the **Send Print job to NAS** option which is now available.



A notification indicates the job transfer to NAS has been successful.



Users are able to print after the jobs have been transferred to NAS even if the client workstation is powered off.

Last modified: 29 September 2022

8.5.6. Configuring the Kerberos SSO Extension

This is useful to people who use other session opening systems than Active Directory in Microsoft. It allows retrieving the user name from different attributes.

To retrieve the user name from UPN

```
Last login: Mon May  9 17:29:47 on ttys000
a256532@MacBook-Pro-di-a256532 ~ % app-sso -i ENELINT.GLOBAL -j
{
  "upn" : "a256532@ENELINT.GLOBAL",
  "networkAvailable" : "1",
  "gss_cred_uuid" : "03461CC4-D6AB-42CE-A541-C23100557789",
  "site_code" : "AWS-EUS1",
  "local_password_changed_date" : "2021-11-15T16:12:37Z",
  "home_directory" : "",
  "login_date" : "2022-05-09T15:03:09Z",
  "delayUserSetupCleared" : "1",
  "user_name" : "luca.arena@enel.com",
  "realm" : "ENELINT.GLOBAL",
  "password_expires_date" : "2022-07-11T07:33:19Z",
  "password_changed_date" : "2022-04-12T07:33:19Z"
}
```

Add the information below to the settings.plist:

```
    <key>Service_Level</key>
    <integer>127</integer>
    <key>ConnectionRetries</key>
    <integer>1</integer>
    <key>Service_FileName</key>
    <string>/Library/Application Support/Celiveo/Celiveo Server Services/Logs/_service.log</string>
    <key>ProcessDLL_FileName</key>
    <string>/Library/Application Support/Celiveo/Celiveo Server Services/Logs/_jobProcess.log</string>
    <key>NASLocation</key>
    <string>/Volumes/Users/Administrator/desktop/jobs</string>
    <key>DbDatabase</key>
    <string>SJPS</string>
    <key>ADuser</key>
    <string></string>
    <key>DelegateTo</key>
    <string></string>
    <key>appSSOUPN</key>
    <integer>1</integer>
    <key>extractUserName</key>
    <integer>1</integer>
</dict>
</plist>
```

To retrieve the user name from user_name:

```
a256532@MacBook-Pro-di-a256532 ~ % app-sso -i ENELINT.GLOBAL -j
{
  "upn" : "a256532@ENELINT.GLOBAL",
  "networkAvailable" : "1",
  "gss_cred_uuid" : "03461CC4-D6AB-42CE-A541-C23100557789",
  "site_code" : "AWS-EUS1",
  "local_password_changed_date" : "2021-11-15T16:12:37Z",
  "home_directory" : "",
  "login_date" : "2022-05-09T15:03:09Z",
  "delayUserSetupCleared" : "1",
  "user_name" : "luca.arena@enel.com",
  "realm" : "ENELINT.GLOBAL",
  "password_expires_date" : "2022-07-11T07:33:19Z",
  "password_changed_date" : "2022-04-12T07:33:19Z"
}
```

Add the information below to the settings.plist:

```
    <key>DbDatabase</key>
    <string>SJPS</string>
    <key>ADuser</key>
    <string></string>
    <key>DelegateTo</key>
    <string></string>
    <key>appSSOUserName</key>
    <integer>1</integer>
    <key>extractUserName</key>
    <integer>1</integer>
</dict>
</plist>
```

Last modified: 29 September 2022

8.6. Multi-SQL Configuration

What is Multi-SQL configuration?

When being part of a large company with its offices distributed across the globe, and you have to travel from one site office to another, the need arises to switch to the appropriate regional database settings to connect and store print jobs locally. The Multi-SQL feature allows you to automatically change the database connection settings in a Serverless Pull Printing client configuration (CVP), to a region-specific database when you travel from one region to another.

The switch to the applicable SQL database is based on the tag combinations and priority value.

Celiveo is able to map together printers, database profiles, and IP Address ranges used in each geography so that they will belong to the same community. It is also able to map users to a community based on AD/LDAP attributes such as Name, Organizational Unit (OU), and Group. Thus, when a user attempts to print using Print Direct/ Pull Print, the tags filter the available printer list to display only those printers that are within the community.

> **NOTE**: A community is a group of users, workstations, printers, and administrators that have a common characteristic. For example, a group of users, workstations, printers, and administrators, located in the same building. The community that a user or device belongs to is determined by the tags assigned to them. Learn more about Tags/ Communities here.

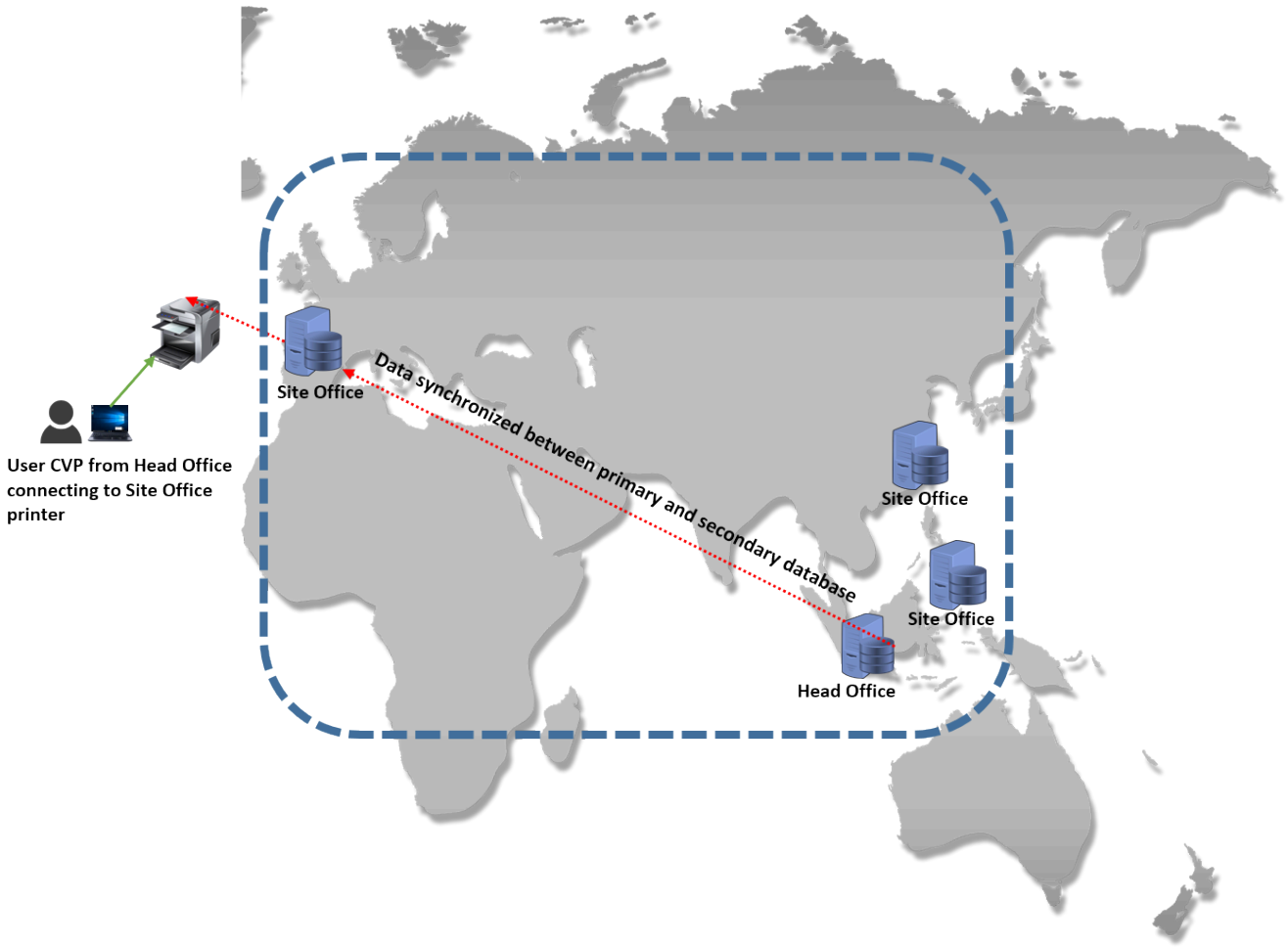
When a user plugs into the network from within a specified community, the user is assigned an IP Address tied to that community.

Now, if the user is a member of a Group/OU, the community setting (tag combination) of the Group or OU or IP Address range with the highest priority value is assigned to the user. Those tag combinations will then be used to search and connect to the SQL server database with the same tag combinations. All communications of the user will then be performed through this database.

Example:

- A large company Azone.Inc has its headquarters in Singapore and regional offices distributed in Malaysia, Hong Kong, and Spain.
- The company uses tags to identify places. Each regional office is organized into a community on the basis of five tags set (Country, State, City, Building, Floor). The printers, database servers, and IP Address ranges are tagged so that the printers and IP Addresses used in geography will belong to the same community.
- Azone employee Simon Phil, who belongs to Singapore Office, travels to Spain Office for a meeting. Now Simon needs to print some important documents before the meeting. Simon uses Celiveo Virtual Printer for Serverless Pull printing in his laptop. He connects his laptop to the Spain Office network.
- Normally, Simon has to switch regions and sub-regions in his CVP application to connect to a region-specific database. With the Multi-SQL feature, the database connection settings will be automatically updated during CVP application boot up.

- The tag settings for the IP Address Range in Spain Office is defined as (Spain, Madrid,,,*) with priority value: 75.
- Now, Simon is also a member of OU=SingaporeUnit (with tag combinations: Singapore, ,,, and priority value: 50) and Group=Managers (with tag combinations: Singapore,*, Orchard, Tower One, 5 and priority value: 20)
- The tag combinations with the highest priority value takes effect. In this case, the tag combination of IP Address Range in Spain Office is chosen for connecting to the SQL Server database.
- The CVP notes these tag combinations and then proceeds to connect to the SQL server database with the same tag combinations.
- The CVP on Simon's laptop will now search for SQL server profiles among the various other profiles for the same tag combination. Once it is successfully connected to the correct Database server profile, all Simon's pending print jobs, even those that were stored in Singapore (primary) database will be moved to the now connected SQL server in Spain.
- Simon also receives a notification of this database change on his laptop.
- Simon can now proceed to submit the print jobs to the already existing Pull print queue configured in his CVP and then release the print jobs at the printer.
- In the case of Print Direct, the CVP searches for the printer to connect in the Spain Office. Because this IP address is tied to the Spain Community, CVP filters the list of printers to show only the Spain printers. Simon can also use a floor map to choose the printer (Choose another printer).



To summarize:

When a user CVP moves its connection from SQL server A to SQL server B due to tag combination:

- The CVP synchronizes with the new SQL server profile.
- It moves all pending print jobs of the user from Server A to server B.
- A popup notification is displayed to the user informing of the database change.
- All communications from user CVP are now done through SQL server B.
- Tracking information of print jobs are however stored on Server A (primary server)

How tag settings work

What if I am a Member of Several Groups/OUs?

If you are a member of more than one Group/OU, and each Group/OU is mapped to a different community (tag assignments), the community setting of the Group or OU with the highest priority value is assigned to you. The same principle applies if your user name is assigned to a community and you inherit a community from the groups you belong to. It is the community with the highest priority that is assigned to you. To know more about priority settings, click here.

What if a matching tag combination is missing for the SQL server profile?

If a SQL server profile does not exist with the same tag combinations, the CVP will connect to the primary SQL server profile.

Tracking information on Primary SQL Server

Print tracking information is always stored in the primary database, irrespective of its location of printing (for example, secondary server sites). This is due to the fact that print quota settings are configured on the primary database and cannot be mirrored across SQL databases.

Creating a Secondary database in Web Admin

A Super Admin can create a primary SQL server profile and define up to five additional secondary SQL server profiles in the Web Admin application.

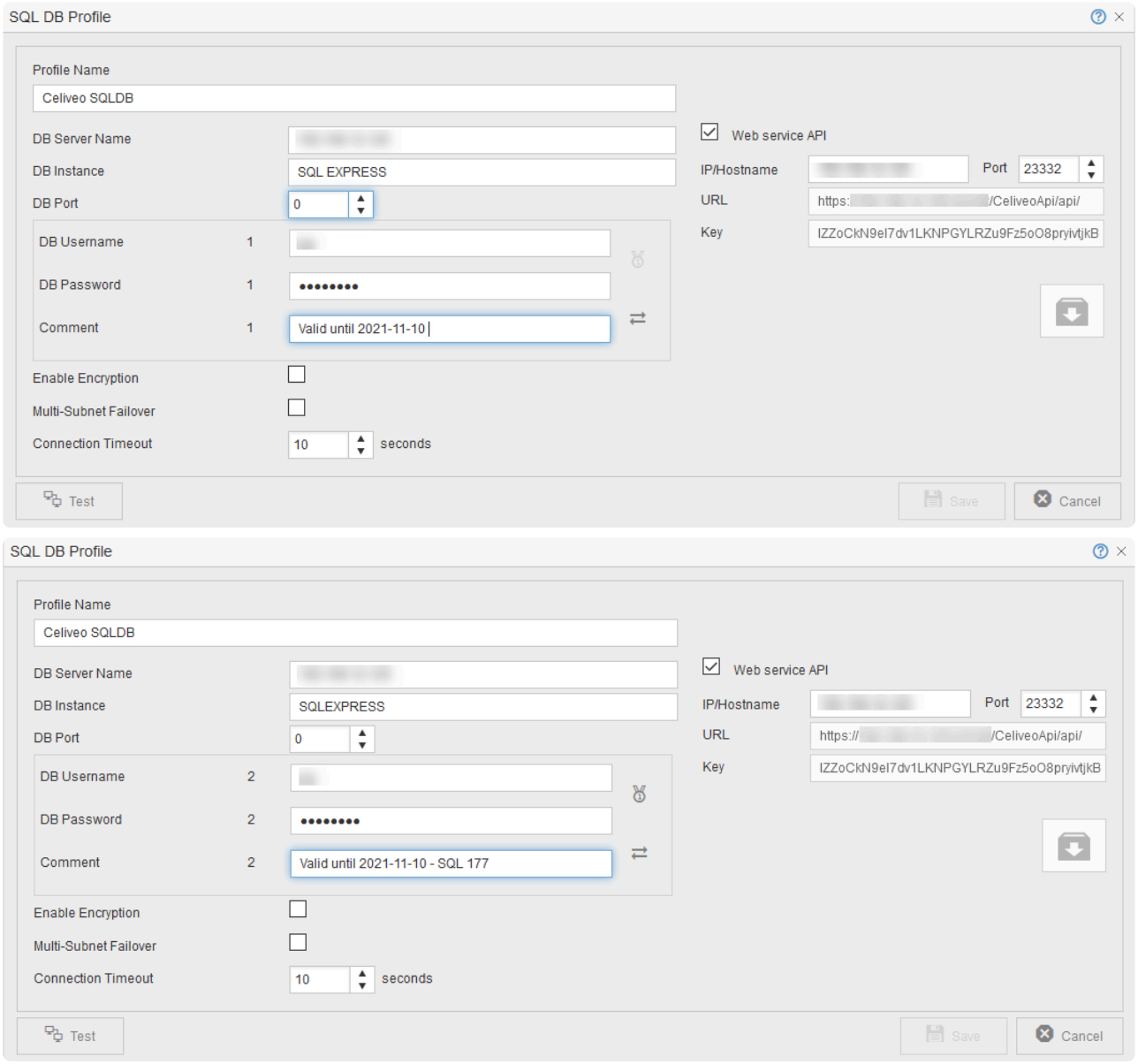
> **Important note:** The printers, SQL server profiles, User Groups/ OUs, and IP Address ranges are identified with nickname and tags combination. While connecting, if there is no matching tag combination found, the user CVP will connect to the primary SQL server profile. So it is important that tags and priority values are properly configured, for the CVP to automatically determine the Regional SQL Database to which print jobs have to be sent.

How to create secondary SQL server profiles in Web Admin?

> **Note**: Before adding a secondary database, make sure that your database is enabled

and working.

1. In the Web Admin, click icon Setup icon at the top right hand corner of the screen.
2. Select the Database Configuration tab.
3. Click the **Add** icon.



4. Enter the following information for creating secondary DB profile:

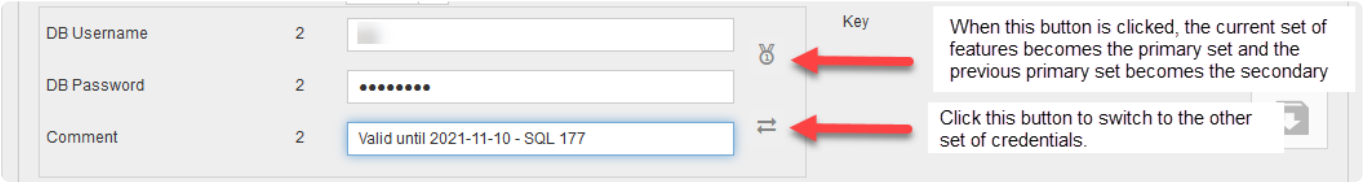
Field	Description
Profile Name	Name of the secondary database profile.
DB Server Name	For the default instance of SQL Server, the server name is the [computer name] or [IP address].E.g. CELIVEO SRVR, 192.68.3.211 For a named instance of SQL Server, the server name is the [computer name] or [IP address]\[instance name].E.g: CELIVEO SRVR\SQLEXPRESS, 192.68.3.211\SQLEXPRESS.

DB Instance	If the default instance of SQL Server is used, leave this field empty. If a named instance of SQL Server is used, provide the instance name. If SQL Server is installed using the Celiveo installer, the instance name is “SQLExpress”.
DB Port	By default, the SQL Server listens on TCP port number 1433. Select the port number configured for this database instance.
DB Username	Type the user name with admin access privileges for this database.
DB Password	Type the corresponding password.
Enable Encryption	Select this option to secure the connection between the Web Admin application and the specified SQL server. This encrypts all the communication occurring between them.
Multi-Subnet Failover	MultiSubnetFailover is a Microsoft configuration introduced in an update for Microsoft SQL Server 2012 and later versions to support the AlwaysOn features. When MultiSubnetFailover is enabled, Web Admin attempts parallel connections to the failover IP addresses of an (Always On) Availability Group during a multi-subnet failover. A multi-subnet failover cluster provides a disaster recovery solution in addition to high availability. For further reference about MultiSubnetFailover, please refer to the following Microsoft articles: • **Microsoft SQL Always On availability groups: a high-availability and disaster-recovery solution** https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server?view=sql-server-ver15 • **Overview of Always On Availability Groups (SQL Server)** https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server?view=sql-server-ver15 • **SQL Server Multi-Subnet Clustering (SQL Server)** https://docs.microsoft.com/en-us/sql/sql-server/failover-clusters/windows/sql-server-multi-subnet-clustering-sql-server?view=sql-server-ver15
Connection Timeout	This denotes the time limit (in seconds), within which the connection to the specified SQL server must be made before terminating the attempt.

> ! It is necessary to set **EITHER** a DB instance **OR** a port for the synchronization to be successful.

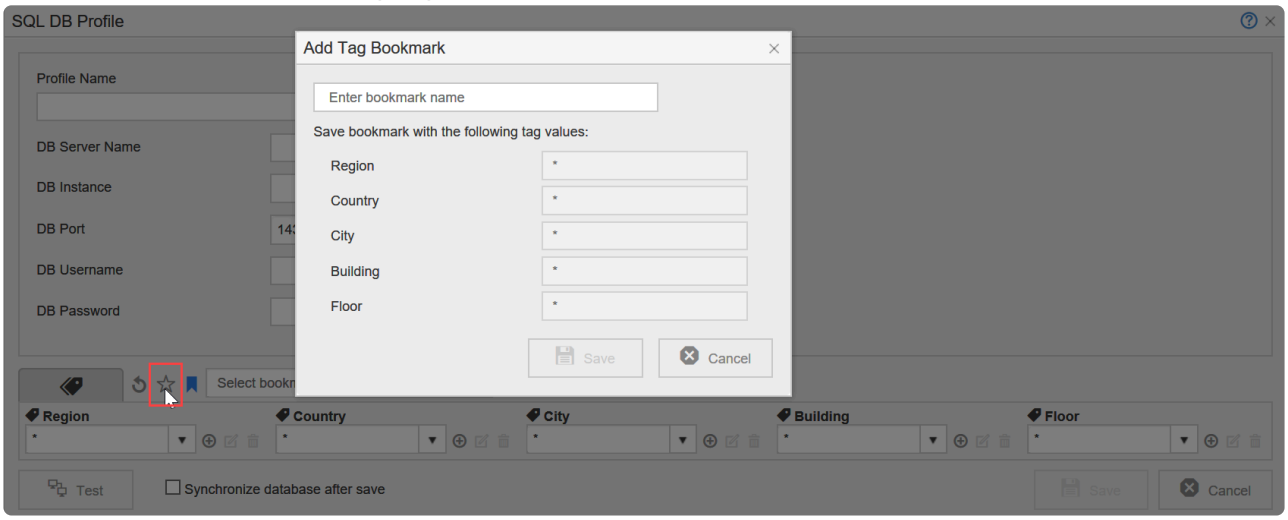
Dual Service Account System

To avoid any connection error after refreshing/changing the login/password on service accounts used by Celiveo, the administrator can define a secondary set of credentials so that if the default (primary) set is declined by the solution, then the secondary set takes over and prevents the access from being denied.



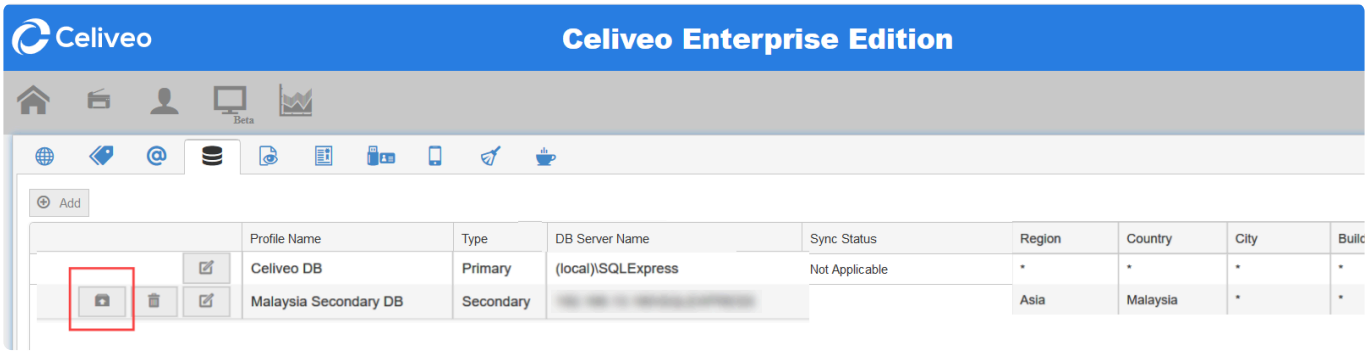
5. To use an API, enable the **Web service API** checkbox. Enter the IP/Hostname of the server on which the API will be installed. The **Key**, **Port** and **URL** fields are automatically filled. You can then download the API package and install it manually.
   You can disable the installed API by unchecking the **Web service API** box without having to uninstall the API package.
6. Define tags for your database profile:

- For each tag category, select a value in the drop-down list or click the **Add** icon next to the drop-down list. To edit a value, click the **Edit** icon. To delete a value, click the **Delete** icon.
- You can also save your tags in a bookmark to reuse it later. To do so, click the **Add Tag Bookmark** icon after entering tag values.



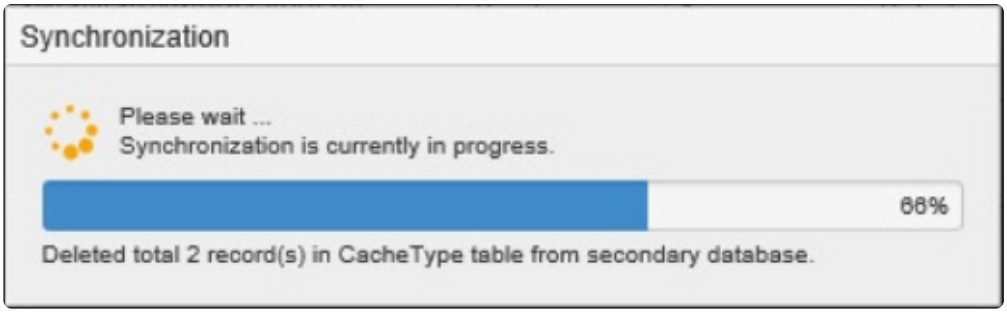
7. Click the **Test** button to perform a connection test on the database. A confirmation message displays if the connection to the database is successful. The **Save** button becomes available.
8. Select the **Synchronize database after save** checkbox to synchronize with the primary database when you click **[Save]**.
   This will synchronize and replicate the primary database as the secondary database is created.

You can also synchronize the secondary database later using the **[Sync]** icon in the **[DB Settings]**.

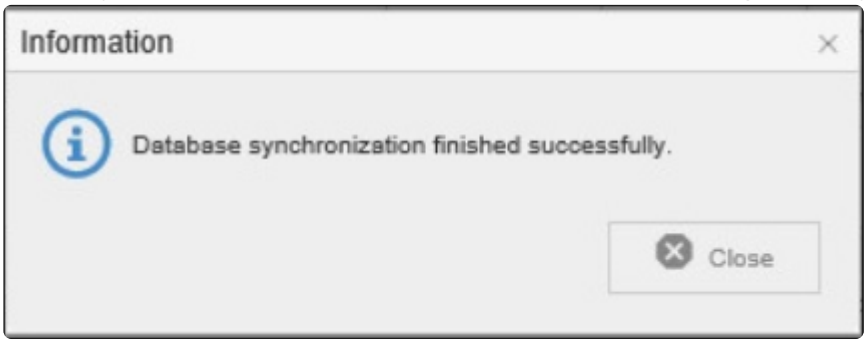


9. A confirmation message displays. Click **OK**.

10. During Synchronization, all unnecessary data is deleted from the secondary database.



11. Once Synchronization is complete, a confirmation message displays.



Last modified: 29 September 2022

8.7. Configuring SQL Database for AlwaysOn Availability feature

Contents

- What is AlwaysOn Availability Group?
- How Celiveo supports AlwaysOn availability?
- Enabling multi-subnet failover during Celiveo installation
- Enabling multi-subnet failover and other options during database configuration

What is AlwaysOn Availability Group?
Microsoft SQL Server's AlwaysOn feature was developed to as solution to support "always" availability of databases during back-end failure or any other disaster, in a corporate (multi-network) environment.
An AlwaysOn Availability Group comprises of the following components:

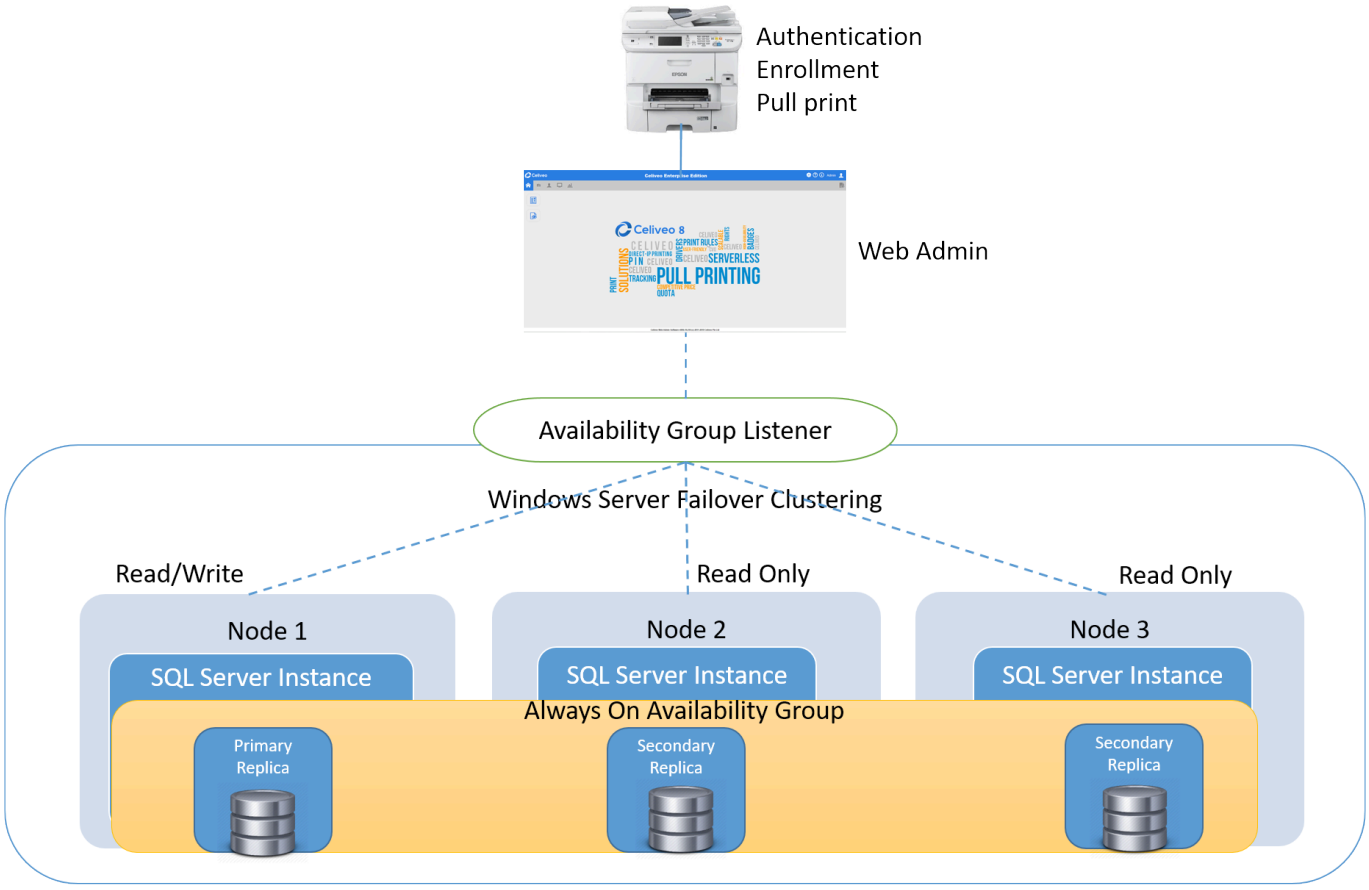
- **Availability Group** — Collection of user databases that is being protected against failover.
- **Primary replica** —This is an instance of the primary SQL Server that hosts the databases that needs to be protected. In case of Celiveo, the databases to be protected from failover are Celiveo database and Track-Green Saver databases. This node will have read and write permissions on a regular day.
- **Secondary replica(s)** —These are instances (one or more replicas) of the primary SQL Server, which host a set of replicated databases, updated consistently so as to take-over if the primary replica fails. These nodes will have only read permission on a regular day.
- **Listener** —This provides access for client applications to the primary and secondary databases in AG and enables automatic client re-connection in the event of a failover.

Methods of synchronizing database nodes

- **Asynchronous-commit mode** — In this method, updates from the primary node are sent asynchronously to the secondary nodes.
- **Synchronous-commit mode** — In this method, secondary nodes are updated consistently with the primary node. This mode of synchronization is high availability.

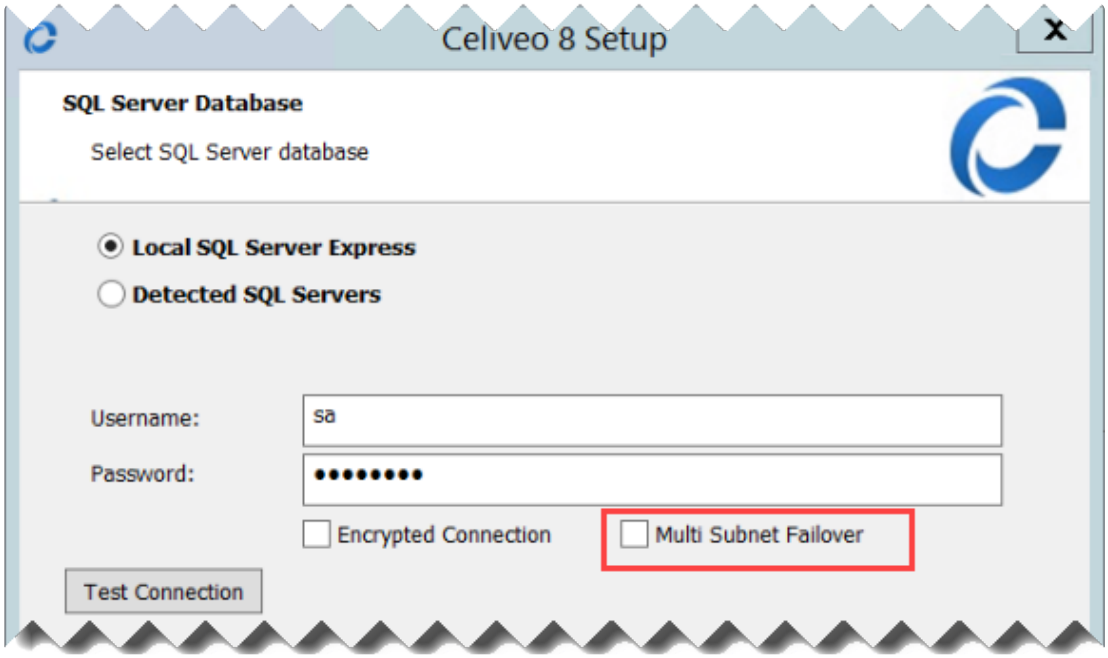
An Availability Group consists of independent SQL Server instances residing on distinct Windows Server instances (nodes) within a Windows clustering environment; working together to protect a set of user databases (primary database) known as Availability databases. These Availability databases can support up to five secondary replicas of the primary database. The primary replica having read/write privileges consistently updates the secondary replicas (with read-only access) either via synchronous or asynchronous mode.

In the event of a failure on the primary database, all of the databases within an Availability Group will fail over together and become active on the designated failover (secondary) replica. This secondary SQL Server instance will now become the primary replica with read/write privileges.



Enabling Multi-Subnet Failover option during Celiveo installation

Thanks to the Microsoft technology, Celiveo has enhanced its features to support **AlwaysOn Availability Groups** in a multi-subnet environment. If you already have an AlwaysOn Availability Group configured, then enable the **Multi-Subnet Failover** option during installation to enable the Microsoft SQL Server MultiSubnetFailover configuration:



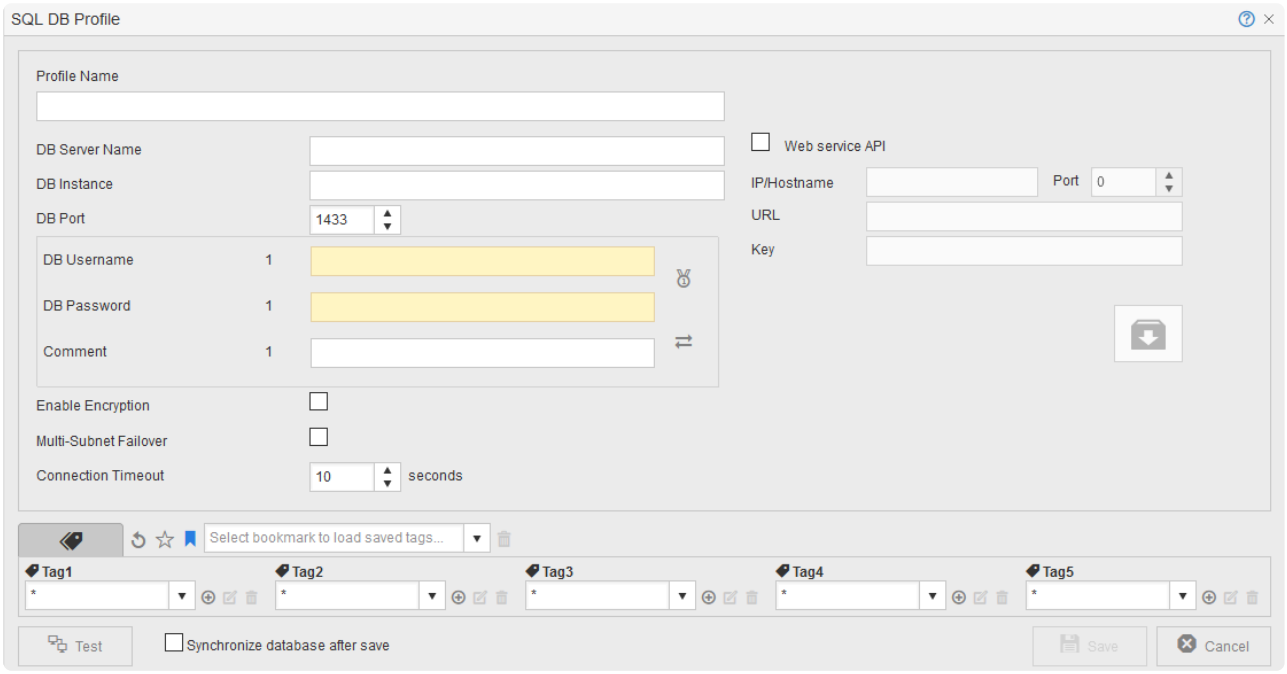
Follow the installation instructions provided here.

Enabling multi-subnet failover in a multi-SQL environment

After Celiveo installation, if you wish to create a database profile (primary or secondary) to support AlwaysOn Availability groups, follow the instructions given below:

In Web Admin:

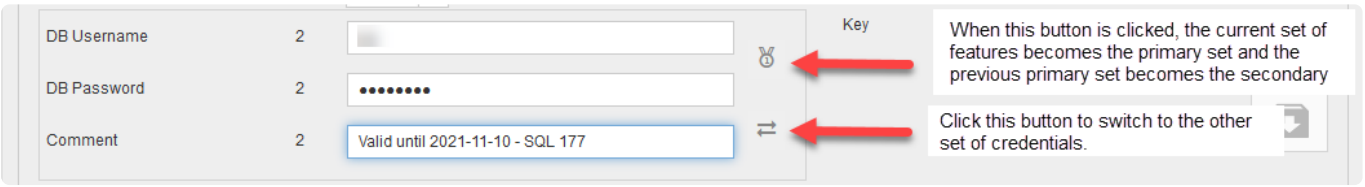
1. Click Setup icon at the top right-hand corner of the screen.
2. Select the Database Configuration tab.
3. Click the **[+Add]** button.



4. Enter the following information for creating the database profile:
   - Profile Name: This is the name of the database profile
   - DB Server Name: The server name is either the [computer name] or [IP address]. E.g. CELIVEO SRVR, 192.68.3.211
   - DB Instance: For the default instance of SQL Server, leave this field empty. For a named instance of SQL Server, provide the instance name.
     Note: If SQL Server is installed using the Celiveo installer (during installation), the instance name is “SQLExpress”.
   - DB Username: Type the user name with admin access privileges for this database.
   - DB Password: Type the corresponding password.

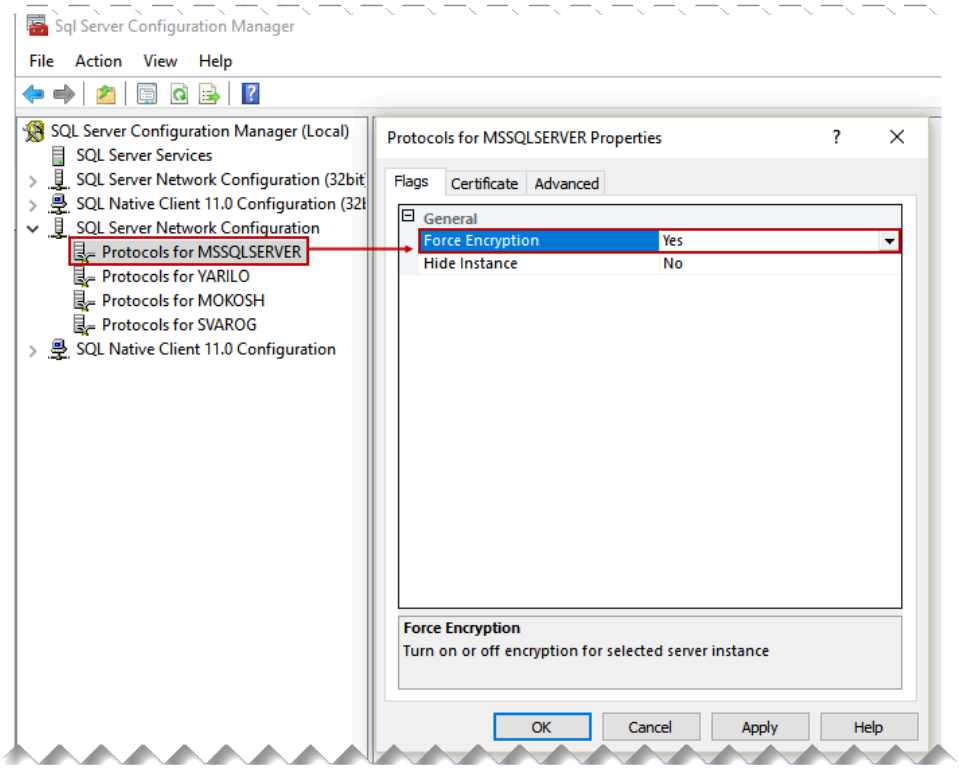
Dual Service Account System

To avoid any connection error after refreshing/changing the login/password on service accounts used by Celiveo, the administrator can define a secondary set of credentials so that if the default (primary) set is declined by the solution, then the secondary set takes over and prevents the access from being denied.



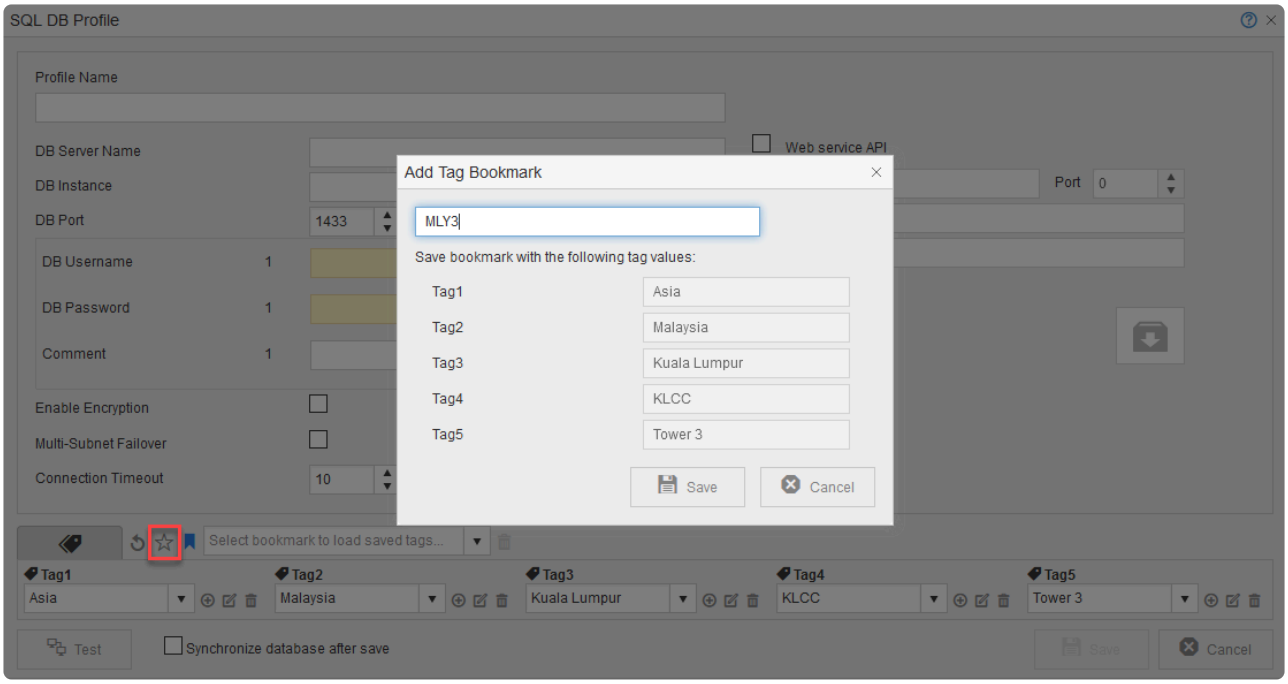
5. **Options**

- **SQL Encryption (SSL over SQL)**
  - Enable Encryption: Select this option to secure the connection between Web Admin application and the specified SQL server. This allows authorized communication to occur between them. The SSL security layer prevents unwanted sensitive data leak, and/or excludes the possibility for any SQL injection attack.
    - Make sure encryption is enabled on the Server. To do this:
      1. Open SQL Server Configuration Manager, go to SQL Server Network configuration.
      2. Choose **Protocols** properties for the SQL Server instance and enable **ForceEncryption** option in **Flags** tab.

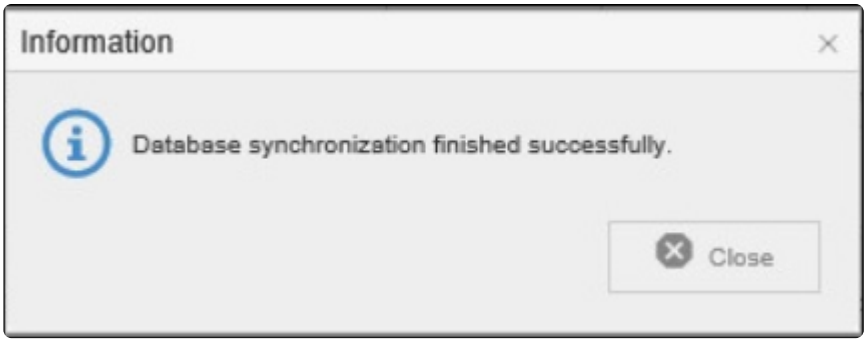


- **AlwaysOn Availability Groups**
  - Multi-Subnet Failover: When enabled, Web Admin attempts parallel connections to the failover IP addresses of an (Always On) Availability Group during a multi-subnet failover.
- **Connection Timeout**:
  - This denotes the time limit (in seconds), within which the connection to the specified SQL server must be made before terminating the attempt.

6. Define tags for your database profile:



7. Click the **Test** button to perform a test on the database.
   A confirmation message displays if the test is successful. The **Save** button becomes available.
8. Select **Synchronize database after save** checkbox to synchronize with the primary database when you click **[Save]**.
   This will synchronize and create a replica of primary database as the secondary database.
9. You can also synchronize the secondary database later using the **[Sync]** icon in the **[DB Settings]**.
10. A confirmation prompt displays. Click **OK**.
11. During Synchronization, all unnecessary data is deleted from the secondary database.
12. Once Synchronization is complete, a confirmation message displays.



Last modified: 29 September 2022

8.8. Set up Access

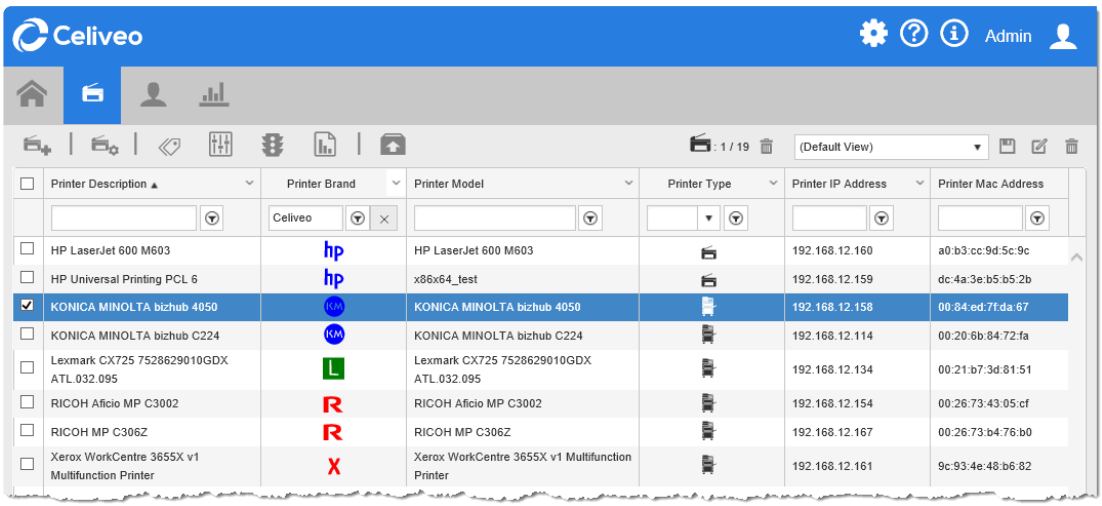
For more details about Celiveo Authentication, please read our Authentication topics.

Enable Card Authentication for Printers

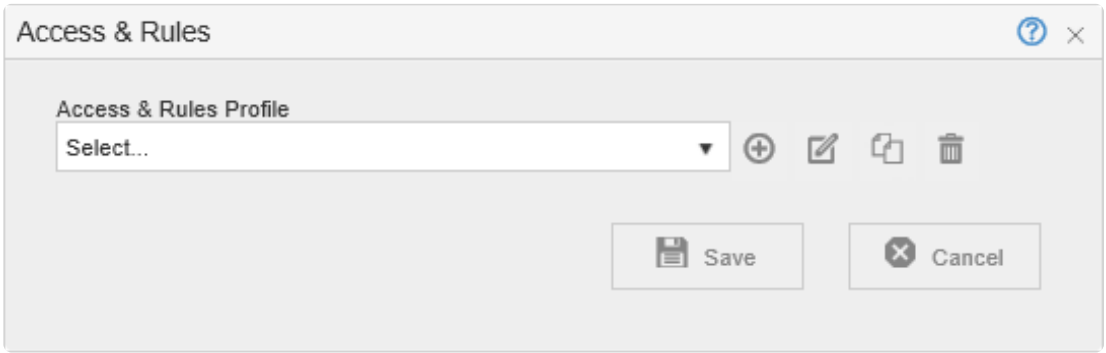
You enable proximity card authentication by creating an Access Control Rule and assigning the rule to a printer. You however cannot assign an Access Control Rule directly to a printer. Instead, you create an Access & Rules Profile for a printer and add the Access Control Rule to the Access & Rules Profile.

Combination of Card and Username/Password Authentication is not supported on HP Pro Printers.

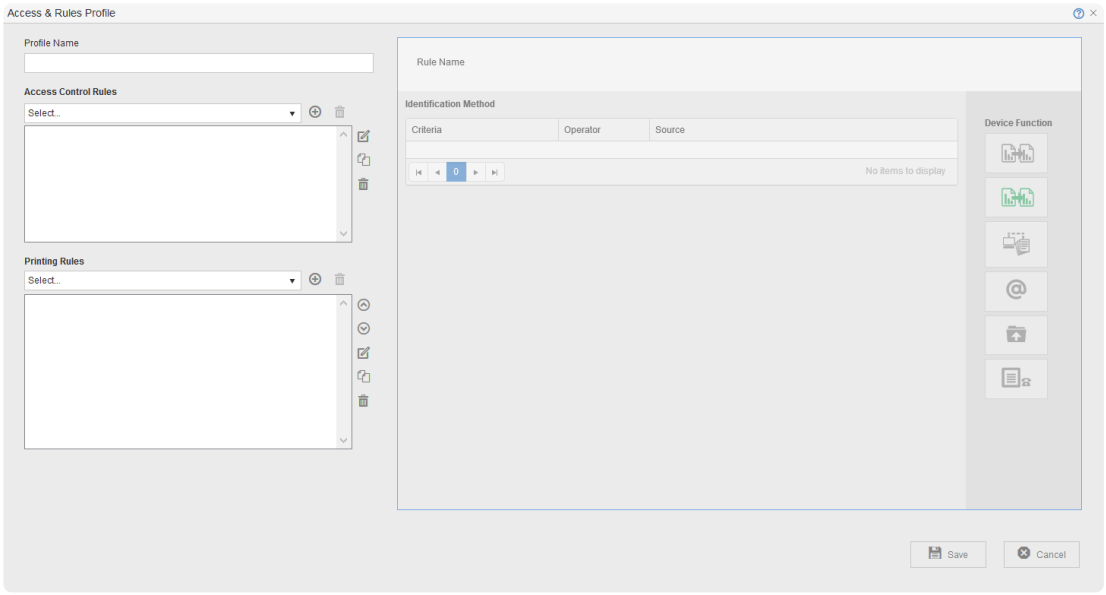
1. Add a New Access & Rules Profile to a Printer



1. Select the printer to add the Access and Rules Profile to.
2. Click . The Access & Rules dialog is displayed.



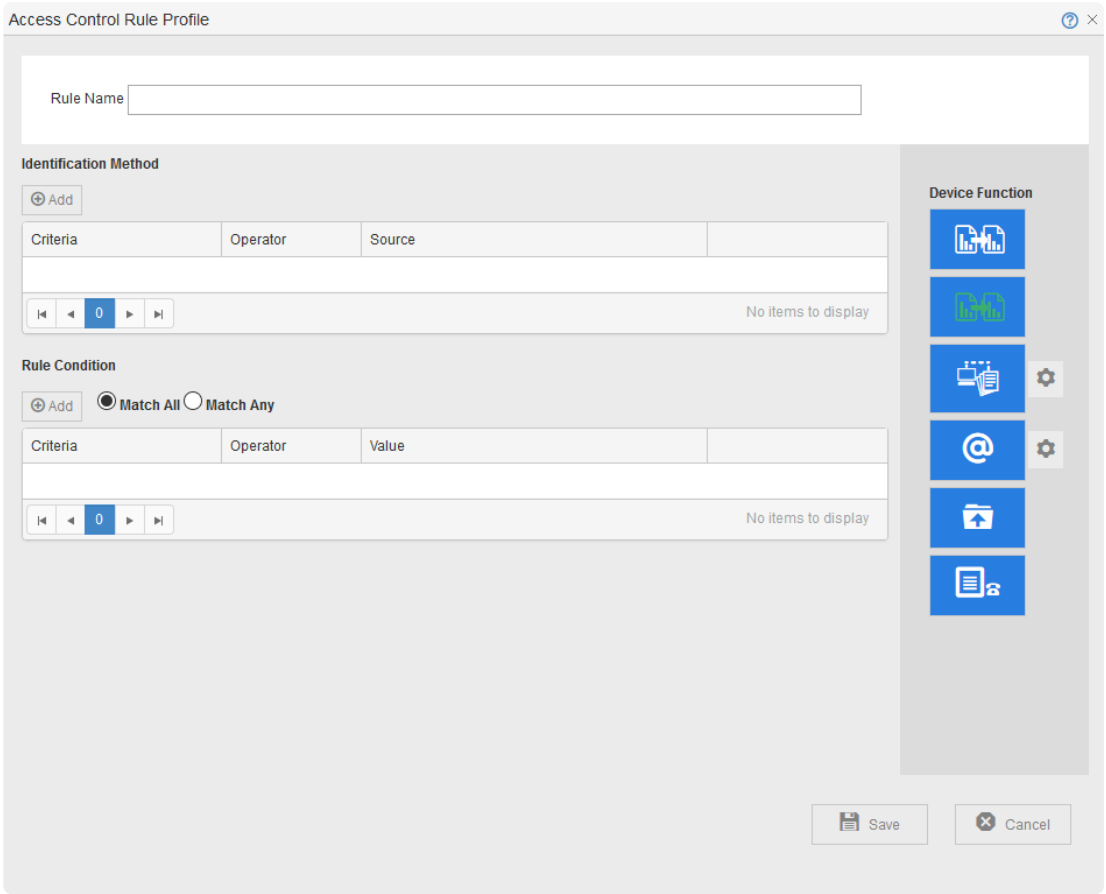
3. Click . The Access and Rules profile is displayed.



4. At **[Profile Name]**, specify a unique name for the Access & Rules Profile.

2. Add a New Access Control Rule to the Access and Rules Profile

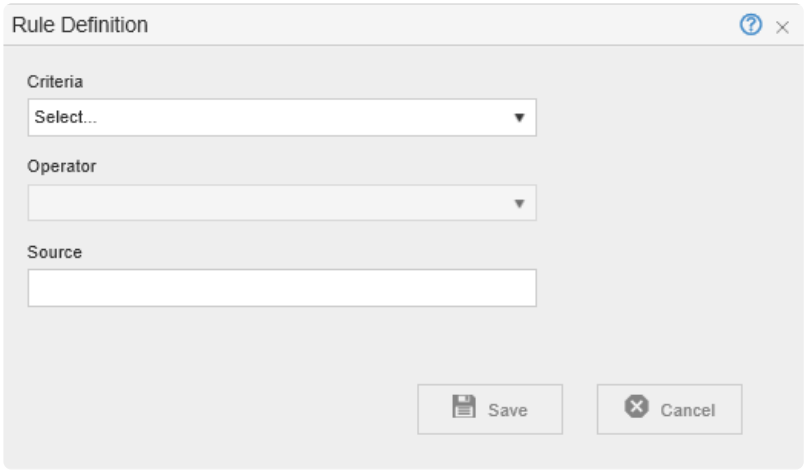
1. Click ⊕, located in the same row as the [Access Control Rules] drop-down. The Access & Rules Profile displays.



2. At **[Rule Name]**, specify a unique name for the Access Control Rule.

3. Add Card Authentication as the Identification Method

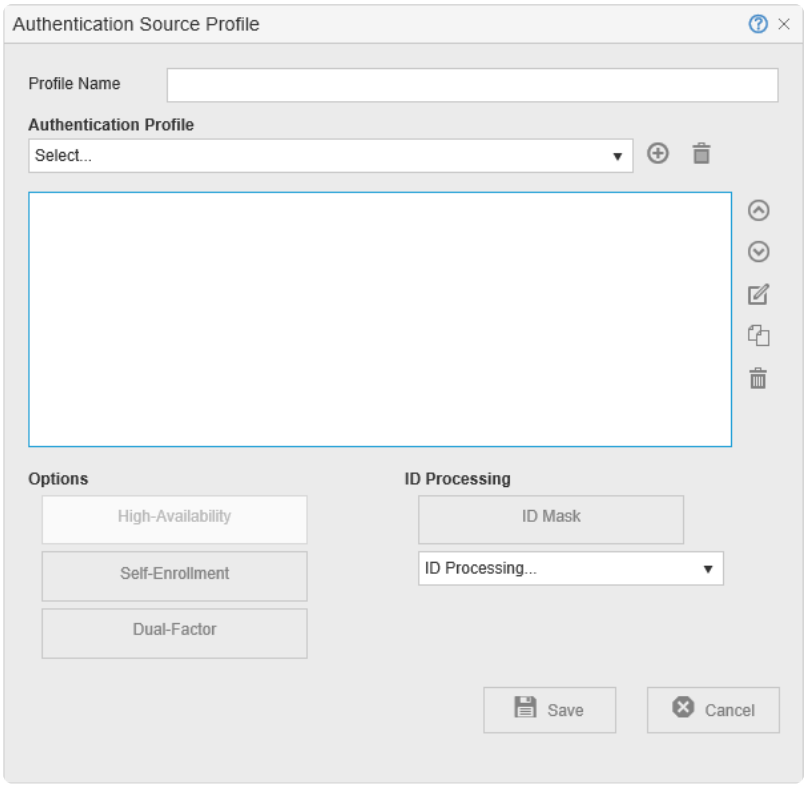
1. Click **[Add]**, located below **[Identification Method]**. The Rule Definition displays.



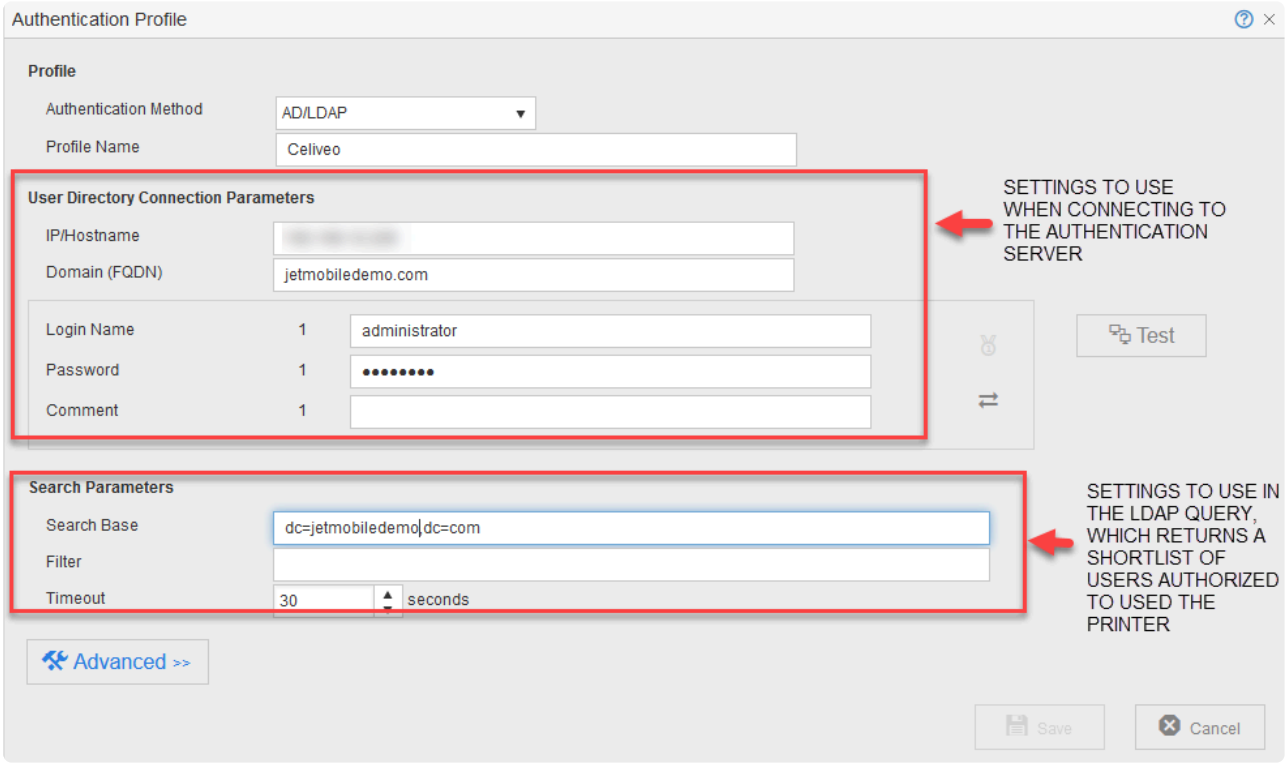
2. From the **[Criteria]** drop-down, select **[Card Number]**.
3. From the **[Operator]** drop-down, select **[Is In]**.

4. Build the Authentication Profile to Validate the Card Number

1. Click ⊕, located next to the **[Source]** drop-down. The Authentication Profile displays.



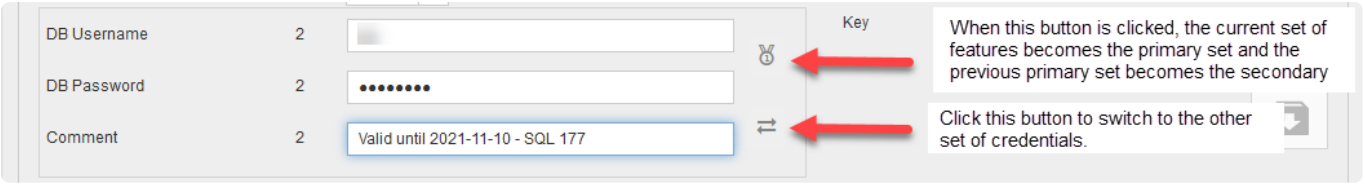
2. In the **[Profile Name]** box, specify a unique name to identify the profile.
3. Click ⊕, located in the same row as the **[Authentication Profile]** drop-down. The Authentication Profile is displayed.
4. Specify the AD/LDAP query (similar to that of the screen capture shown below) that returns the list of users who are authorized to use the printer.



5. Click **[Test]**.
   If login to the Authentication Server is successful, a message is displayed below the [Test] button.
6. Click **[Save]**. You are returned to the Authentication Source Profile.

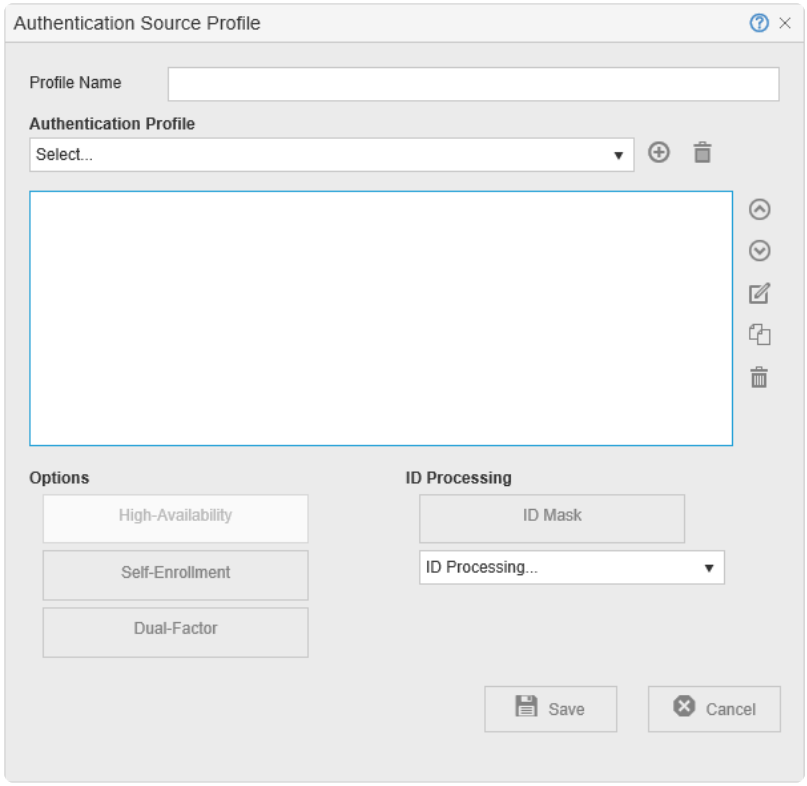
Dual Service Account System

To avoid any connection error after refreshing/changing the login/password on service accounts used by Celiveo, the administrator can define a secondary set of credentials so that if the default (primary) set is declined by the solution, then the secondary set takes over and prevents the access from being denied.

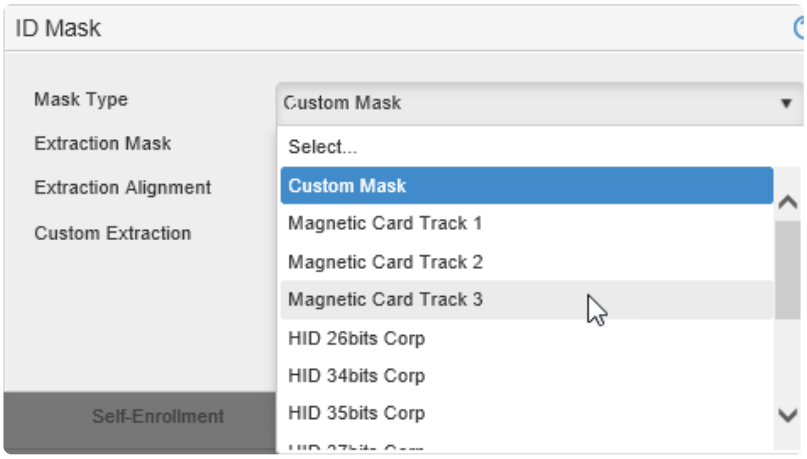


Note: The Login User (Login Name) used in Celiveo Authentication Profile requires AD/LDAP Read and Write rights to the user's attributes.

5. Specify How to Process Card Number

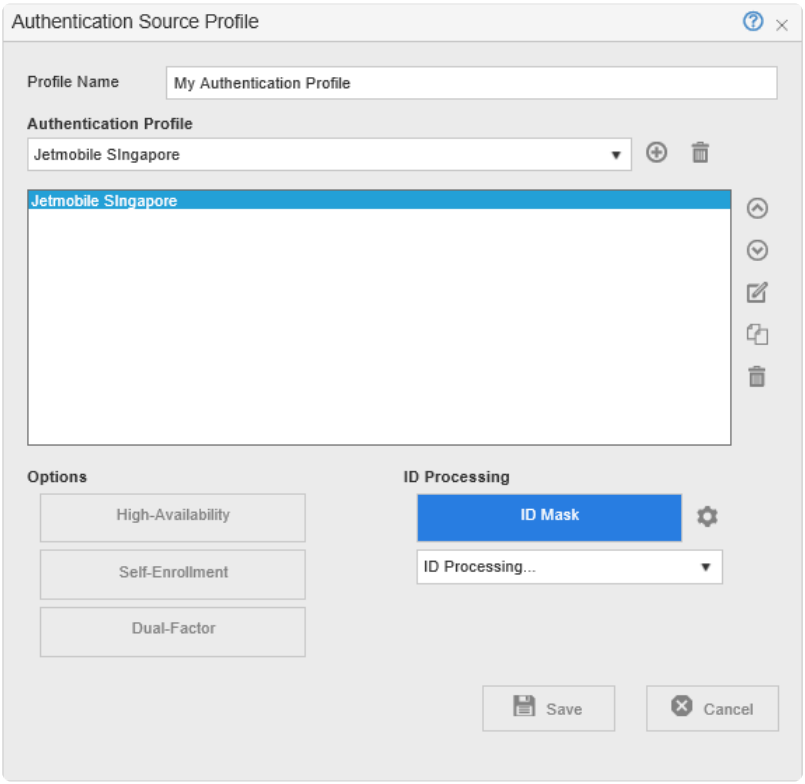


1. Click **[ID Mask]**.
2. Click ⚙ next to the **[ID Mask]**.
3. From the **[Mask Type]** drop-down, select the mask that extracts the card number.

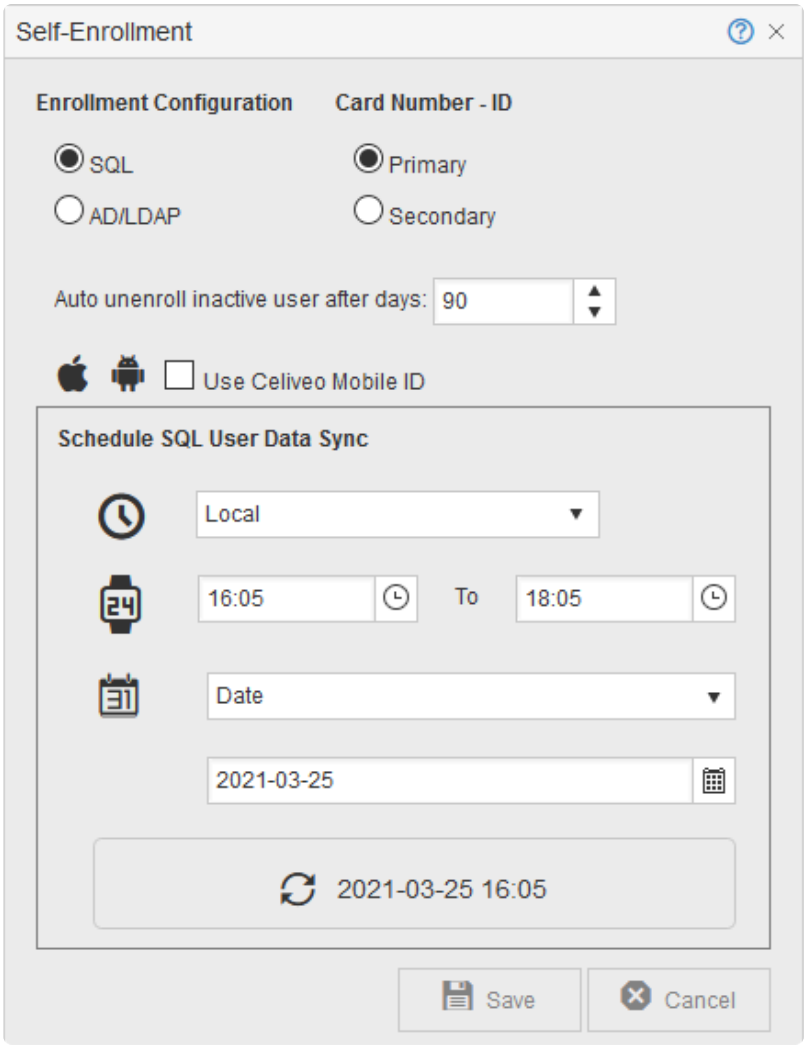


4. Click **[Close]**.
5. From the **[ID Processing]** drop-down, specify how the Card Number is processed.

6. Enable Self Enrollment



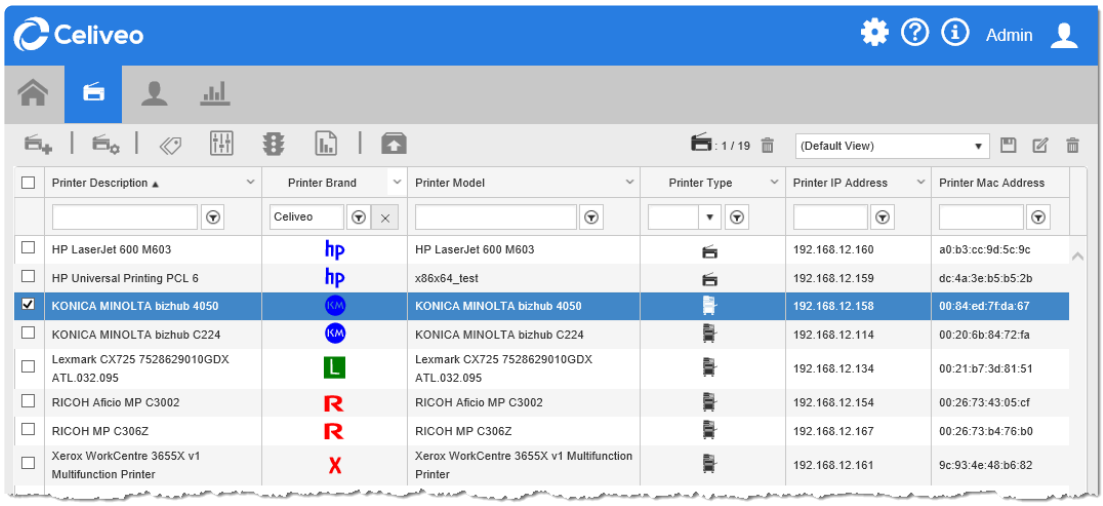
1. Click **[Self-Enrolment]** to turn it on.
2. Click ⚙ next to the **[Self-Enrolment]**.



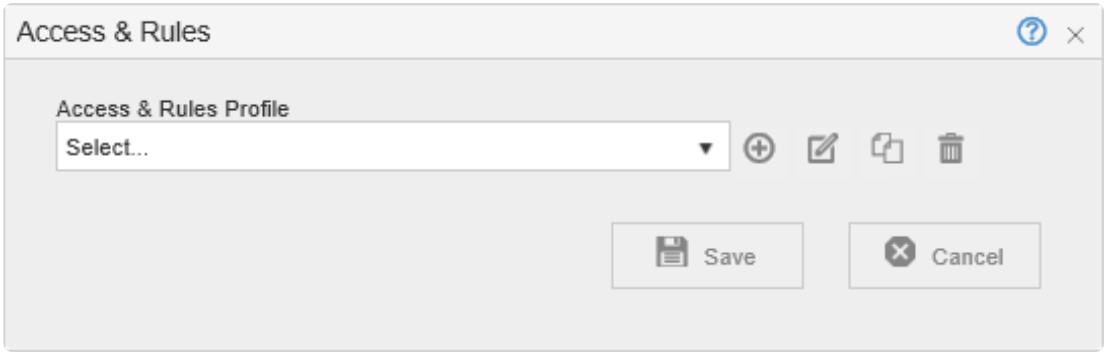
3. Verify that **[SQL]** is selected and click **[Close]**.

4. Click **[Save]** until all dialogs close.

7. Enable Card Authentication for Remaining Printers



1. In the Printers List, select the printers you want to apply the Access and Rules Profile to.
2. Click . The Access & Rules dialog is displayed.



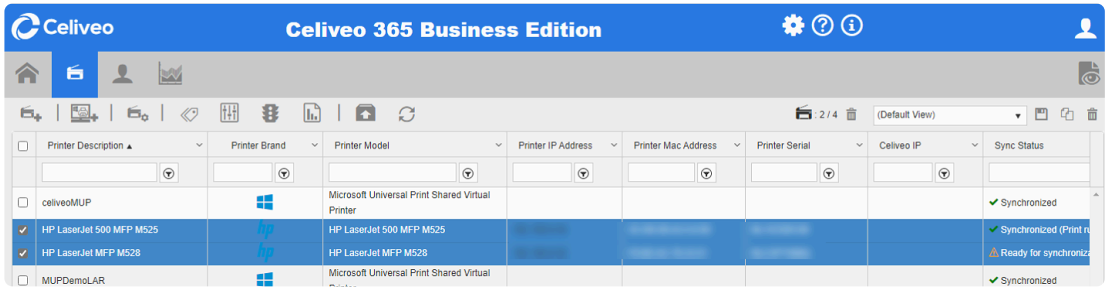
3. From the **[Access & Rules Profile]** drop-down, select the Access and Rules profile for the Printer.

> **Note for HP Printers:** When authenticating by showing a card to the printer card reader, follow the instructions shown on the bottom of the printer screen and wait until the authentication is complete before pressing any button.

Last modified: 29 September 2022

8.9. Synchronize Printers

Once you have defined all needed settings for a physical printer, these settings must be uploaded to the printer. You upload the settings by synchronizing the printer with the Web Admin.



1. Select the printers to synchronize.

   Note: Only physical printers that have their Celiveo Pull Print property enabled can be synchronized.

2. Click .
   The selected printers are synchronized, one at a time.

> **IMPORTANT NOTE:** on HP devices, make sure the printer status is “Print Ready” before starting the synchronization.

Last modified: 29 September 2022

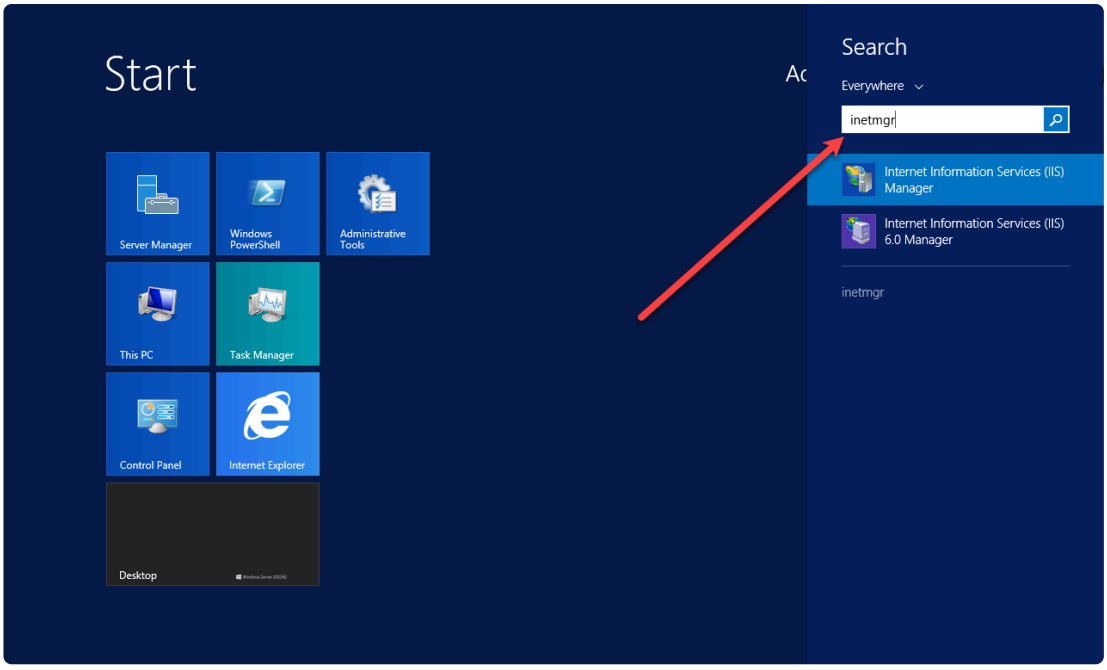
8.10. Set the Session Timeout

What is the Session Timeout?

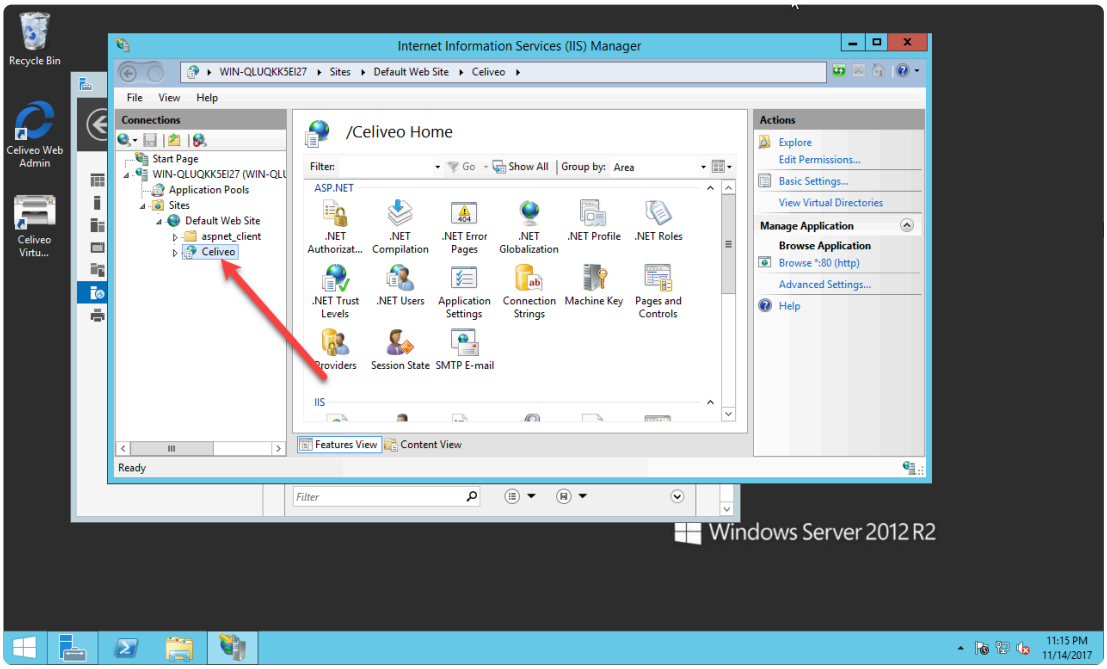
The Session Timeout specifies how long the system should wait before ending a Web Admin session, if no activity is detected.

To Specify the Session Timeout:

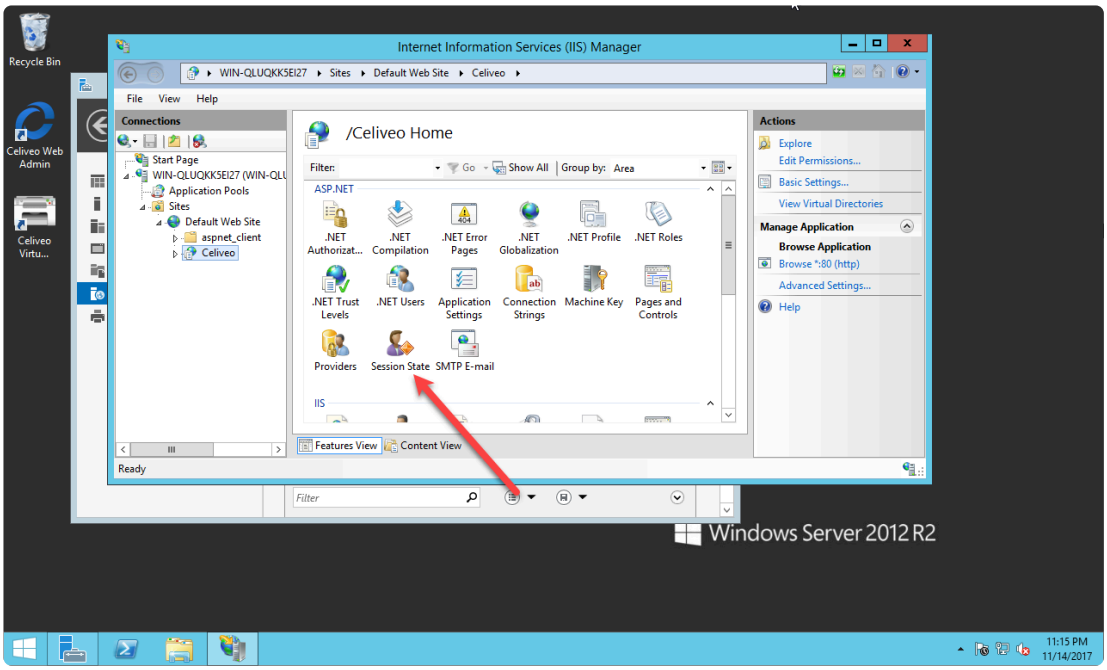
1. Open IIS Manager.
   To open IIS Manager, type **inetmgr** in the **Start Search** box and press ENTER.



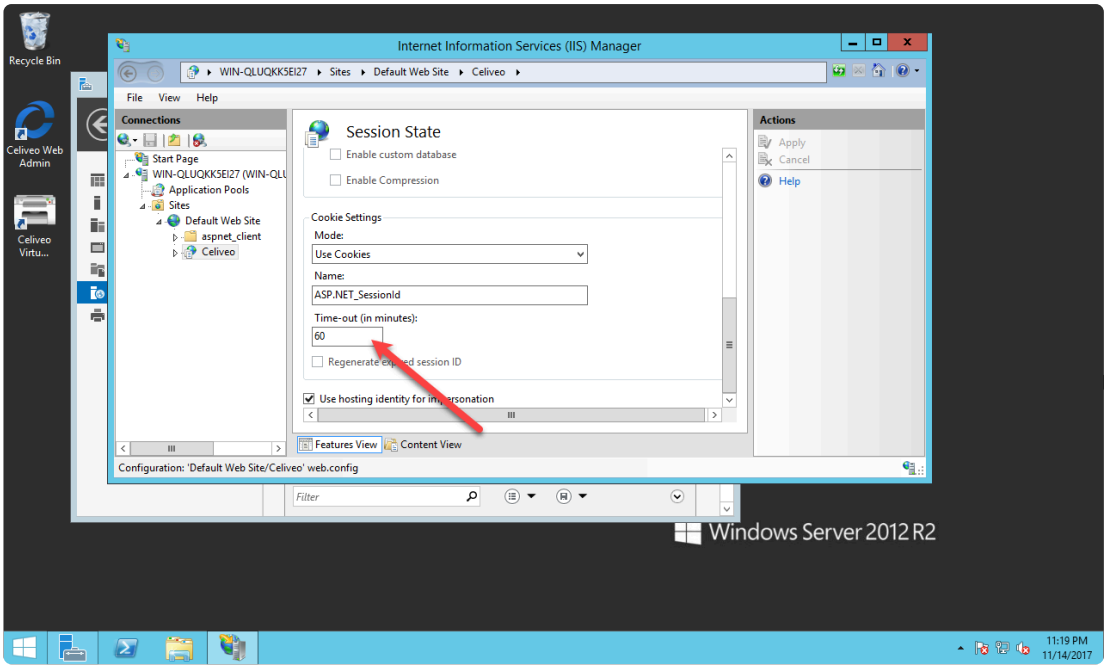
2. In the left pane, select ***Server Name*** **> Sites > Default Web Site > Celiveo**.



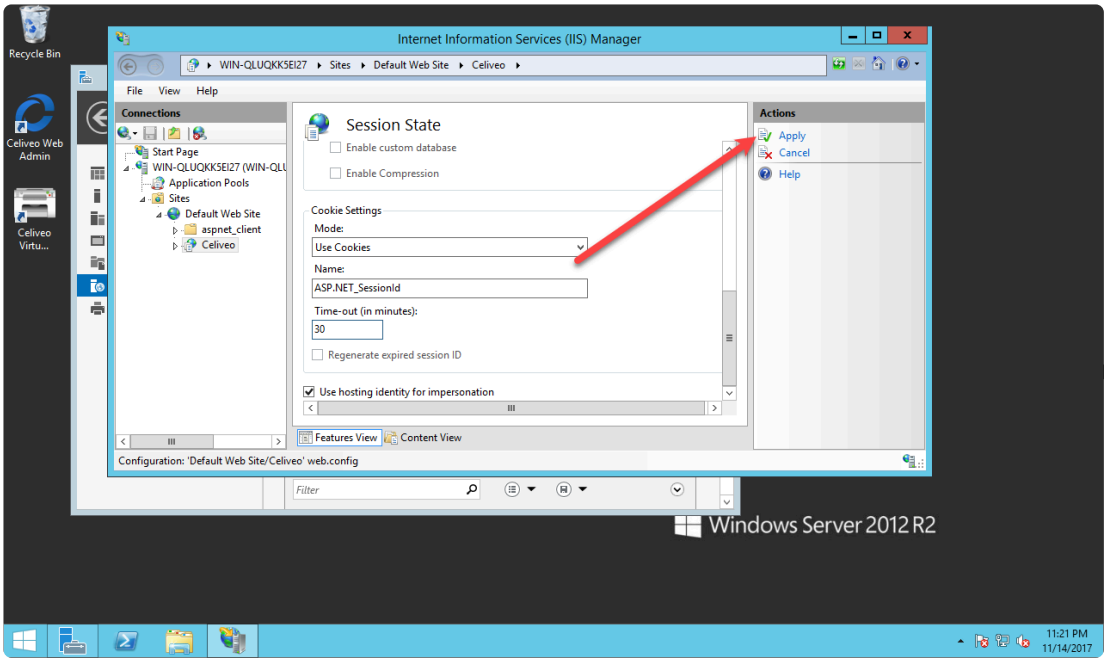
3. In the middle pane, double-click **Session State**.



4. In **Cookie Settings**, at **Time-out (in minutes)** specify the new session timeout.



5. Click **Apply**.



Last modified: 29 September 2022

8.11. Configuration to be done at the Printer

Configuration on Konica Minolta Devices
Configuration on Lexmark Devices
Configuration on Ricoh Devices
Configuration on Xerox Devices
Configuration on HP Devices

Last modified: 29 September 2022

8.11.1. Konica Minolta

Here, you will learn about the prerequisites and required settings to be done on the Konica Minolta printer device before and after installation of the Celiveo solution.

1. Prerequisites
2. Ports and Communication
3. Configure the device using Konica Minolta Page Scope Web Connection
4. Configuration after installing Celiveo

1. Prerequisites

Before you install, make sure these prerequisites are met:

- The device is connected to an active LAN connection.
- The device has a fixed IP or DHCP reserved IP address.
- The network allows management by Simple Network Management Protocol (SNMP) v1/v2.
- The badge authentication should be configured as “Unset” (deactivated) on the Konica Minolta devices. To enable/disable this feature, contact a Konica Minolta technician.
- User authentication (for Print without authentication) should be disabled on the Konica Minolta driver.
- The Celiveo Smart Appliance is connected to the device.

1.1 Configuring CSA

By default, the CSA is set in DHCP mode. You can also opt for fixed IP network settings.

The steps to configure CSA for DHCP and for fixed IP network settings can be found here.

1.2 Celiveo Version upgrade on CSA

Follow the procedure given here to upgrade the Celiveo Version on CSA.

2. Ports and Communication

A comprehensive list of all the ports used by Celiveo solutions, describing the ports and applications used for communication between the Celiveo components that consist of the Celiveo Server Services, Web Admin Server, Active Directory, Database (SQL) server, the device, and the PC/laptop/workstation can be found here.

Konica Minolta Printers use HTTPS protocol for communicating between Celiveo Smart Appliance and the printer device.

3. Configure the device using Konica Minolta Page Scope

Web Connection

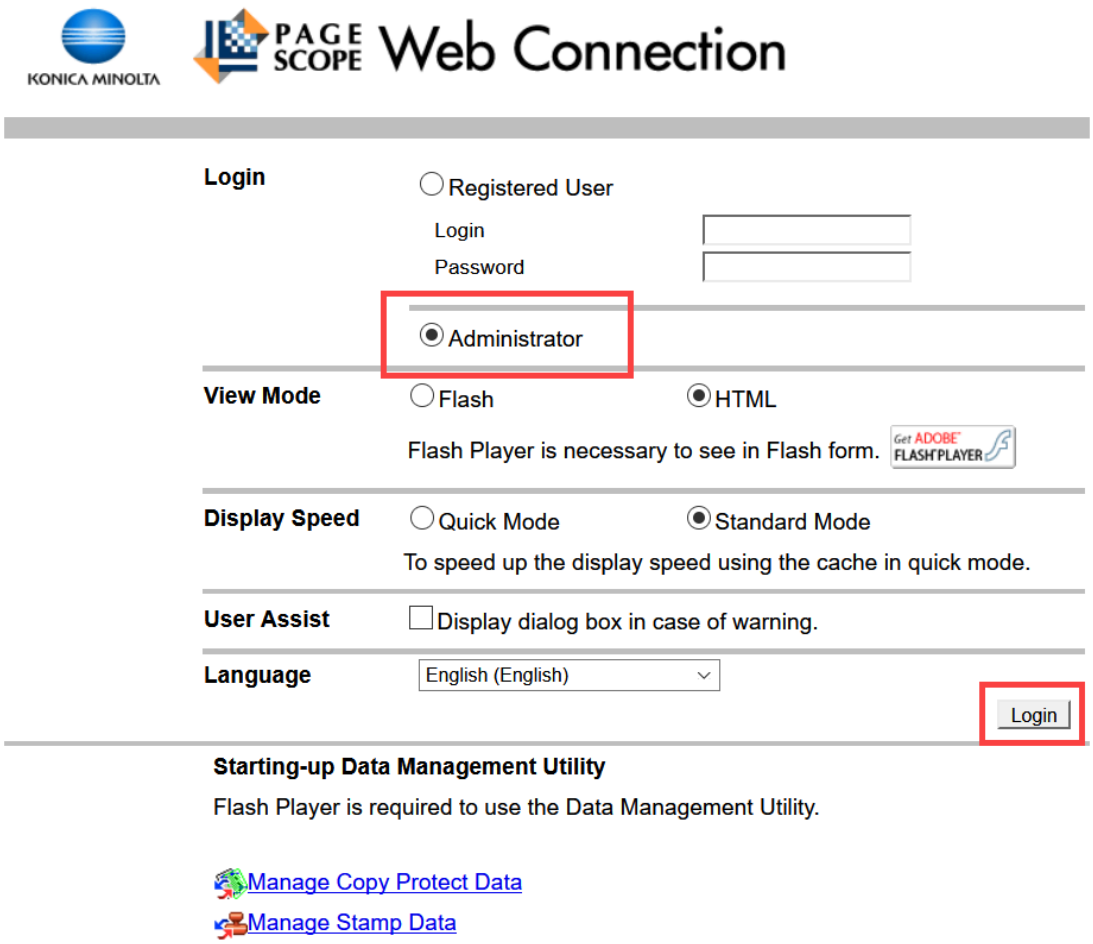
This section describes the required configurations to be performed on the device's web service page before you install the Celiveo solution.

- Create and upload an SSL certificate
- Enable SSL communication on socket

3.1 Create and upload an SSL Certificate

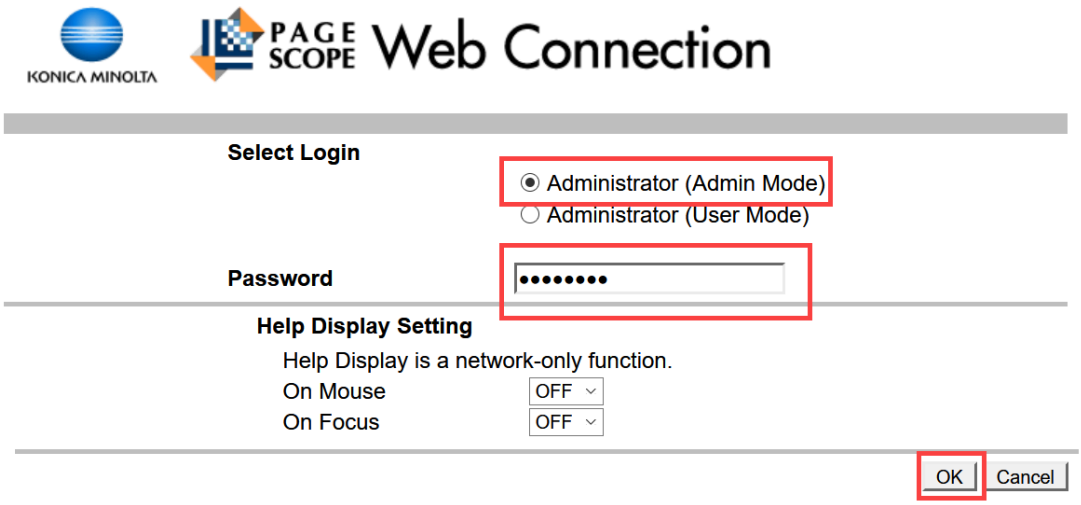
A valid SSL certificate is required for the solution to work. Either use an approved SSL certificate provided, or create a self-signed certificate on the device.

1. At the web browser, enter the IP address of the Konica Minolta device.
2. Select the Administrator radio button and click **Login**.

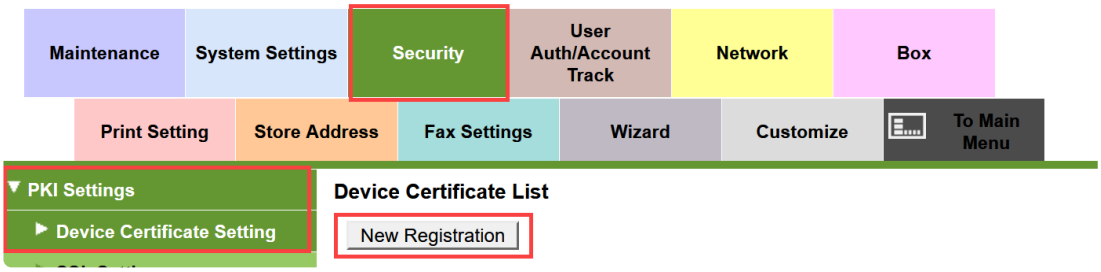


3. Select the **Administrator (Admin Mode)** radio button.
4. Enter the administration password and click **OK**.

> **Note**: Refer to the device manufacturer documentation for the default password.

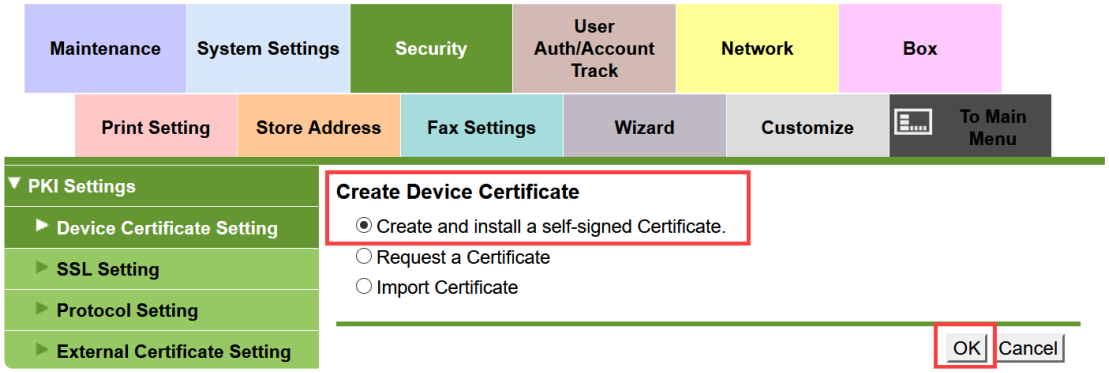


5. After logging in, click **Security**.
6. Go to **PKI Settings > Device Certificate Setting**, click **New Registration**.

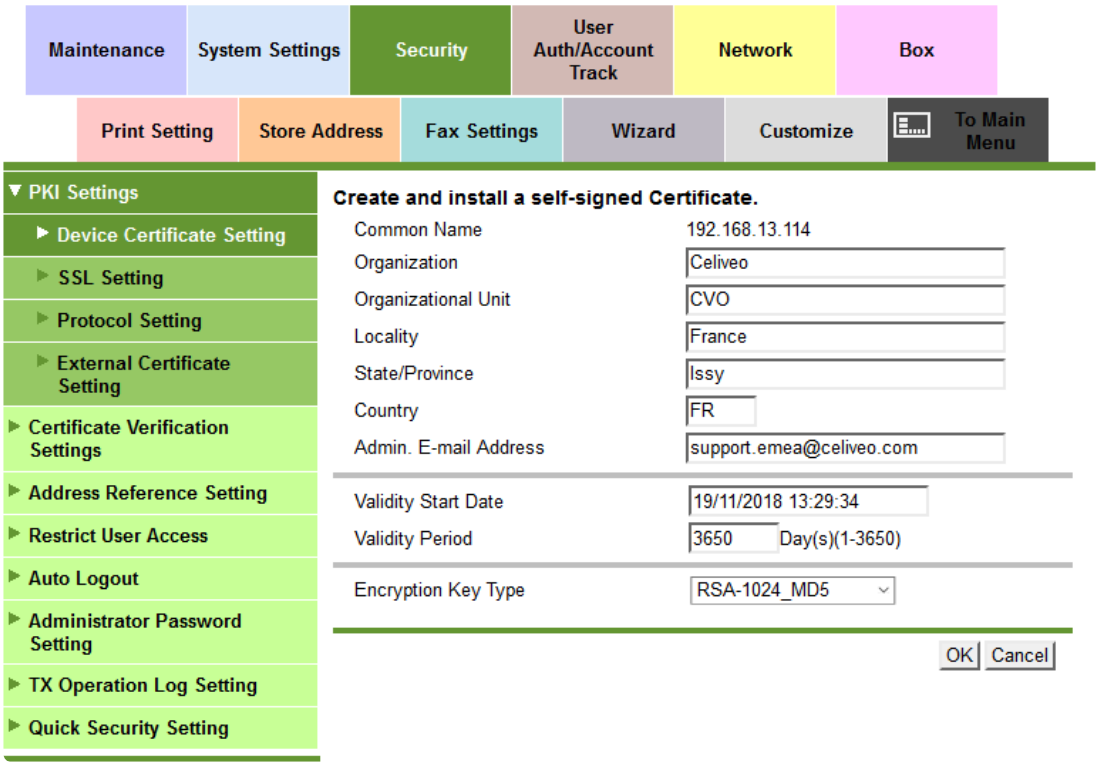


7. Under **Create Device Certificate**, select the **Create and install a self-signed Certificate** radio button and click **OK**.

> **Note**: If the SSL certificate is already available, click **Import Certificate**. Browse to the location and select the appropriate SSL certificate. Upload the required SSL certificate, enter the password and click **OK**.



8. Enter the information in the self-signed certificate fields as shown and click **OK**.



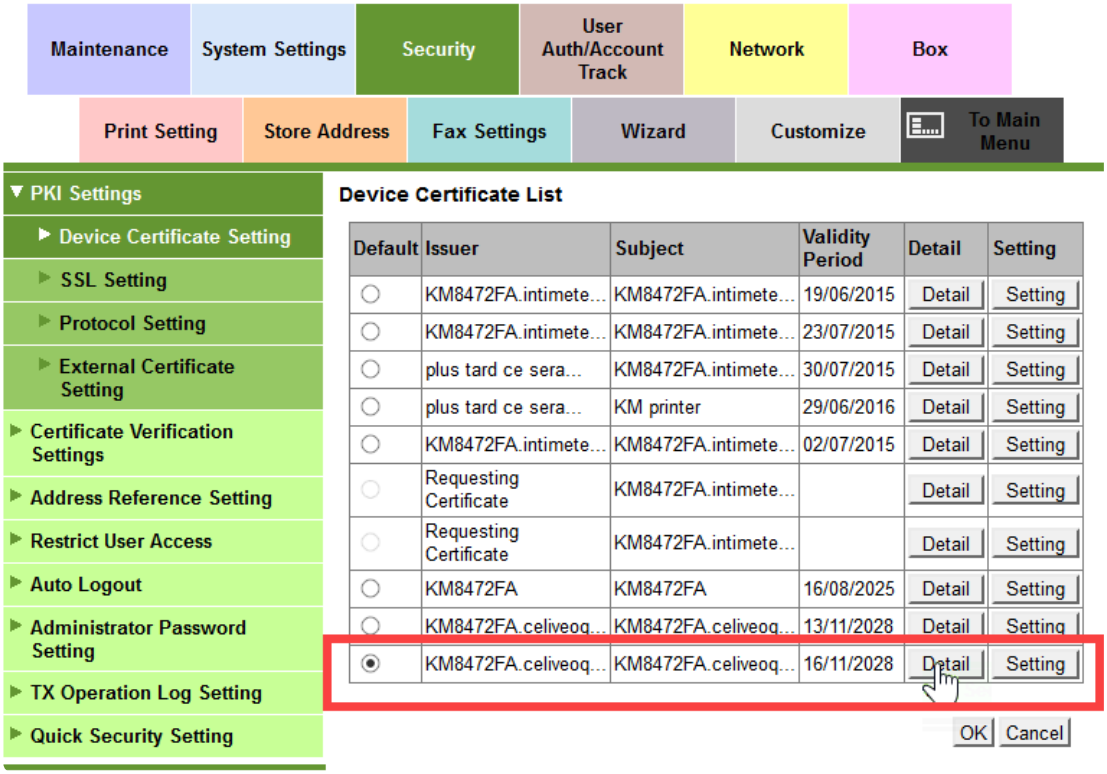
The messages are displayed:
'Certificate is being created. Please wait'
'Certificate has been created and installed. SSL/TLS can now be used. (After OK is clicked, SSL Mode setting will be available.)'

9. Click **OK** to apply the SSL mode settings.
10. After the certificate has been created and uploaded, click on **Security**, then click **Device Certificate List**.
11. Select the newly created certificate, then click **OK**.

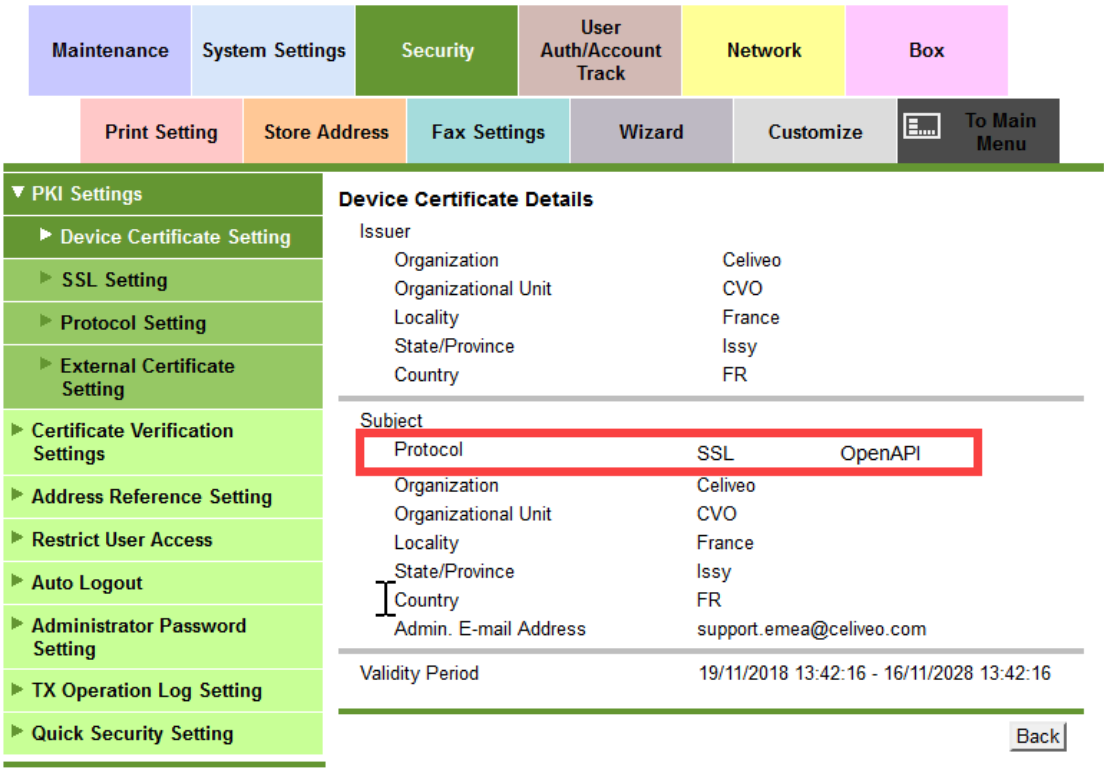
The following message is displayed: 'Completed. Activate your browser again.

3.2 Verify the Protocol set for the Certificate

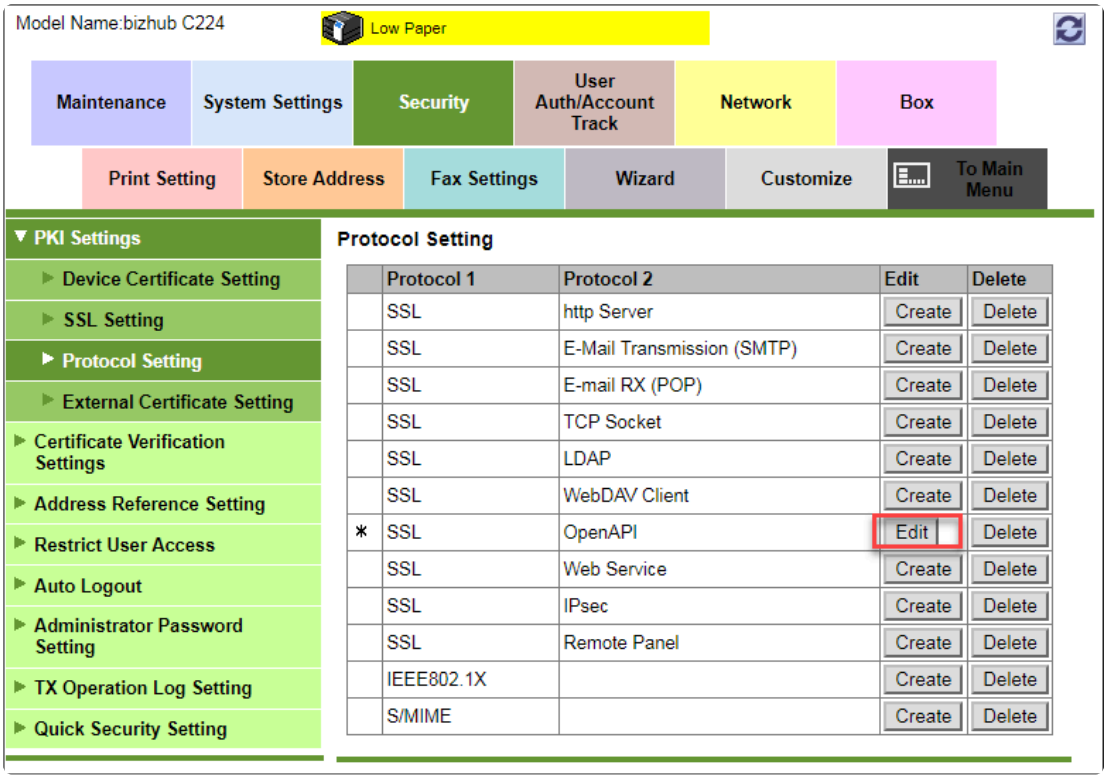
1. Go to **Security > PKI Settings > Device Certificate Settings**, then click **Details** next to the certificate to use.

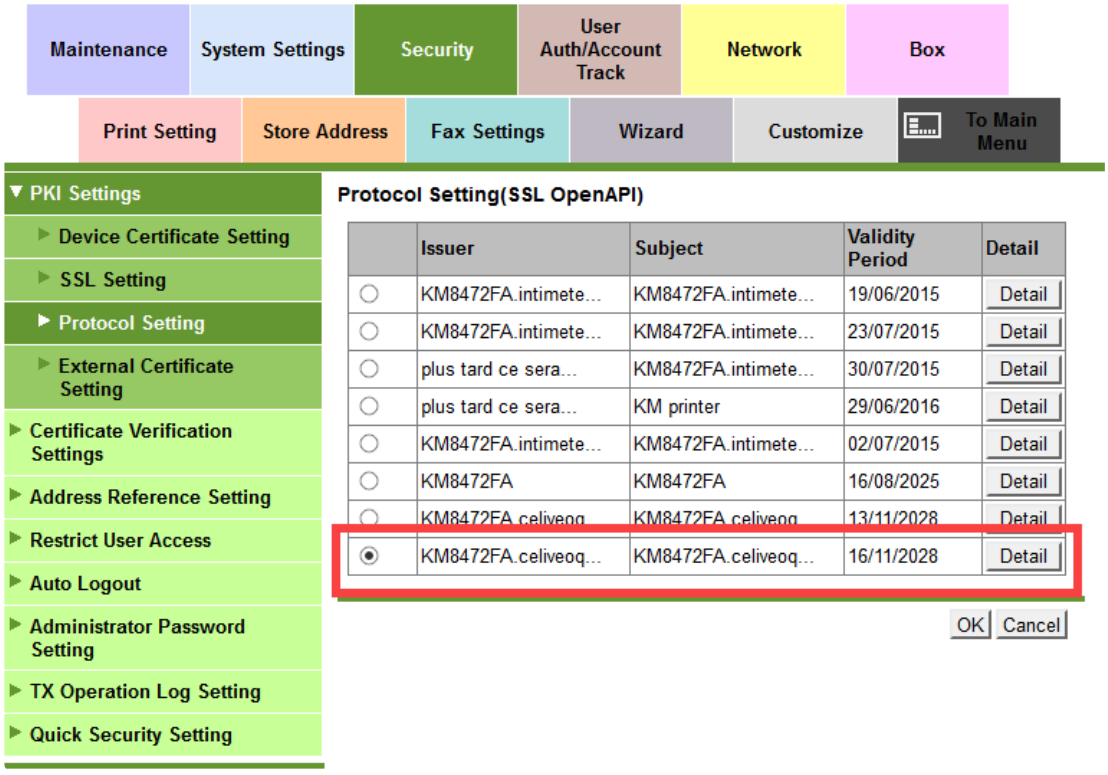


2. Check that the Protocol is set to **SSL OpenAPI**. Otherwise, follow step 3.



3. Go to **Protocol Setting**, click the **Edit** button next to **SSL OpenAPI** and select the required certificate.





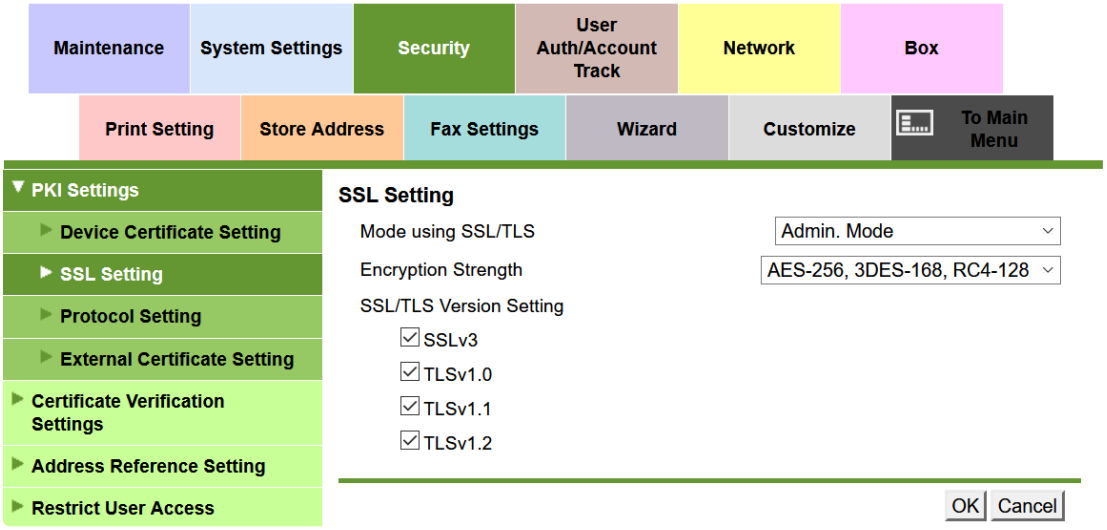
3.3 Enable SSL Communication on socket

This section describes the steps to enable the SSL/TLS port number so that it can establish the communication on the socket.

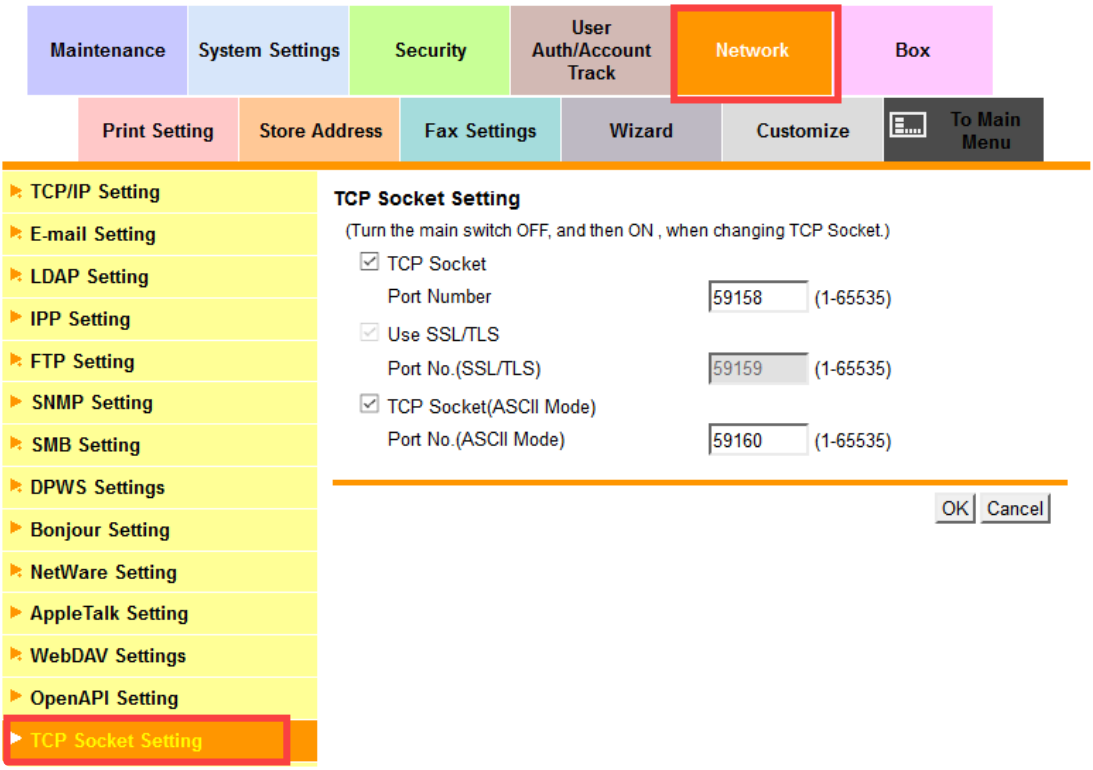
1. Log into the Web interface as Administrator.
2. After successful login, go to **Security> PKI Setting> SSL Setting**
3. In the drop-down menu, select **Administrator mode**. Click **OK**.

Your browser will reconnect to the web server in “https” mode. You may need to confirm an invalid certificate in your browser.

IMPORTANT NOTE: Ensure that TLS 1.2 protocol is enabled in the SSL setting. You may need to upgrade the printer firmware, if the options are not available.

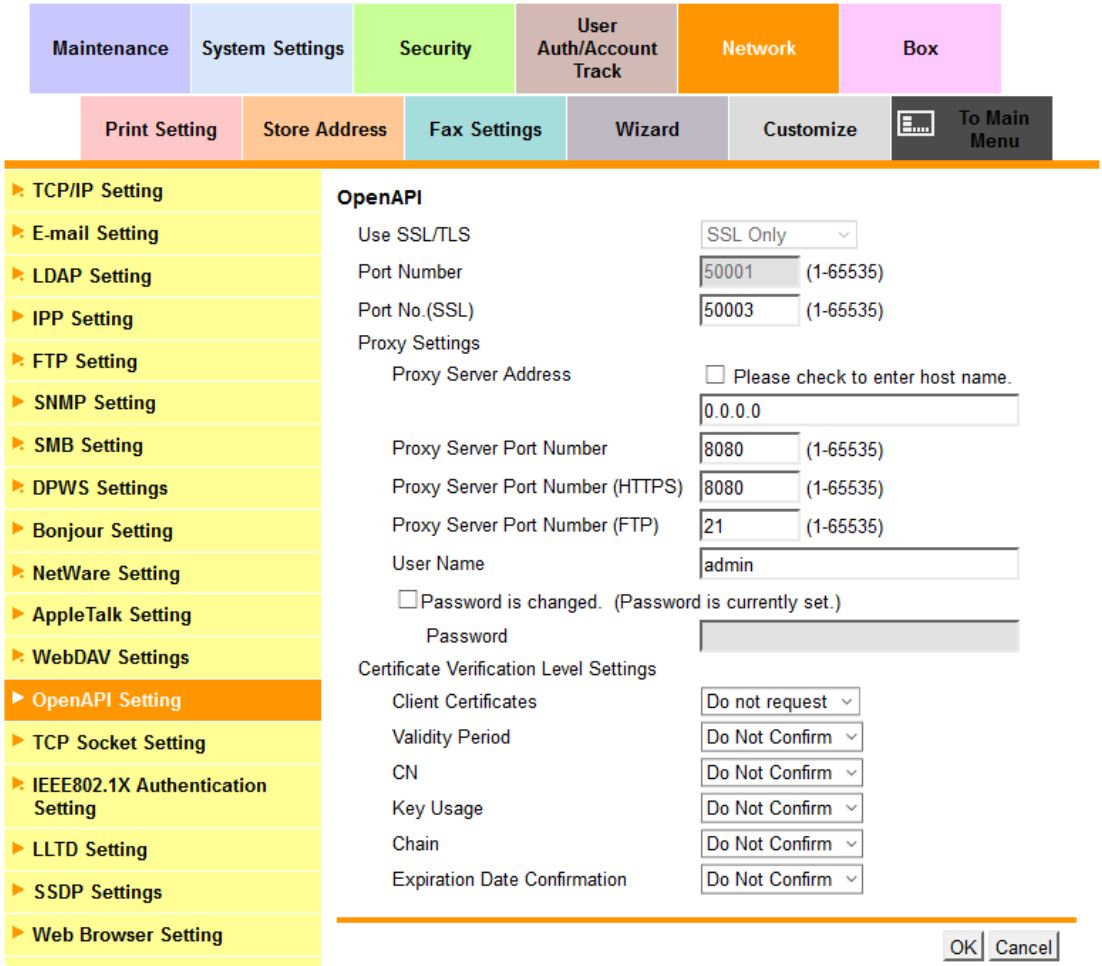


4. Go to **Network > TCP Socket Setting** page, select **Use SSL/TLS Port No. (SSL/TLS)** and click **OK**.
   The message is displayed: ‘Turn the main switch OFF, and then ON, when changing the settings.’



5. Log in again to the Web interface as Administrator and in the **Network** section, select **OpenAPI Settings**.
   - In the **Use SSL / TLS** drop-down list, select **SSL Only**.

- Verify that the SSL port number is **50003**.
- **Certificate Verification Level Settings** must be set as follows: Client Certificates: “Do not request”.
  For all other items, select “Do Not Confirm” (even for the Validity Period item for which “Confirm” is often set by default).



6. To apply the settings, click OK.
7. Reboot the device.

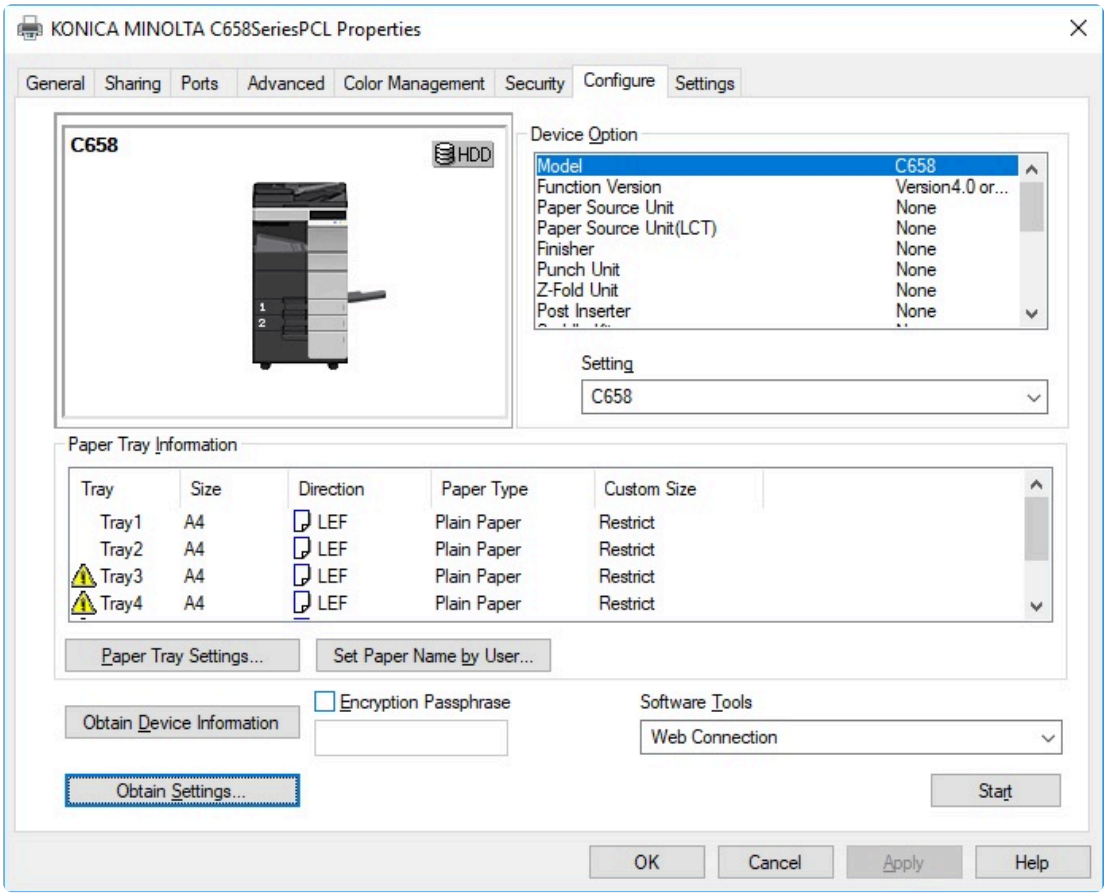
4. Configuration after installing Celiveo

Make these configurations after the installation of the Celiveo solution.

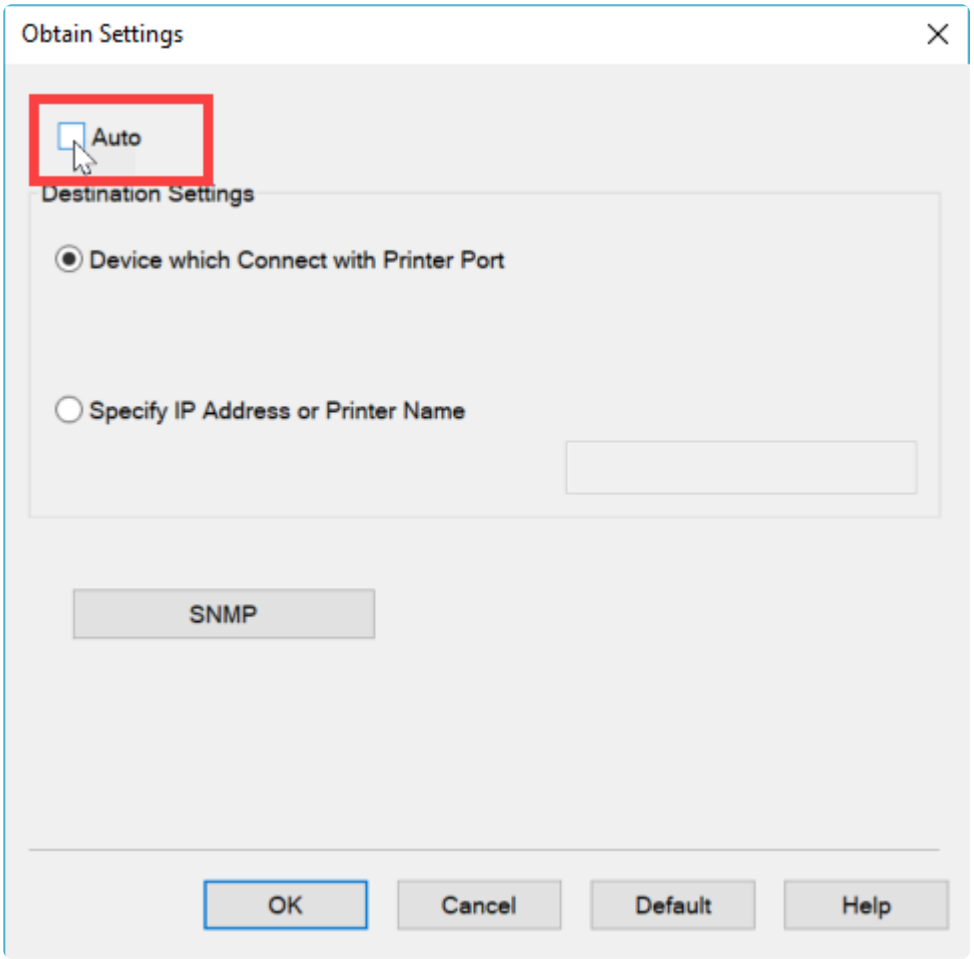
4.1 Disable user authenticated printing in printer properties

After installation of the Celiveo solution, disable the unauthenticated printing setting by the printer driver. This allows the Celiveo solution to take over tracking of device usage activities after user authentication.

1. At the client machine, open the print queue properties.
2. Select **Configure**.
3. Click on **Obtain Settings**.



When prompted, uncheck **Auto** and click **OK**



Note: On some models, the IP address and device administrator password have to be entered before the Auto option can be unchecked.

4. In the **Device Options** list, select **User Authentication**.
5. Select **Disable**, then click **Apply**.
6. To exit, close the dialog box.

4.2 Disable user authenticated printing on device UI

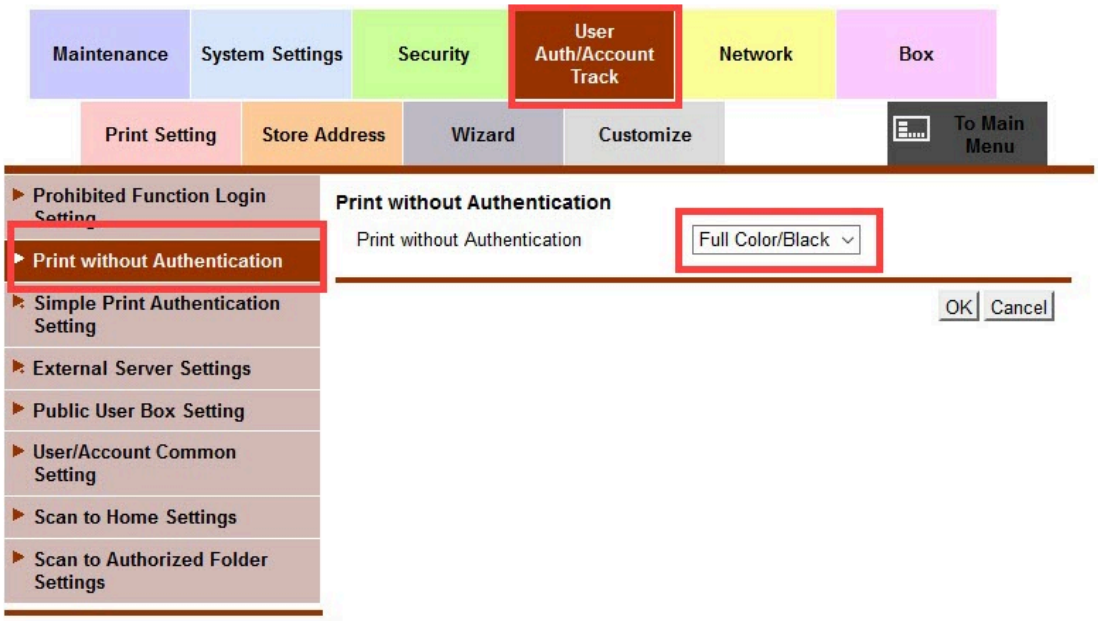
Note: The settings in this section are required only if you have not disabled user authenticated printing in Konica Minolta Web Services.

1. On the front panel of the device, press the **MENU** button.
2. Press **Utility**, then press **Administrator Settings**.
3. Enter the administrator password and press **OK**.
4. Press **User Authentication/Account Track**.
5. Press **Print without Authentication**.
6. To save the settings, press **Full Color/Black**, then press **OK**. (On some models, select **Allow**, if **Full Color/Black** is not available)

4.3 Disable user authenticated printing from Konica Minolta Page Scope Web Connection

Note: The settings in this section are required only if you have not disabled user authenticated printing at the printer UI.

1. Log in to Web interface as Administrator.
2. Go to **User Auth/ Account Track > General Settings >Print without Authentication**.
3. In Print without Authentication drop-down menu, select **Full Color/Black**.



4. To save the settings, select **OK**.

Last modified: 29 September 2022

8.11.2. Lexmark

System Requirements

The system requirements for installing Celiveo 8 solution can be found here.

Ports and Communication

A comprehensive list of all the ports used by Celiveo solutions, describing the ports and applications used for communication between the Celiveo components that consist of the Celiveo Server Services, Web Admin Server, Active Directory, Database (SQL) server, the device, and the PC/laptop/workstation can be found here.

> Lexmark Printers use HTTPS protocol for communicating between Celiveo Smart Appliance and the printer.

Prerequisites

Before you install, make sure these prerequisites are met:

- The device is connected to an active LAN connection.
- The device has a fixed IP or DHCP reserved IP address.
- The network allows management by Simple Network Management Protocol (SNMP) v1/v2.
- From the device embedded web services, set the device session time to be longer than the default Celiveo Web Admin inactivity time out (30 sec).

Configuring CSA

By default, the CSA is set in DHCP mode. You can also opt for fixed IP network settings.

The steps to configure CSA for DHCP and for fixed IP network settings can be found here.

Celiveo Version upgrade on CSA

Follow the procedure given here to upgrade the Celiveo Version on CSA.

Once the Celiveo embedded solution is installed on the device, there are additional settings to be done in order to operate in the Celiveo environment. This section includes the topics:

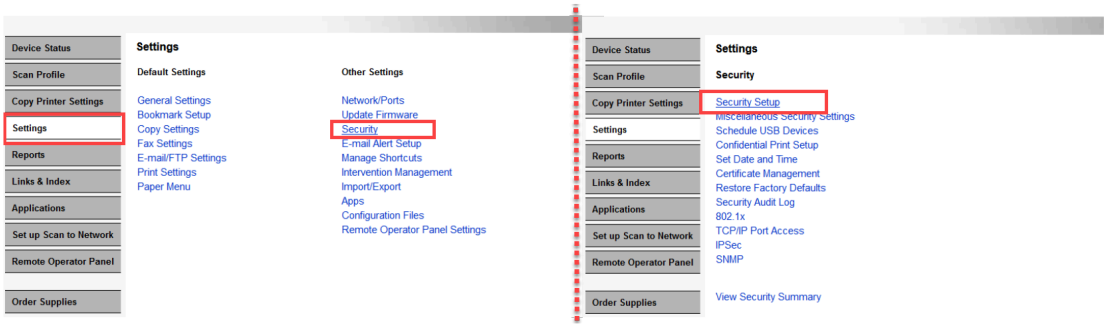
1. Basic Security Setup
2. Enable Lexmark Device Logs
3. Reset Factory
4. Timeout Settings

Basic Security Setup on Lexmark Devices

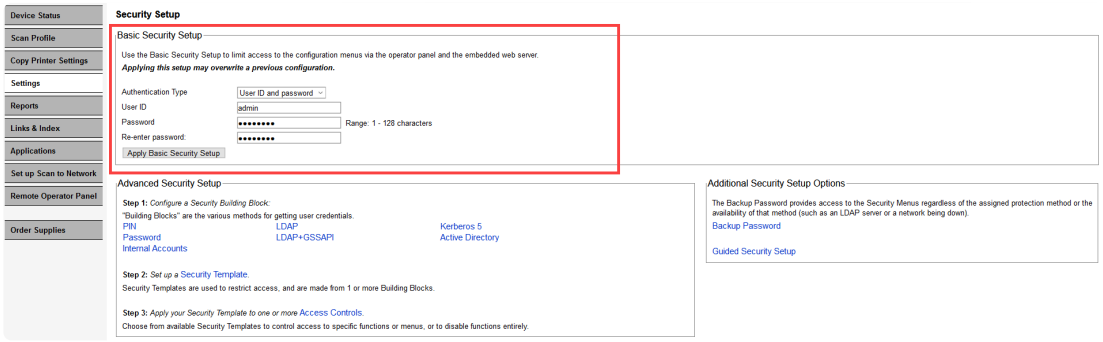
Setup Basic Security on Lexmark Device running on Framework 3.x/ 4.x

1. In the browser address bar, enter the IP address of the printer in the format shown below:
   https://Device_IP_Address
   The device Embedded Web Server page opens.

2. Click **Settings** in the left panel, then go to **Other Settings > Security > Security Setup**.

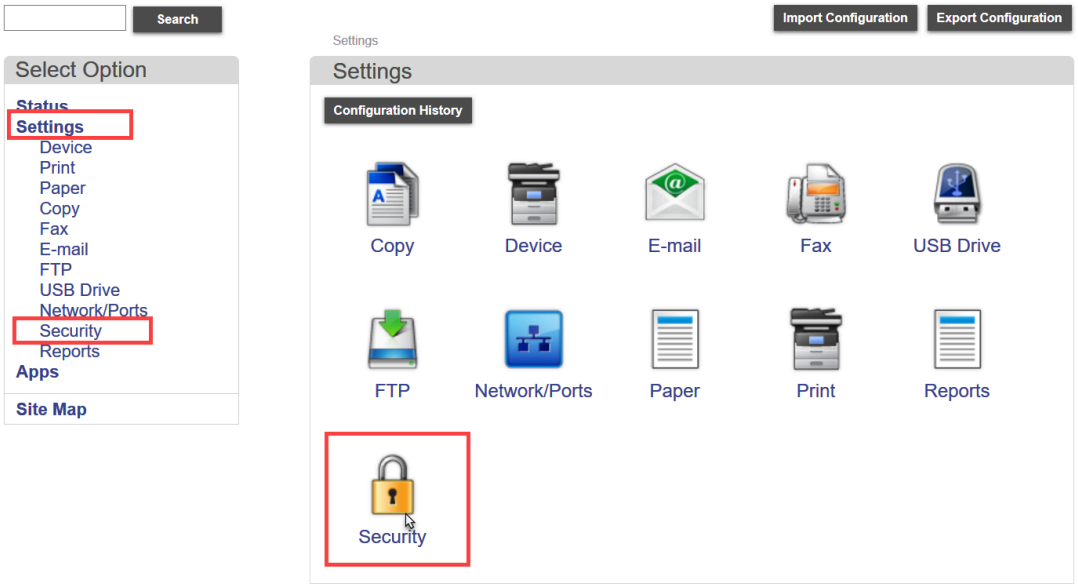


3. In the **Basic Security Setup** section, select **User ID and password** option as **Authentication Type**.
4. Set the User ID and password and click **Apply Basic Security Setup**.

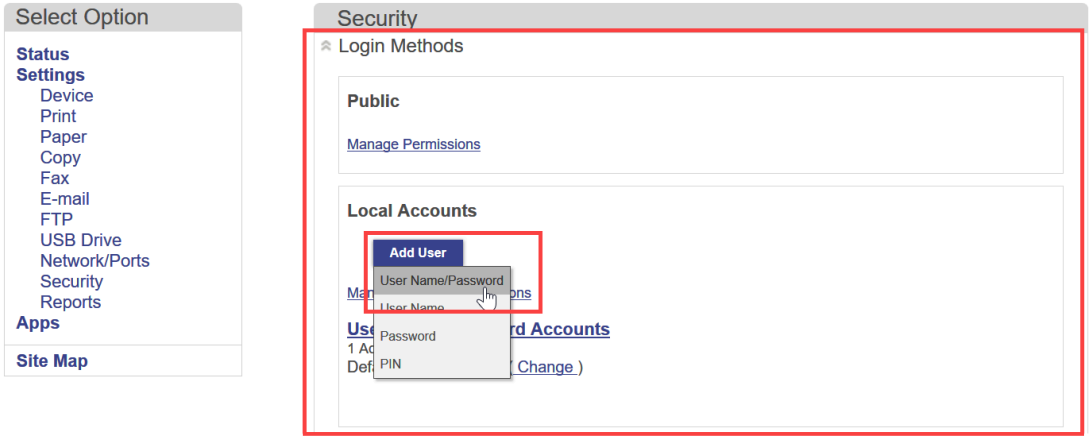


Setup Basic Security on Lexmark Device running on Framework 5.x/ 6.x

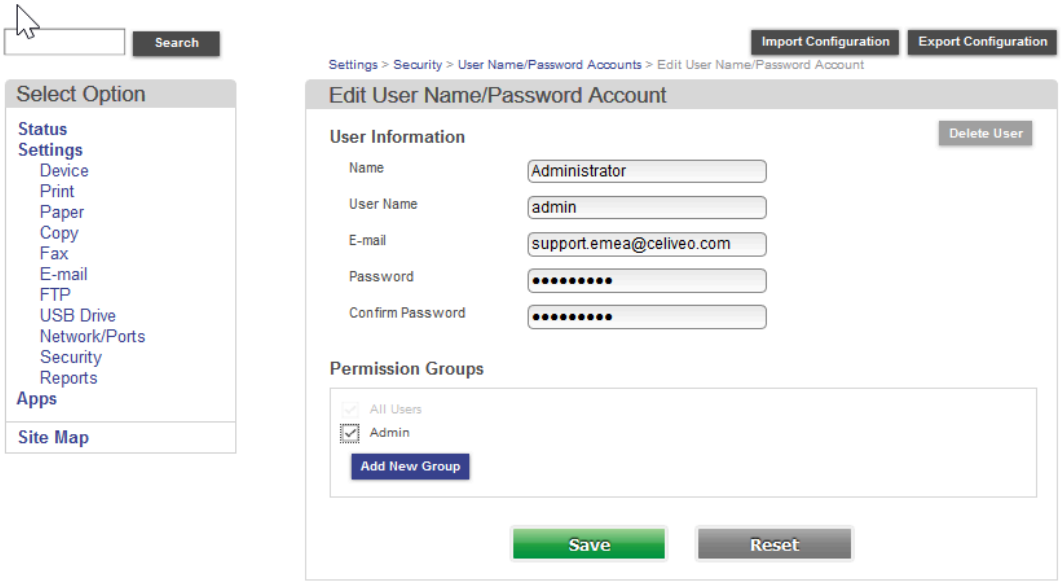
1. In the browser address bar, enter the IP address of the printer in the format shown below:
   https://Device_IP_Address
   The device Embedded Web Server page opens.
2. Click Settings in the left panel, then click Security and open Login Methods block.



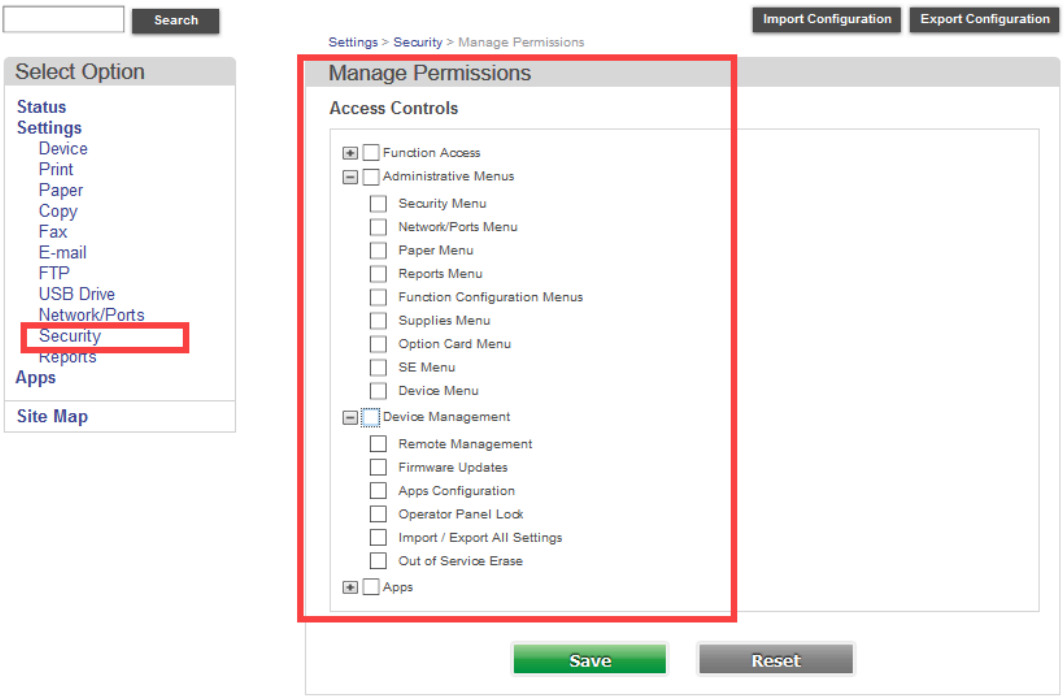
3. Under **Local Accounts** section, click **Add User** button.



4. Fill in user information such as name, username, e-mail, password etc.
5. Select **Admin** checkbox under **Permission Groups**, and click **Save**.



6. Go back to **Security**.
7. In the **Public** section, click **Manage Permission** link.
8. Uncheck all “Administrative Menus, “Device Management” and “Apps” controls.
9. Uncheck all Function Access that you want to be restricted.
10. Then, click **Save**.

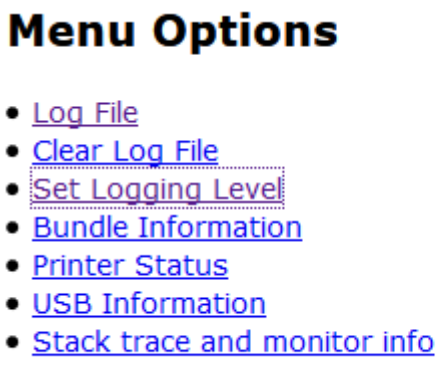


Enable Lexmark Logs

Enabling the Lexmark device logs helps in detecting and diagnosing a problem.

To enable device logs on the Lexmark device:

1. In the browser address bar, enter the IP address of the device in the format shown below:
   https://Device_IP_Address/se
   For example: https://192.168.8.82/se
   The Lexmark Embedded Web Server page opens.
2. Login as Admin user.
3. Click on Embedded Solutions, then click on **Set Logging Level**.



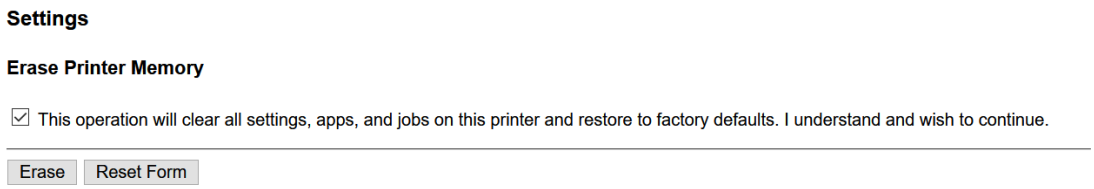
4. Click **Yes** option to allow debugging entries in the log, then **Submit**.
5. Repeat the above step.
6. Go back to Embedded Solutions, then select **Log File**.
7. Copy all the solution logs and send it to the Celiveo Support team.
8. After the solution logs are copied, return to step 3.
9. Click on **Default** option, then **Submit**.

Reset Factory

Reset Factory on Lexmark Device running on Framework 3.x / 4.x:

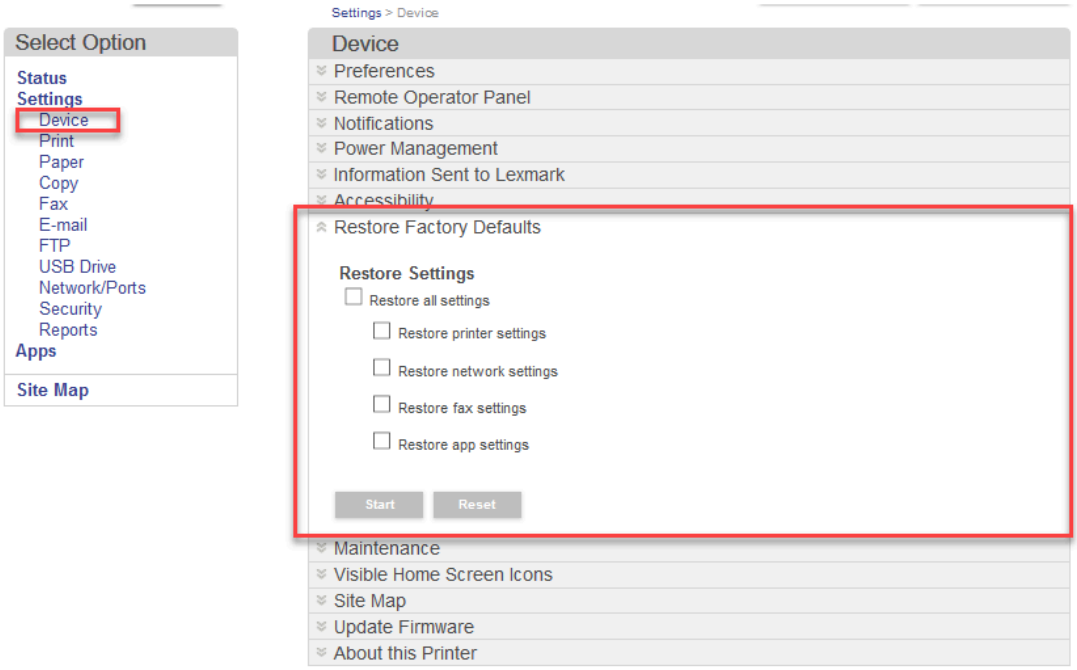
To enable device logs on the Lexmark device:

1. In the browser address bar, enter the IP address of the device in the format shown below:
   https://Device_IP_Address
   For example: https://192.168.8.82
   The Lexmark Embedded Web Server page opens.
2. Login as Admin user.
3. Click **Settings** in the left panel, then click on **Security**.
4. Click “Restore Factory Defaults”, then click on Erase Printer Memory.
5. Check “This operation will clear all settings, solutions, jobs, and faxes on this printer, and restore to factory defaults. I understand and wish to continue.”
6. Then click **Erase**.



Reset Factory on Lexmark Device running on Framework 5.x / 6.x:

1. In the browser address bar, enter the IP address of the device in the format shown below:
   https://Device_IP_Address
   For example: https://192.168.8.82
   The Lexmark Embedded Web Server page opens.
2. Login as Admin account.
3. Then click on **Device** on the left panel.
4. Go to **Restore Factory Defaults** block.
5. Check the required settings and click **Reset**.
6. Confirm the action when prompted.

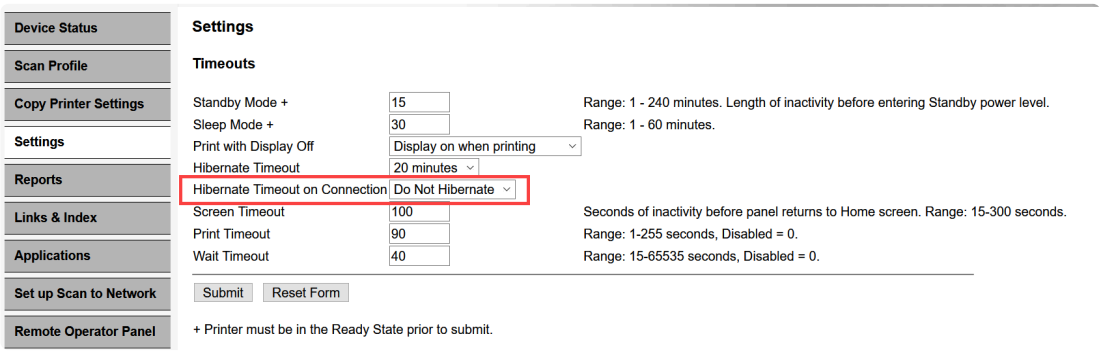


Timeout Settings

This configuration is necessary to ensure that the connection between the printer and Celiveo Smart Appliance is not disrupted.

Configure Timeout settings on Lexmark Device running on Framework 3.x / 4.x:

1. In the browser address bar, enter the IP address of the device in the format shown below:
   https://Device_IP_Address
   For example: https://192.168.8.82
   The Lexmark Embedded Web Server page opens.
2. Login as Admin user.
3. Click **Settings** in the left panel, then click go to **General Settings > Timeouts**.
4. Under the **Timeouts** section, make sure that **Do not Hibernate** is selected for **Hibernate Timeout on Connection**.
5. Configure the settings as shown in the image below:



6. Click **Submit**.

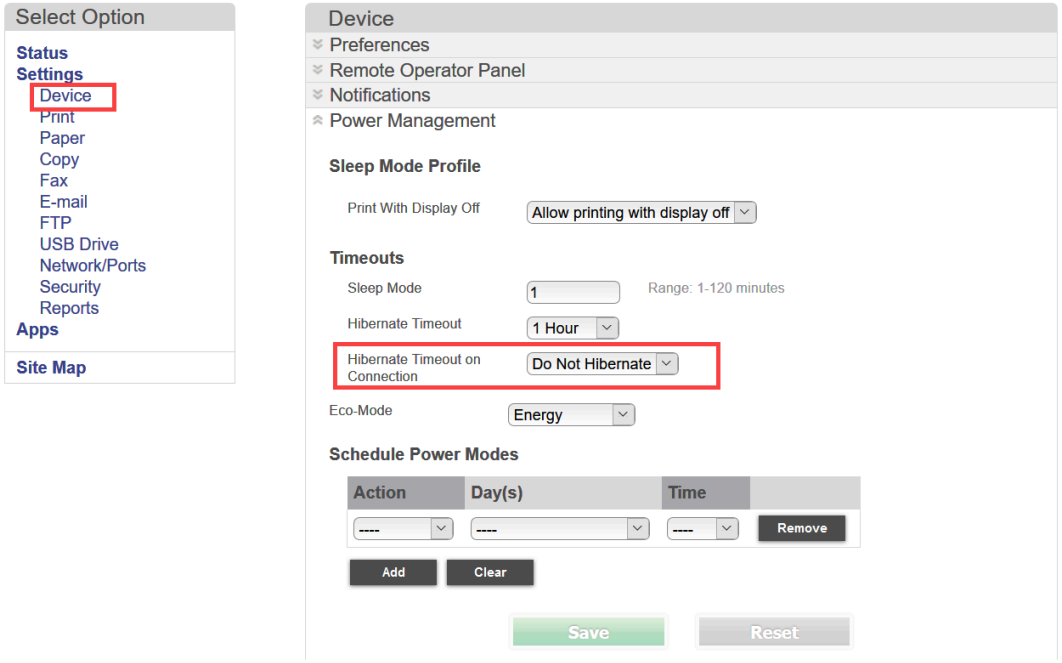
Configure Timeout settings on Lexmark Device running on Framework 5.x / 6.x:

1. In the browser address bar, enter the IP address of the device in the format shown below:
   https://Device_IP_Address

For example: https://192.168.8.82

The Lexmark Embedded Web Server page opens.

2. Log into Admin account.
3. Then click **Device** on the left panel.
4. Go to **Power Management** block.
5. In the **Timeouts** section, select **Do Not Hibernate** for **Hibernate Timeout on Connection**.
6. Select the configurations as shown in the image below:



7. Click **Save**.

Last modified: 29 September 2022

8.11.3. Embedded Agent for Ricoh Android SOP 2.x MFP

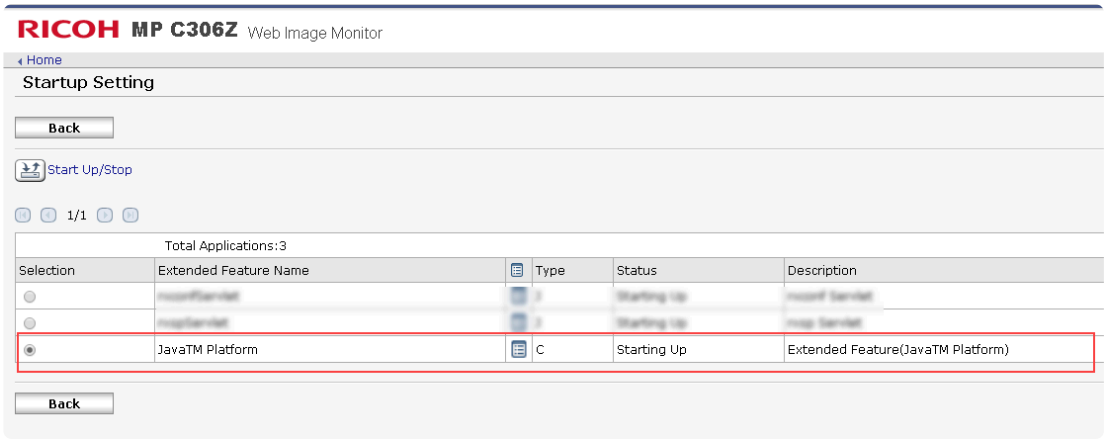
Contents

1. Prerequisites
2. Configure the printer before installing the Embedded Agent
3. Configuring the printer using Web Image Monitor
4. Connecting Celiveo Authentication Hardware (Card Reader) to the printer device.

1. Prerequisites

Before you install, make sure these prerequisites are met:

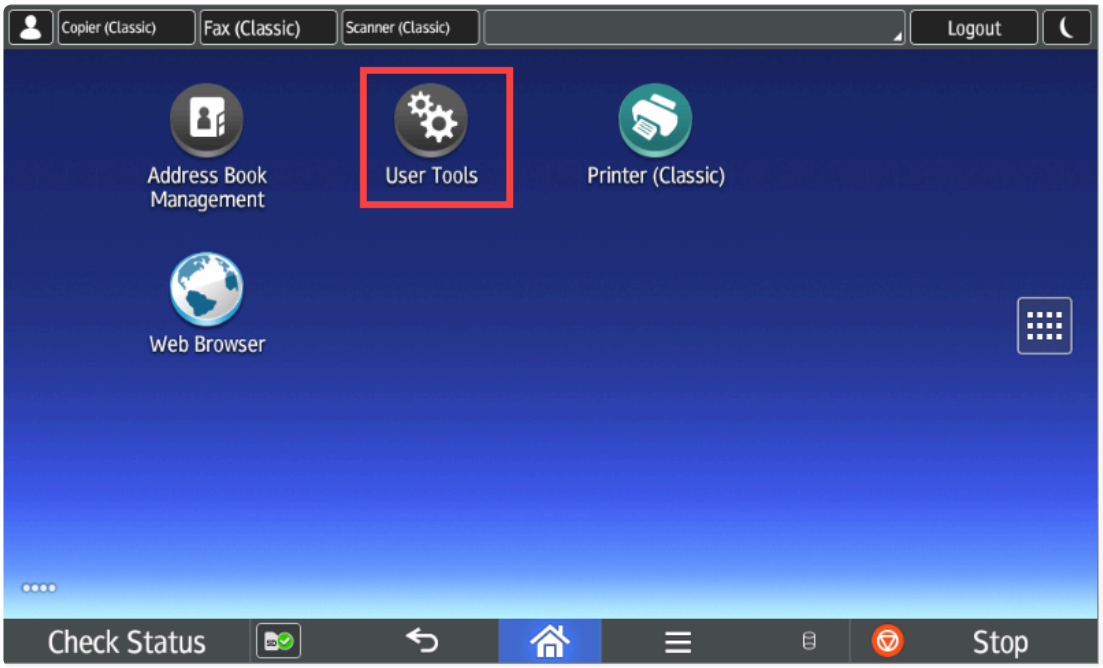
- The printer is connected to an active LAN connection.
- The printer has a fixed IP or DHCP reserved IP address.
- The network allows management by Simple Network Management Protocol (SNMP) v1/v2.
- Enable HTTPS for Ricoh secure access.
- JRE (Java SE Runtime Environment) 8 is installed on the virtual machine where the Celiveo solution (Web Admin) is hosted.
- Non-API Environment: SQL Server is configured to listen to port 1433 for TCP/IP connections.
- API Environment: SQL Server can be configured with using dynamic Port. Click here to download the API Package which to be installed on the same machine as hosted the Web Admin.
- Java TM platform is enabled on the printer (this is applicable for SOP2.0 Ricoh Models ONLY).



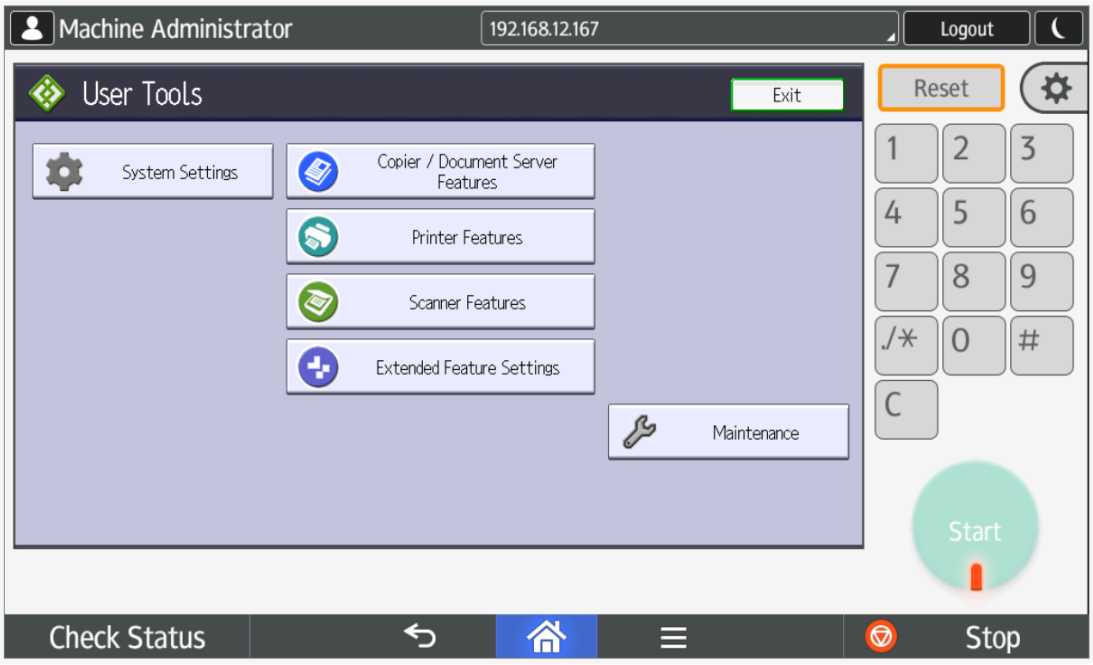
2. Configure the printer before installing the Embedded Agent

2.1 Configure network settings (IP and DNS settings)

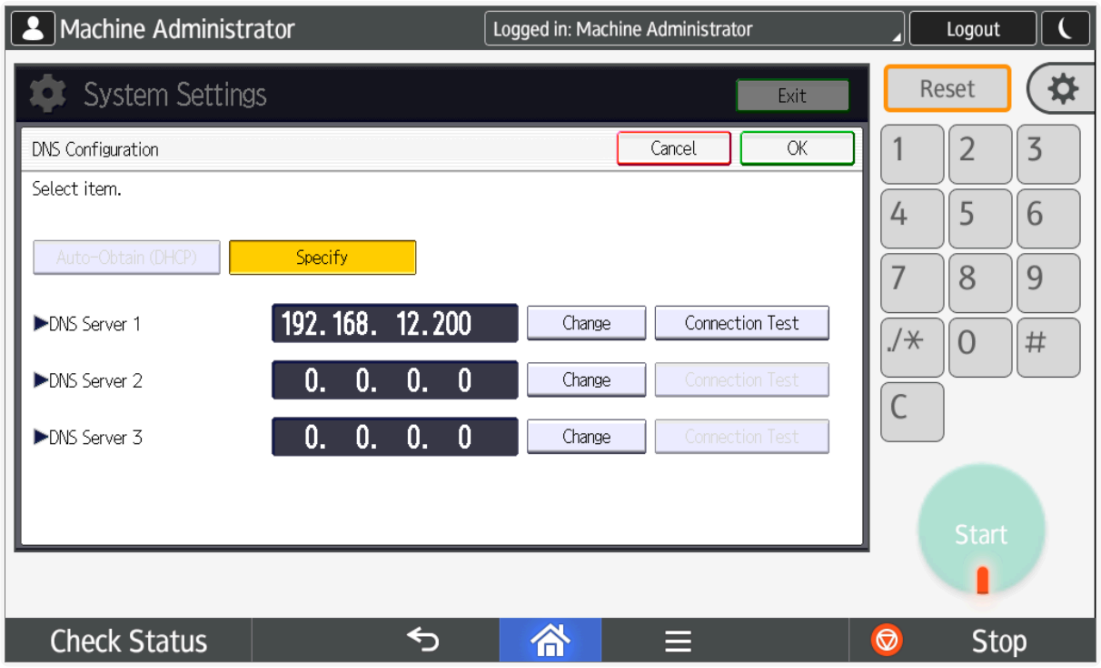
1. Press User Tools, then select Machine Features.



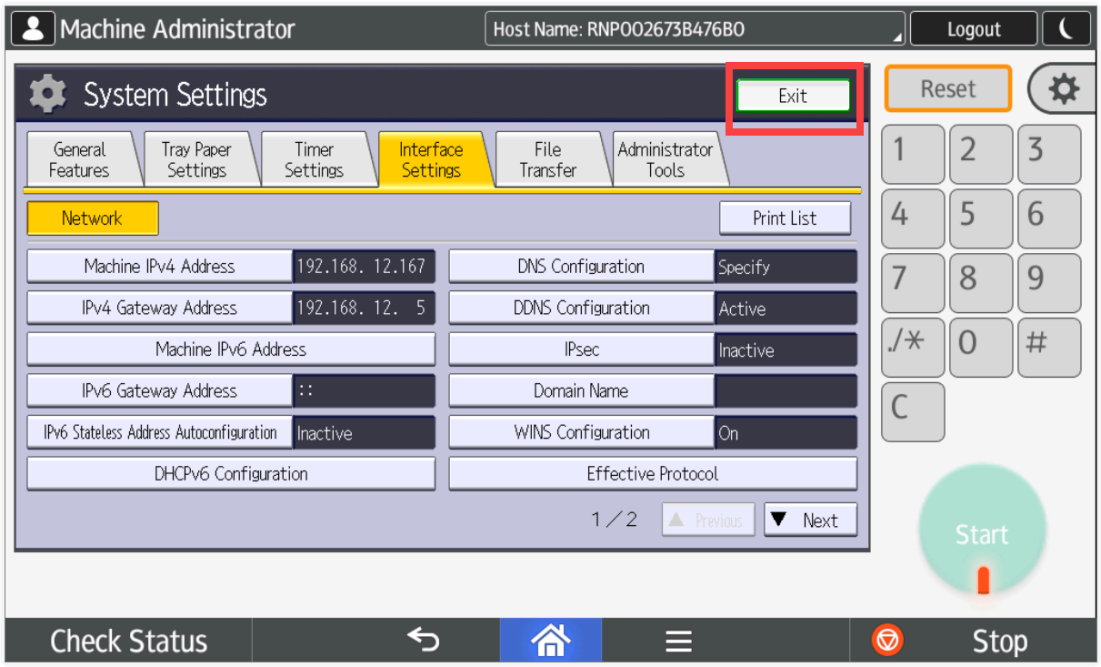
2. When prompted, enter a valid username and password.
3. Choose System Settings and then select Interface Settings tab.



4. Press DNS Configuration
5. Enter the required DNS settings for your network.



6. To apply the settings, press [Exit] button.



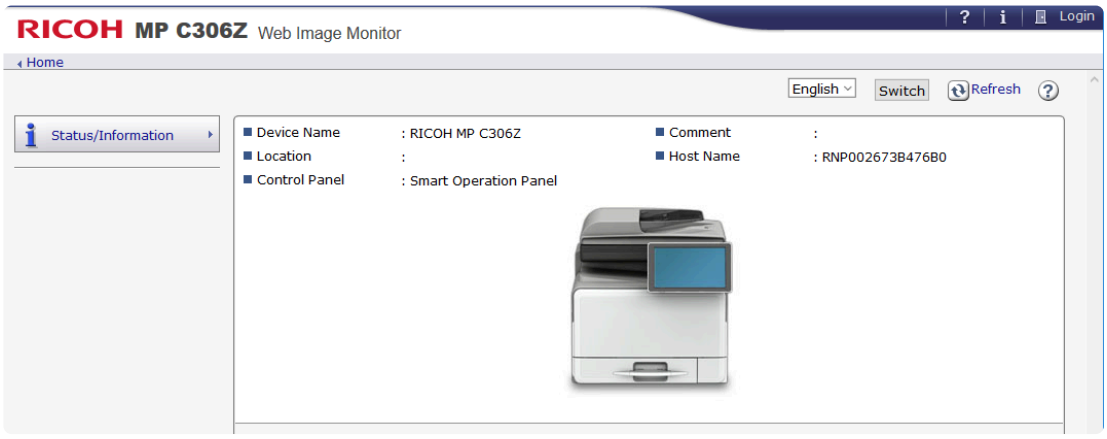
> **Note**: Ensure that Celiveo Web Admin and Ricoh printer are in the same network, i.e. they are connected to the same DNS server and have network accessibility to each other.

3. Configure Ricoh Android printer through Web Image Monitor

Follow these instructions to configure the Ricoh printer through Web Image Monitor.

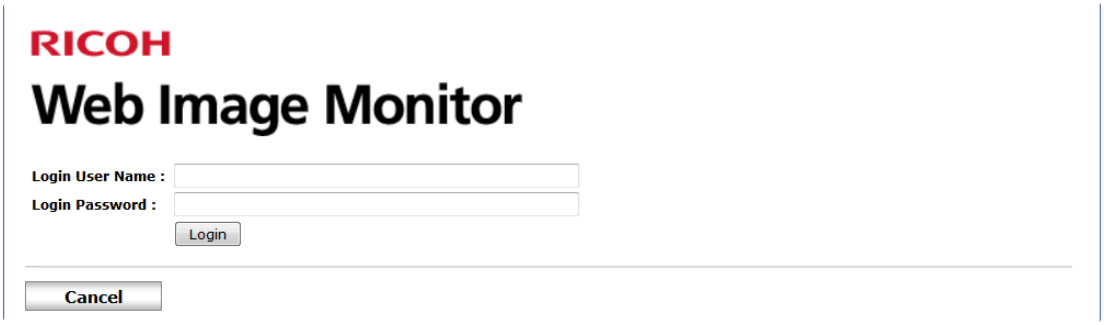
3.1 Login to printer

1. At the web browser, enter the IP address of the Ricoh printer.



2. On the printer home page, click **[Login]**.
3. When prompted, enter a valid administrator username and password.

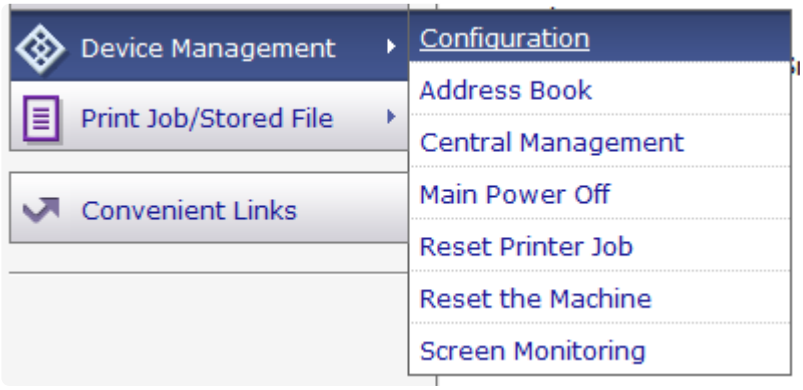
> **Note**: Ensure that the same login credentials are entered when adding the printer in Celiveo Web Admin.



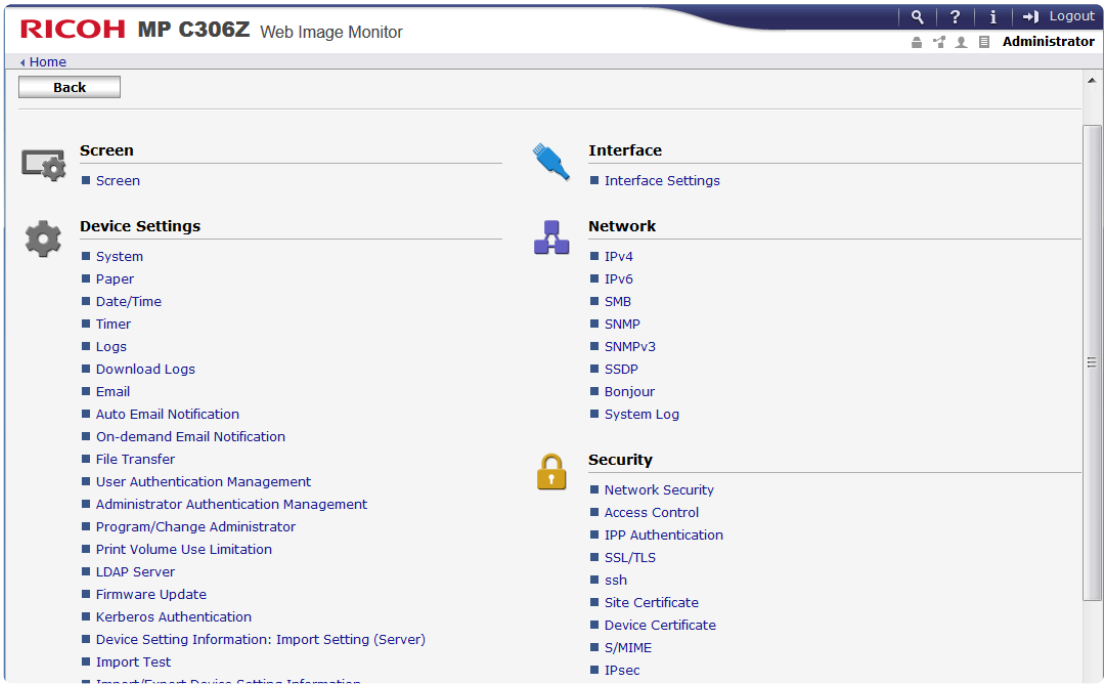
4. Click **[Login]**.

3.2 Enable SSL from Web Image Monitor

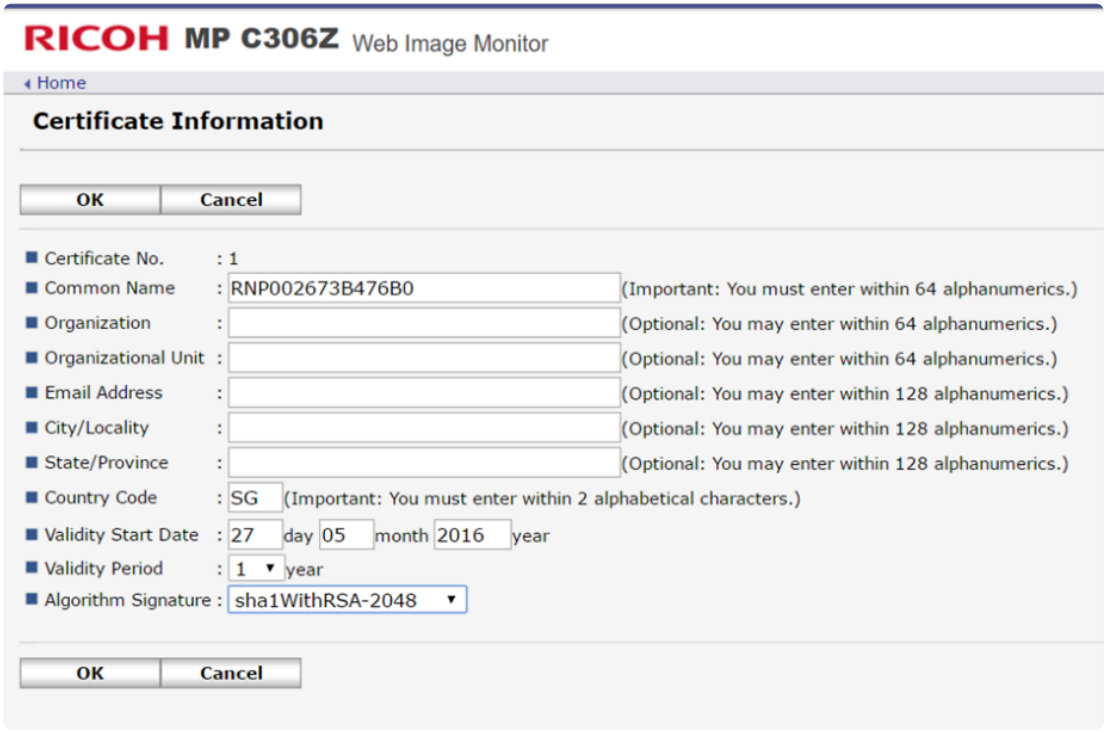
1. Login to the printer's Web Image Monitor.
2. Go to **Device Management > Configuration**.



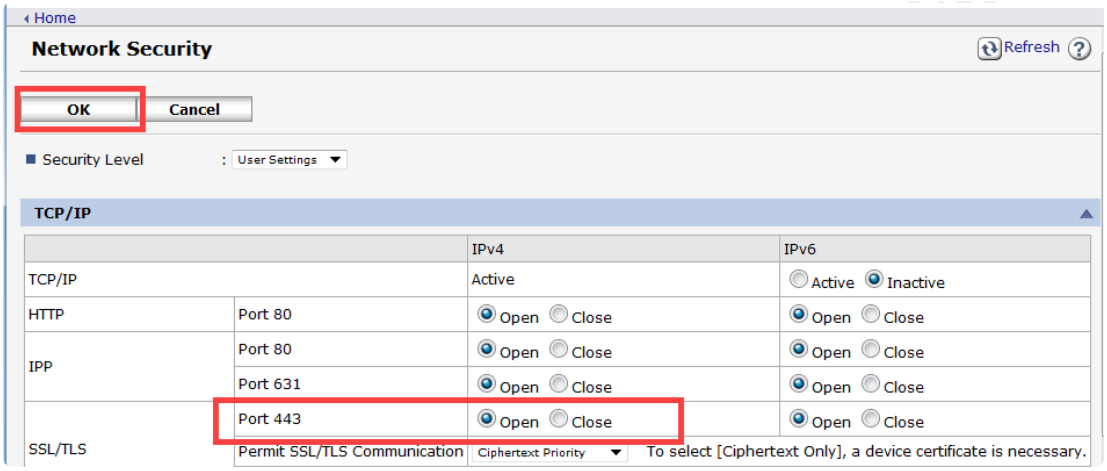
3. To create a device certificate, go to **Security > Device Certificate**.



4. Select the radio button for **Certificate1** and click **Create**.
5. Enter the required information and click **OK**.



6. Click **Home**.
7. Go to **Device Management > Configuration > Network Security**.
8. At **SSL/TLS – Port 443**, select **Open**. Then click **OK**.



4. Connecting Celiveo Authentication Hardware to the Printer device

Celiveo Authentication Hardware refers to the card readers that are used to authenticate users on the device.
These card readers are supported by default; no manual setup is required on the printer:

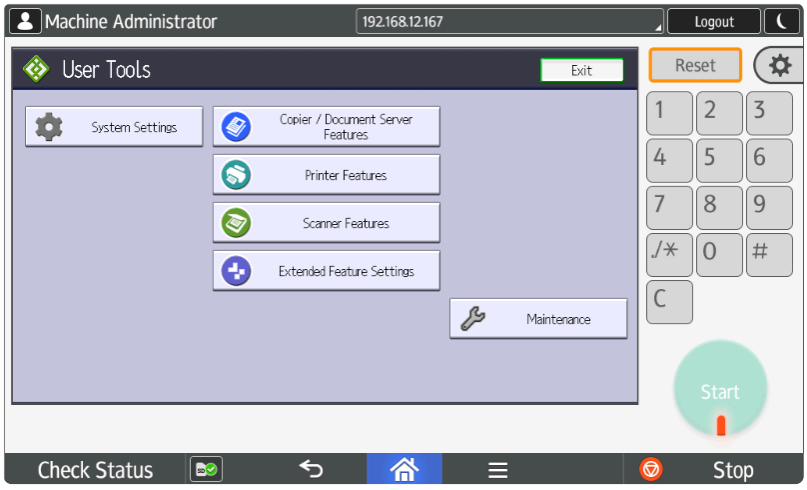
Manufacturer	Model	VID/PID
HID	Omnikey 5427ck	076b/5428
HID		076b/5128
Ricoh supported Reader		0c27/3bfa

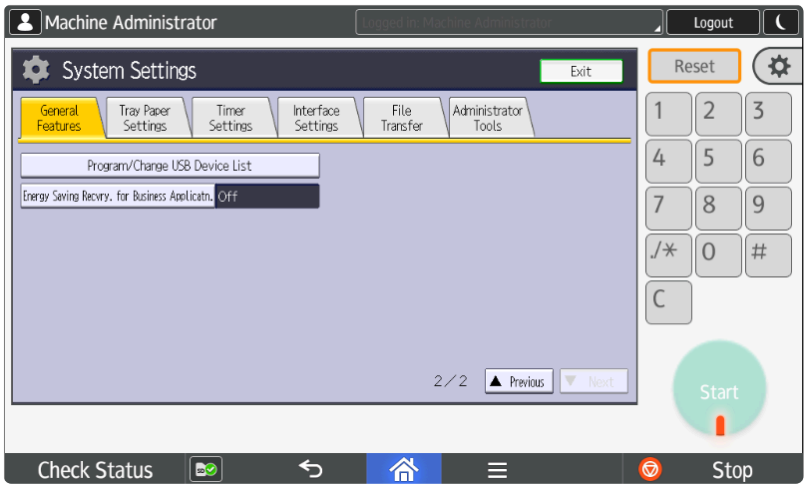
		19e5/0002
		0c27/3b24
		076b/5427
		09D8/0410

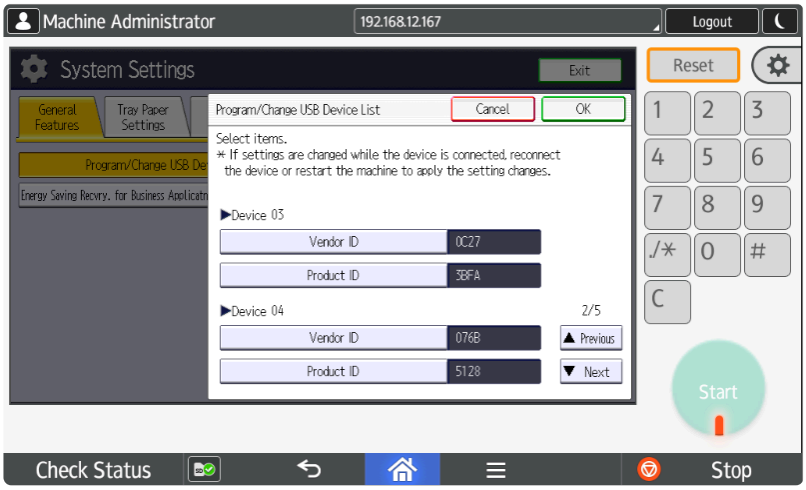
Configuring additional Vendor ID and Product ID at the Printer

Before connecting the Celiveo Authentication Hardware, you need to configure the Vendor ID and Product ID (VID/ PID) at the printer. This is a one-time configuration.

1. At the printer panel, login as Machine Administrator.
2. Go to **System Settings > Program/ Change USB Device List**
3. Select a **Device** item and enter the **Vendor ID** and **Product ID**
4. Click **OK** to save the settings.







Connect to device

The Celiveo Authentication Hardware can be connected the Ricoh Android printer device using the USB or mini-USB port available near the printer panel. Ricoh recommends to use the mini-USB slot to connect card readers to the printer.

To connect Celiveo Authentication Hardware

1. Switch off the device and disconnect the power cable.
2. Locate the mini-USB slot connector.
3. Connect a USB or mini-USB cable from the Celiveo Authentication Hardware to the mini-USB port on the device.
4. Connect the device to the power cable.
5. Switch on the device.

Last modified: 29 September 2022

8.11.4. Xerox

System Requirements

The system requirements for installing Celiveo 8 solution can be found here.

Ports and Communication

A comprehensive list of all the ports used by Celiveo solutions, describing the ports and applications used for communication between the Celiveo components that consist of the Celiveo Server Services, Web Admin Server, Active Directory, Database (SQL) server, the device, and the PC/laptop/workstation can be found here.

Xerox printers use HTTPS protocol for communicating between Celiveo Smart Appliance and printer device.

Prerequisites

Before you install, make sure these prerequisites are met:

- The device is connected to an active LAN connection.
- The device has a fixed IP or DHCP reserved IP address.
- The network allows management by Simple Network Management Protocol (SNMP) v1/v2.
- Enable HTTPS for Xerox secure access.
- For some Xerox devices, enable “Custom services” if it is not an in-built option.
- From the device embedded web services, set the device session time to be longer than the default Celiveo Web Admin inactivity time out (30 sec).
- Xerox devices require (EIP) Extensible Interface Platform 1.5 or higher and (JBA) Job-Based Accounting to run the Celiveo solution.
- The Celiveo Smart Appliance is connected to the device.

With Xerox Altalink C81XX devices, the CSA needs to be upgraded to the latest version of the firmware.

Configuring CSA

By default, the CSA is set in DHCP mode. You can also opt for fixed IP network settings.

The steps to configure CSA for DHCP and for fixed IP network settings can be found here.

Celiveo Version upgrade on CSA

Follow the procedure given here to upgrade the Celiveo Version on CSA.

Configure Xerox WorkCentre devices in CentreWare Internet Services

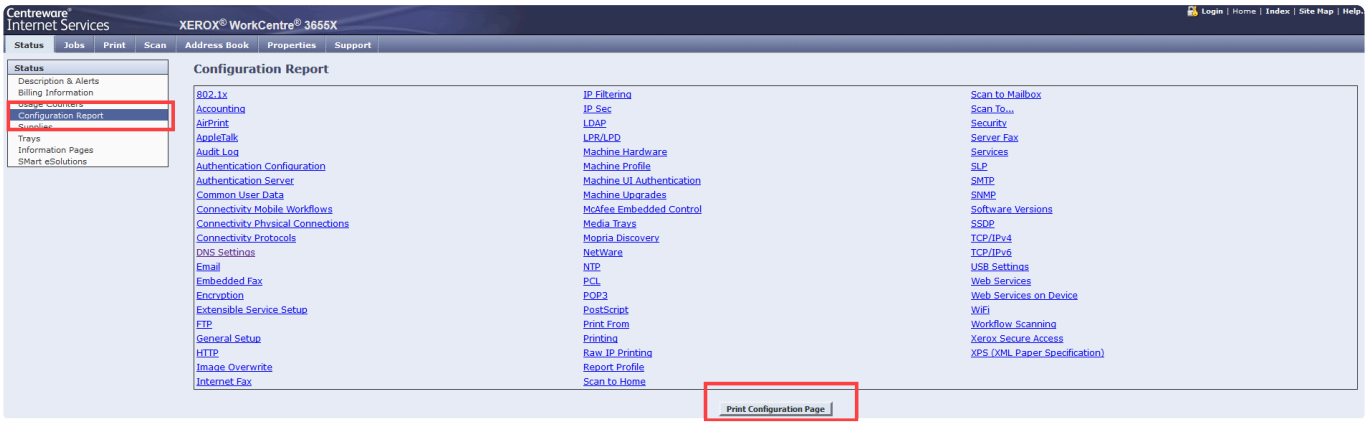
Follow these instructions to configure the Xerox WorkCentre device through CentreWare Internet Services:

1. At the web browser, enter the IP address of the device.
2. Click Login, then enter a valid username and password.

> **Note**: Refer the device manufacturer guide for default login credentials.

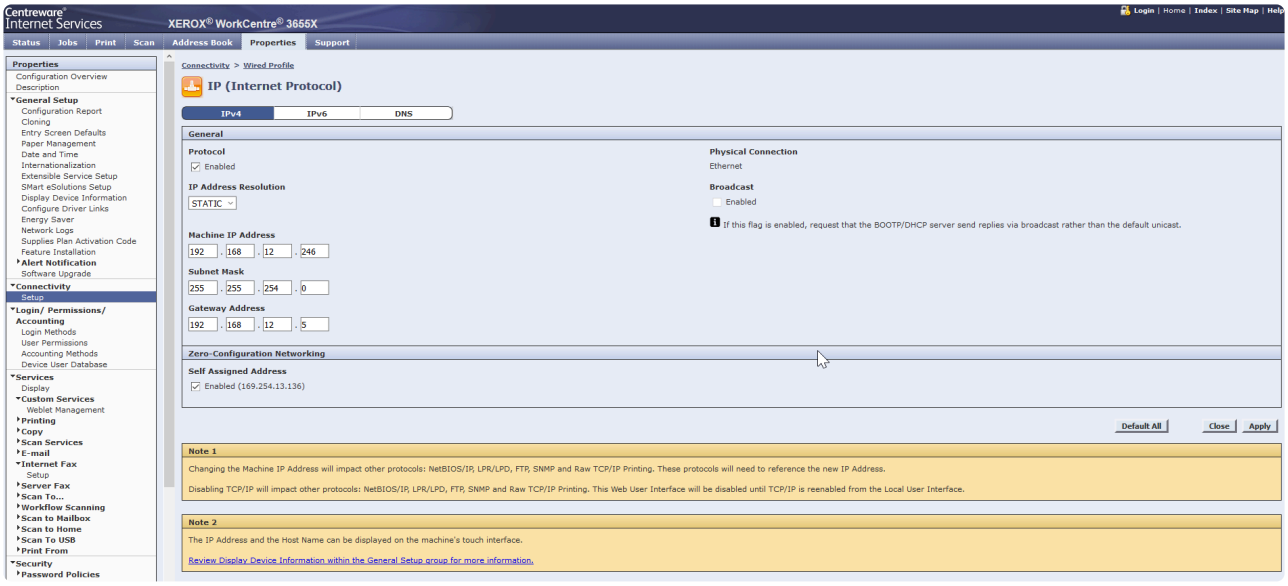
The Celiveo solution automatically configures the settings for the device.

Current device configuration settings are listed on the Configuration Page, and can be printed as a Configuration Report via that web page or the device local user interface.



To manually setup the connectivity settings:

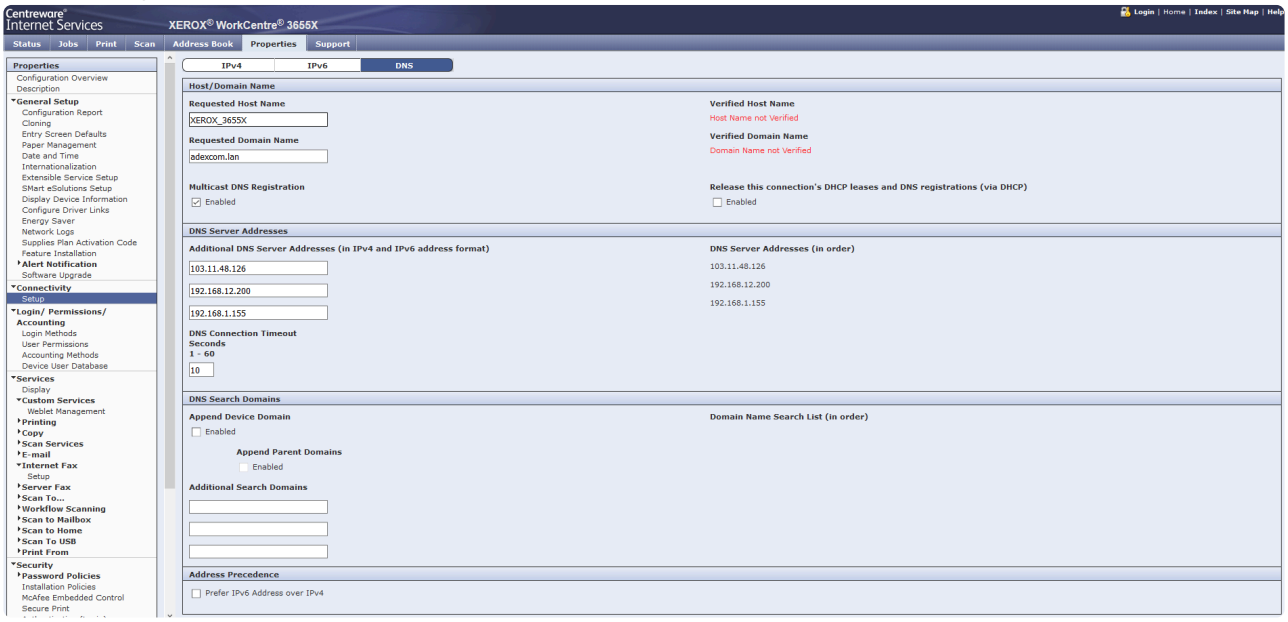
1. Go to **Properties > Connectivity >Setup**
2. Under **Network** section, verify that **Wired connection** profile is selected.
3. Click the **Edit** icon to configure the IP settings for the device.
4. Under the **IPv4** tab, in **General** section, select the **Enabled** checkbox for **Protocol**.
5. Choose the **IP Address Resolution** from the drop down list.
6. Enter the IP address for the device and other details, in case Static IP Resolution is selected. Refer to the image shown below.



7. Click **Apply**.

> **Note**: Changing the IP address will impact the protocols: NetBIOS/IP, LPR/LPD, FTP, SNMP and Raw TCP/IP Printing. These protocols will need to reference to the new IP address.
> Disabling TCP/IP will impact these protocols. The Web user interface will be disabled until the TCP/IP is re-enabled at the device control panel.

1. Similarly, you can configure the settings for IPv6. IPv6 is optional. This may be used in addition to, or in place of IPv4.
2. Select the **DNS** tab. Provide the Host name, Domain name, and DNS server addresses.
3. Click **Apply**.



Memory Clear and Diagnostic Entry

This is an optional procedure. You may follow this process to clear the printer memory and restore the factory settings:

Note: When performing Memory Clear, all the address books and mailboxes stored in the printer will be deleted and the device setting is reset to default.

As precaution, do the following before performing memory clear for the device:

1. Print the following reports:
   - Fax phone book
   - Local and group members e-mail address books.
   - System configuration.
2. To save the printer settings, export the fax address book, local and group email address books and then perform a cloning procedure through Xerox Web interface.

To perform Memory Clear on the device:

1. Select Copier Diagnostics > Memory Clear.
   Selecting Memory Clear will result in the following:
   - Mailboxes to be deleted.
   - Templates to be deleted from the hard disk.
   - NVM values to be reset to default.
   - Fax (if available) to be re-installed.
2. Import the fax address book, local and group email address books, and then install the clone file through Xerox Web interface.

Diagnostic Entry

Note: When the diagnostic mode is entered, all existing copy jobs are cancelled. If the machine is connected to network, the current job will be completed before diagnostic mode is entered. All scheduled jobs will be held in queue due to the machine being offline.

To enter **Diagnostics** mode in Workcenter model printers:

1. Switch on the device.
2. When the device is in the **Ready** state, on the device panel, press and hold **#** key and then press the **Log In/Out key**. The **Diagnostics Entry** screen opens.
3. Enter the password.

Note: Refer to the device manufacturer guide for default password. Press the **C** key to clear an incorrect password entry. Three incorrect entries will cause the screen to lock for three minutes.

4. Select **Start** on the device panel.
   The Diagnostics Screen will be displayed.

To exit from Diagnostics:

1. Select the Close tab on the UI to exit from the dC procedures.
2. Select the Call Closeout button to exit diagnostics.
3. When the Call Closeout window is displayed, the following options are available:
    - Reset All Counters. The default is No. If the Yes button is touched, the following counters are reset:
        - Error Messages.
        - Last 40 Error Messages.
        - Total Images made after the last service call.
        - Exit Only (in 4265)
        - Exit and Reboot (in 4265)
        - Cancel (in 4265)
    - Reboot device. The default is Yes. Image processor, IOT, scanner, UI, DADF and Finisher are rebooted. Touch the **No** button if the device reboot is not needed.

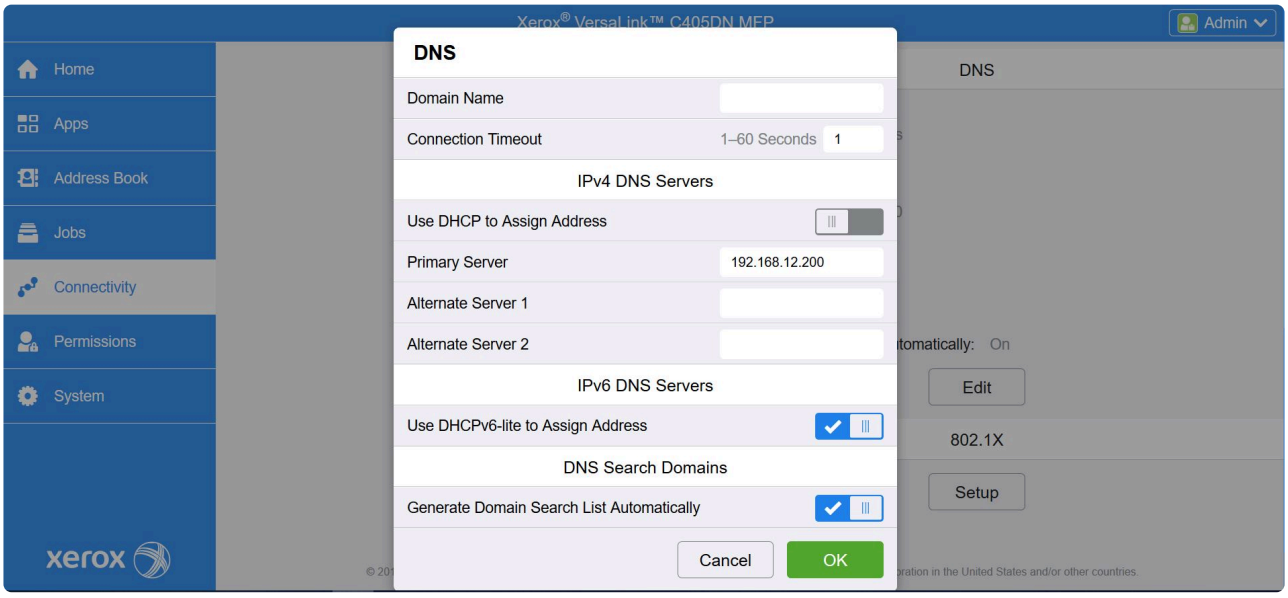
> **Note**: If the device is not rebooted, the exit time from diagnostics is decreased.

Configure Xerox VersaLink Series devices via the Internet Services interface

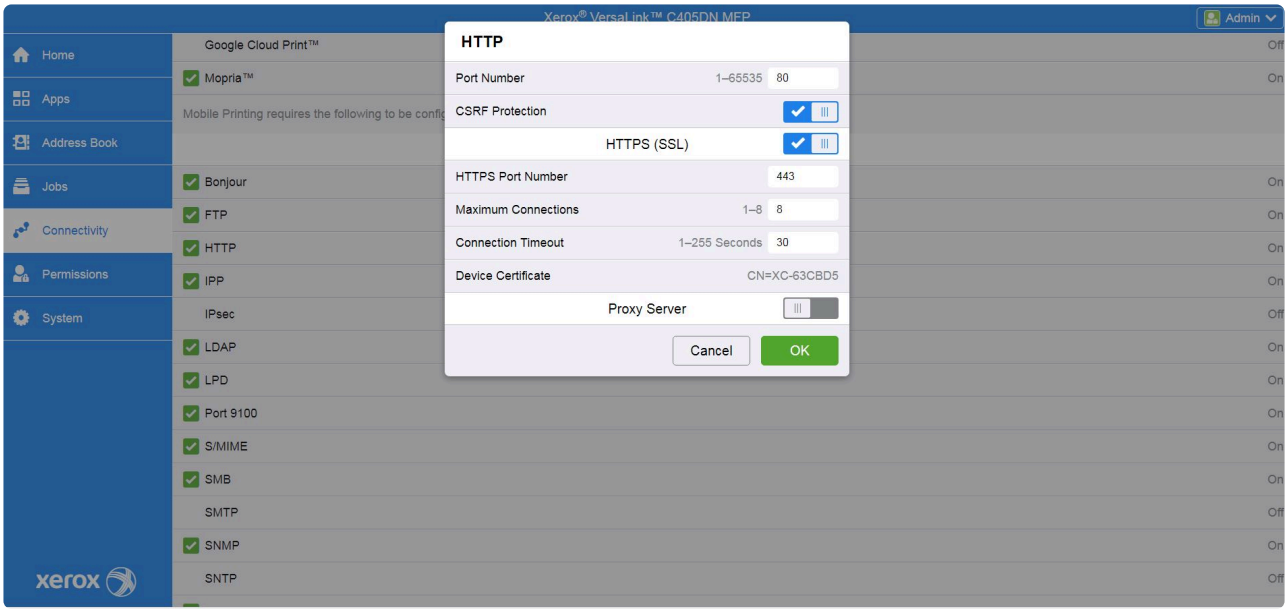
1. Open a Web browser and enter http:// in the Address field
2. Log in with your Administrator credentials

Connectivity Settings

1. On the left panel, select **Connectivity > Ethernet**.
2. In the **DNS** section, select **Edit** to configure DNS settings.

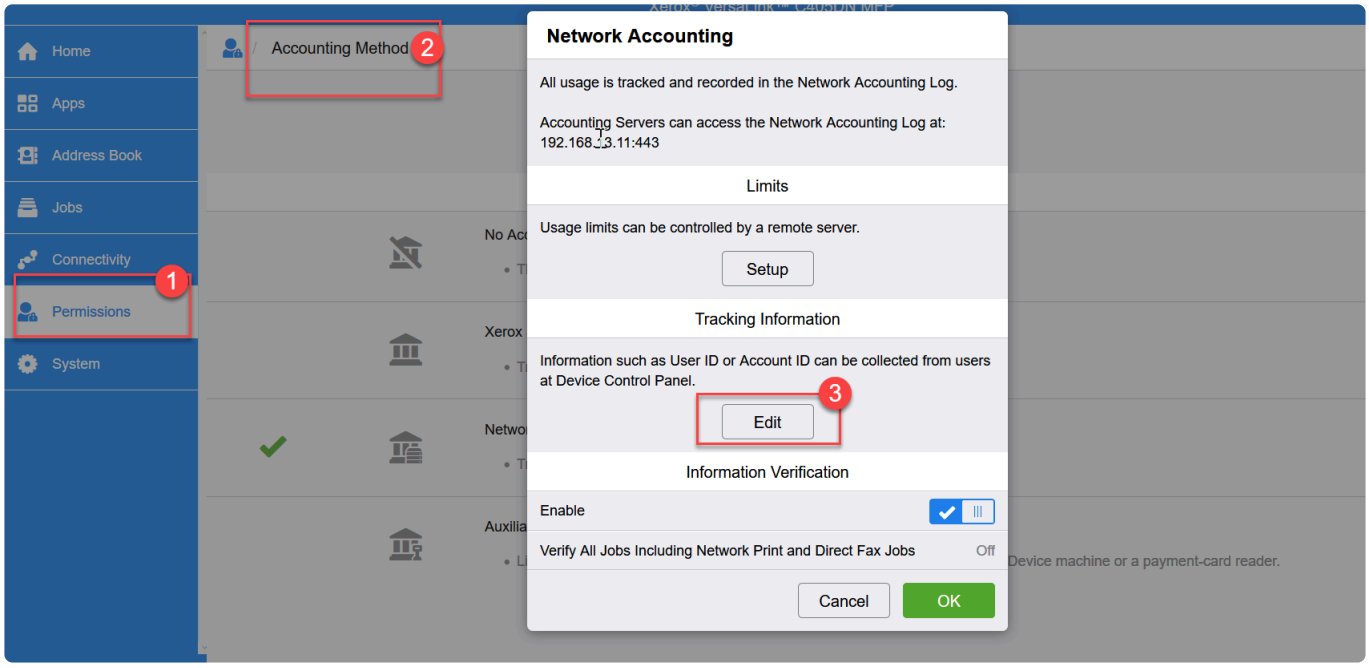


3. Once DNS settings are properly configured, click **OK** and go back to **Connectivity** and in the **Protocols** section, select **HTTP**.
4. Make sure the **HTTPS (SSL)** option is enabled and that the corresponding fields are filled.

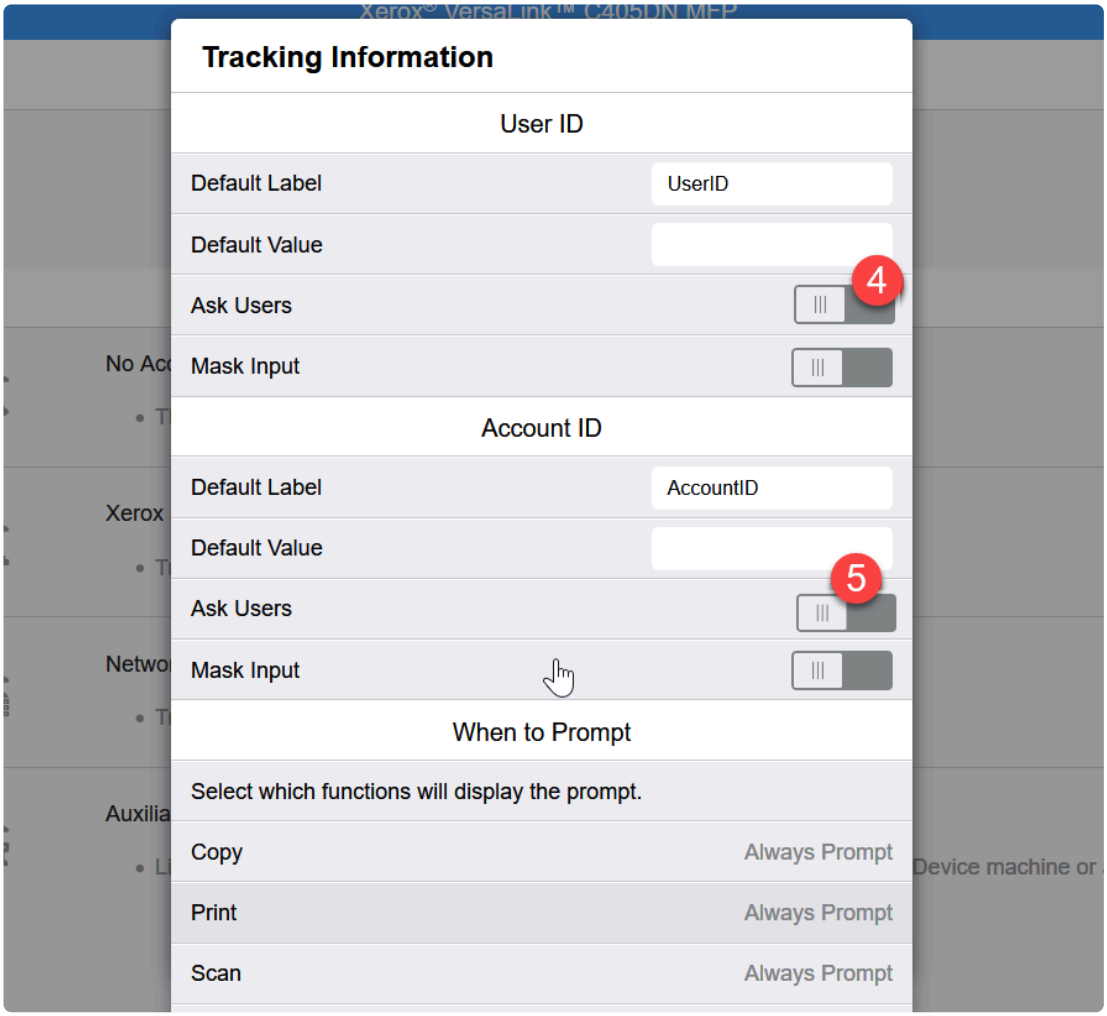


Permissions settings

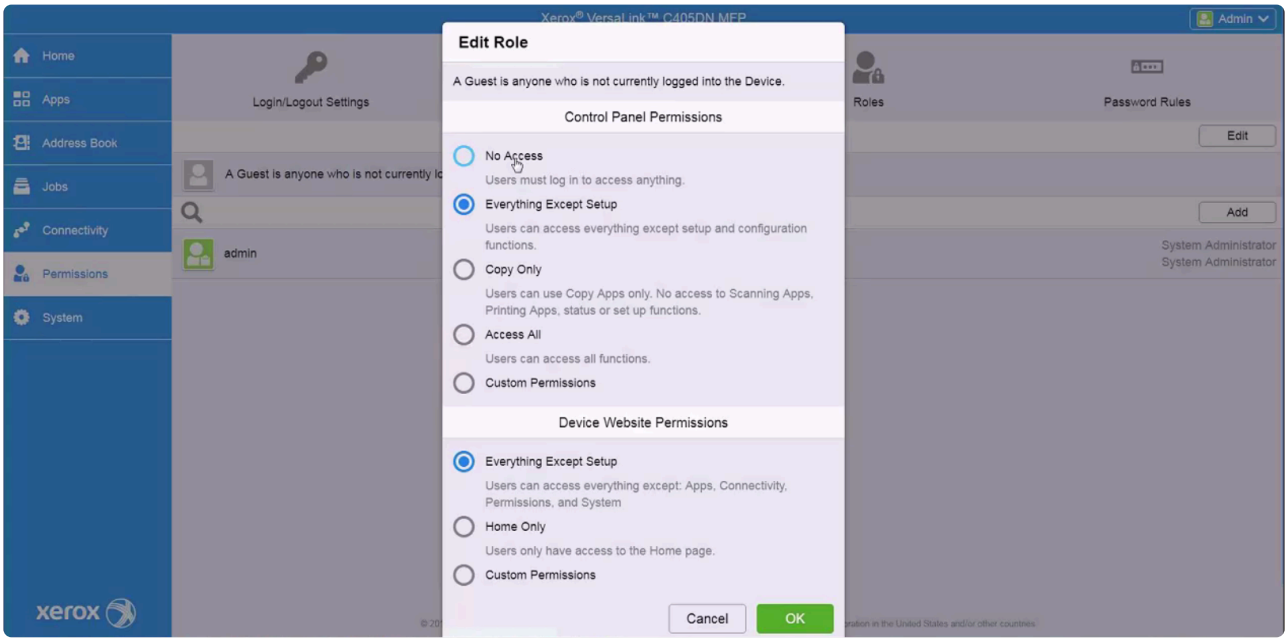
Check that all permission parameters are correctly set:



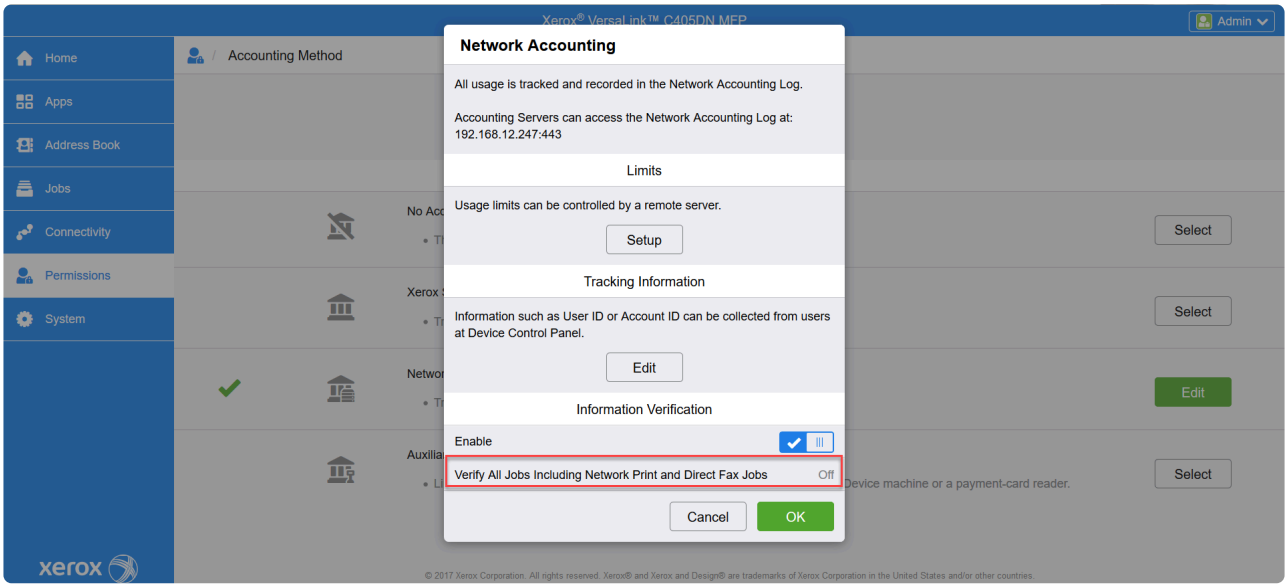
1. Go to **Permissions > Accounting Method** and click the **Edit** button in the **Tracking Information** section.
   Make sure that the **Ask Users** options under **User ID** (4) and **Account ID** (5) are **DISABLED**.



2. In **Permissions**, click the **Edit** button next to **Guest Access** to configure the access permissions to non-authenticated users.



3. Then go to the **Login/Logout Settings** menu and click the **Edit** button below **Advanced Settings**. Make sure the **Obtain User Information on Login** option is enabled.
4. In **Permissions** > **Accounting Method**, click the **Edit** button next to **Network**.

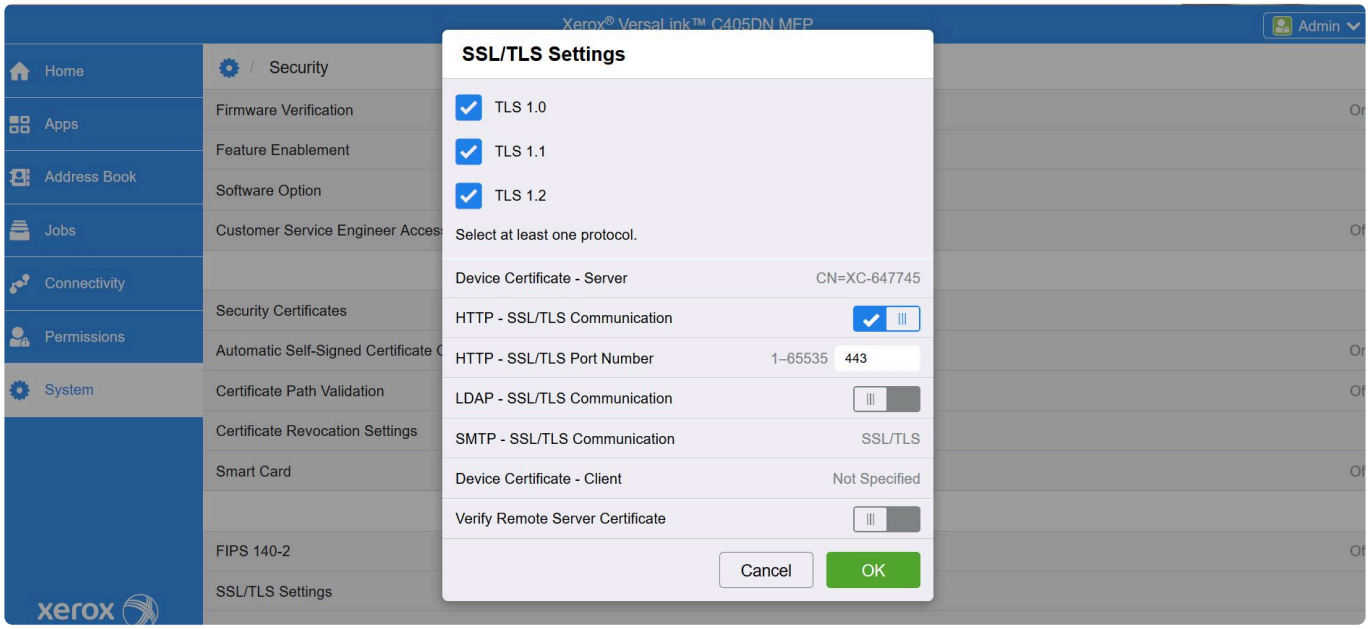


5. Under **Information Verification**, make sure the **Verify All Jobs Including Network Print and Direct Fax Jobs** option is disabled.

> **Attention**: This setting is mandatory. Enabling the **Verify All Jobs Including Network Print and Direct Fax Jobs** would prevent print jobs from being released.

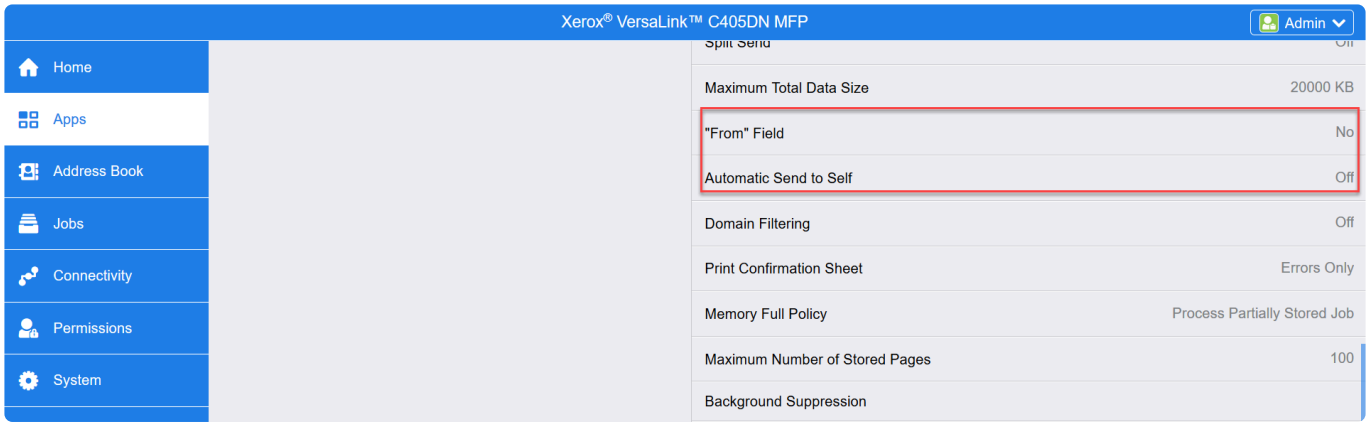
System Settings

In the left menu, select **System > Security > SSL/TLS Settings** then configure the options as shown below:



Scan to Email Settings

In the left menu, select **Apps > Email** and make sure the **“From” Field** and **Automatic Scan to Self** options are disabled.



Resetting the Printer Settings

> **CAUTION** : **Reset to Factory Defaults** erases all settings and returns the printer to the original factory state. All jobs, presets, apps, and device settings are reset. When finished, the printer restarts and the Install Wizard starts to guide you through the setup process.

1. At the printer control panel, log in as administrator, then press the **Home** button.
2. Touch **Device > Resets**.
3. To reset the settings for 802.1X and IPsec, touch Reset 802.1X and IPsec.
4. At the confirmation message, touch **Reset**.
5. To delete all the downloaded fonts, forms, and macros from the printer memory storage, touch **Reset Fonts, Forms, and Macros**.
6. At the confirmation message, touch **Reset**.
7. To reset the printer to factory defaults, touch **Reset to Factory Defaults**.
8. At the confirmation message, touch **Reset**.

Source: *Xerox® VersaLink® Series Multifunction and Single Function Printers System Administrator Guide available at* http://download.support.xerox.com/pub/docs/6510/userdocs/any-os/en_GB/VersaLink_series_sag_en-us.pdf

> **IMPORTANT**: After a factory reset, make sure to change the printer EWS admin password.

Configure Xerox AltaLink Series devices via the Internet Services interface

Xerox Altalink devices do not need any additional configuration. The Default settings should be left as is.

Upgrade OSI from 8.9.022.0302 to 8.9.022.0602

On Xerox VersaLink C405

1. Synchronize the printer with OSI 8.9.022.0302.
2. Authenticate to display the Celiveo icon on the Home page
3. Synchronize the printer with the OSI upgrade from 8.9.022.0302 to 8.9.022.0602
4. Check the Apps on EWS. Only Celiveo should be visible without the My print jobs and Unenroll me buttons.
5. Synchronize the printer again.
6. Wait around 30 seconds. The printer reboots.
7. Authenticate on the printer. The My print jobs and Enroll me icons appear on the Home page.

On Xerox WorkCentre 3655X

1. Synchronize the printer with OSI 8.9.022.0302.
2. Authenticate to display the Celiveo icon on the Home page
3. Synchronize the printer with the OSI upgrade from 8.9.022.0302 to 8.9.022.0602
4. Authenticate on the printer. The Celiveo icon displays on the Home page
5. Delete the printer from the Web Admin.
6. Add the printer again on the Web Admin and synchronize it.
7. Authenticate on the printer. The My print jobs and Enroll me icons appear on the Home page.

Limitations

Some Xerox printer screens do not feature Asian languages fonts and print job names may not appear correctly if they contain such characters.

Last modified: 24 October 2022

8.11.5. HP

This section provides the information regarding the prerequisites, specific settings to be made on the HP device and the configurations to be performed on the device web server page for installation of Celiveo solution.

System Requirements

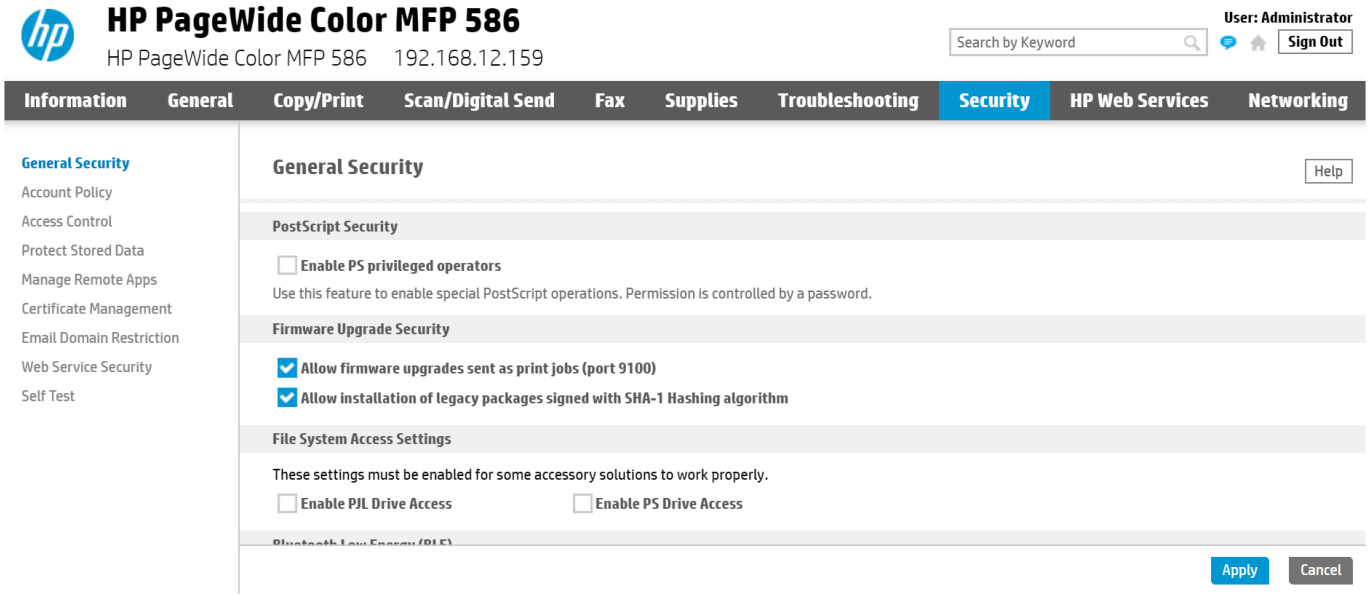
FIRMWARE NOTES – IMPORTANT

Important: Do not use HP Futuresmart firmware 4.9.0.1 on MFPs or 4.10.0.1 on SFPs as some problems have been encountered. You need to use more recent firmware (i.e. 4.10.0 on MFPs) or earlier for SFPs.
Link to HP printers firmware download page: https://support.hp.com/us-en/document/c03933242

4.10 or later

If you are using HP Futuresmart firmware 4.10 or later, you need to disable port 9100 after the synchronization is complete.
This can be done through the EWS:

1. On the Printer panel, in Administrator mode, select **Security** > **General Security** and disable the **Allow firmware upgrades sent as print jobs (port 9100)** option.
2. Click **Apply**.



Compatibility with HP Futuresmart 4.10.0 firmware

HP Futuresmart firmware 4.10.0.1 has a defect on HP Single Functions Printers (SFP) such as the M607/M608/M609.
It loads multiple times solutions instead of just once. This results in corrupted print job data.
This problem and the solution can easily be diagnosed by checking the printer configuration page, where

repeated lines about Celiveo being “Enabled” appear. Solution: downgrade the printer firmware to a version earlier than 4.10.0.1, or upgrade the firmware when HP releases a fix.

4.9.0.1

Do not use HP Futuresmart firmware 4.9.0.1 as some problems have been encountered.
You need to stay with a 4.8.x.x firmware or earlier until a 4.9.x.x is released, that fully support added solutions.

Crash 49.38.13 with HP Futuresmart firmware releases between 4.11.0.2 and Futuresmart 5.1
Some random crash 49.38.13 may happen when Celiveo is installed in the printer equipped with such firmware.
The issue is fixed with the HP Futuresmart 5.2 firmware release.
If your HP printer does not have Futuresmart 5.2 available, we recommend you used Futuresmart 4.11.0.1.

5.2
IMPORTANT: The Celiveo HP Modern solution is not compatible with the HP Firmware 5.2.

The system requirements for installing Celiveo 8 solution can be found here.

Recommended driver

Recommended driver for Windows:
HP Smart Universal Printing Driver for Windows V3 (64-bit) More information

Ports and Communication

A comprehensive list of all the ports used by Celiveo solutions, describing the ports and applications used for communication between the Celiveo components that consist of the Celiveo Server Services, Web Admin Server, Active Directory, Database (SQL) server, the device, and the PC/laptop/workstation can be found here.

HP Printers use HTTPS protocol for communicating between Celiveo Smart Appliance and the printer device.

Prerequisites

Before you install, make sure these prerequisites are met:

- The device is connected to an active LAN connection.
- The device has a fixed IP or DHCP reserved IP address.
- The network allows management by Simple Network Management Protocol (SNMP) v1/v2.
- From the device Embedded Web Services (EWS) page, set the device session time to be longer than the default Celiveo Web Admin inactivity time out (30 sec).

Configuring CSA

> **Note**: This configuration is necessary for HP printers that do not belong to FutureSmart category.

By default, the CSA is set in DHCP mode. You can also opt for fixed IP network settings.

The steps to configure CSA for DHCP and for fixed IP network settings can be found here.

Celiveo Version upgrade on CSA

Follow the procedure given here to upgrade the Celiveo Version on CSA.

Limitations

HP PageWide Pro and HP OfficeJet Pro models are only supported for ID to Print All.

For print jobs stored on the printer HDD (secure push printing) the “Print B&W” and printer print rules do not apply as of today.

Push Printing

In Push Printing, jobs are sent to the device for authentication and release. Push Printing is convenient as it makes a powerful serverless secure printing solution. On the other hand, the limited hard disk drive capacity on a device can be an issue as compared to that of a server, if large jobs are to be retained. The print jobs can also be released only from the device where they are stored.

Push Printing is supported on HP devices with a hard disk drive, and a minimum disk space of 30GB. The Push Printing feature is not supported on CM8050 and CM8060 multi-function printers. Printers must have storage media (HDD, USB stick) with 50MB free, and an active TCP-IP LAN connection.

A special driver plug-in to benefit from the Secure Push Printing feature is available in the Downloads section.

HP Printer Setup

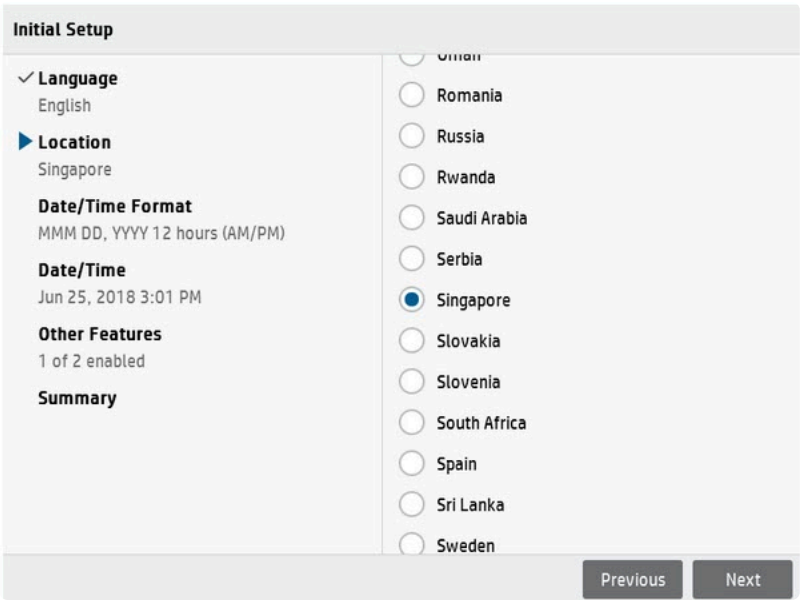
1. Configuring Settings on the Device

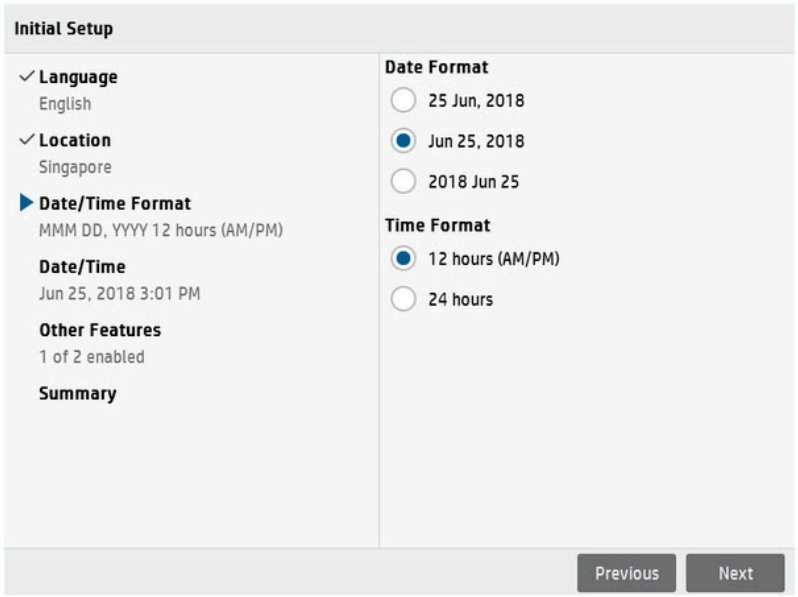
On initializing the HP printer, the date and time, location, and language need to be set for the device. This is done through the device’s control panel.

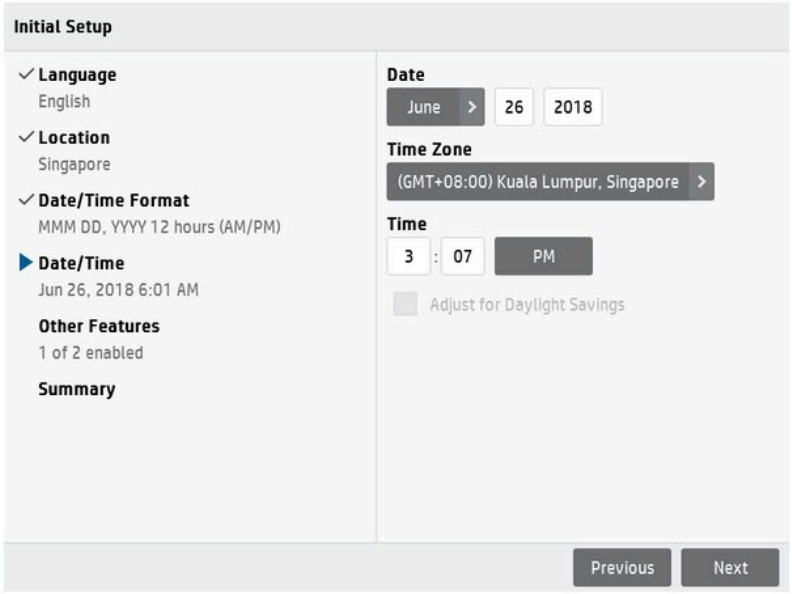
To configure initial setup for the device:

1. When the printer completes its initial boot up, the **Initial setup** screen is displayed on the device control panel. Select appropriate values for the following attributes on the screen:

- Language
- Location
- Date/Time Format
- Date/Time







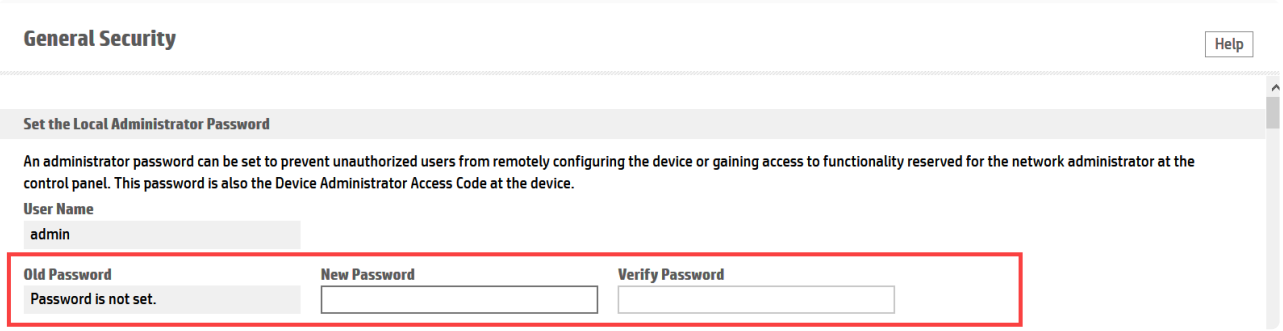
2. Press **Finish** to apply the settings.

2. Setting up Printer Administrator credentials

Administrator password is set to prevent unauthorized users from remotely configuring the device or gaining access to functionality reserved for the network administrator at the control panel. This password acts as the Device Administrator Access Code at the device.

To set password for Administrator:

1. In the browser address bar, enter the following URL by replacing the text in bold typeface with the IP address of the HP device: https://*{device IP address}*/hp/device/DeviceStatus/Index.
   The device EWS page opens.
2. Go to **Security** tab and select **General Security**.
3. The user name is predefined here. Set the password for the Admin user and click **Apply**.



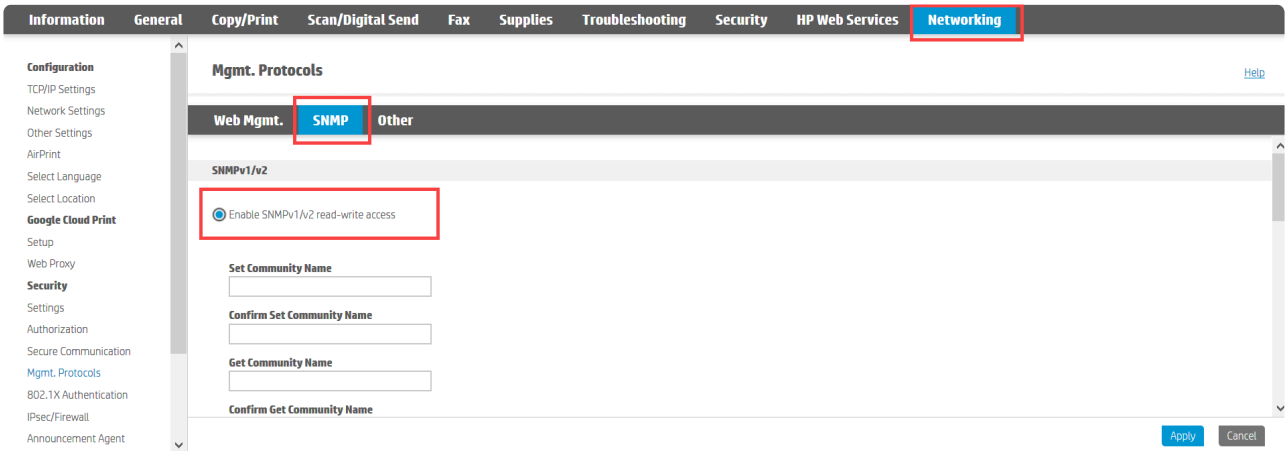
3. Configuring SNMP and Network Settings

The SNMP and network settings can be configured for the printing device using the device EWS page.

To enable SNMP:

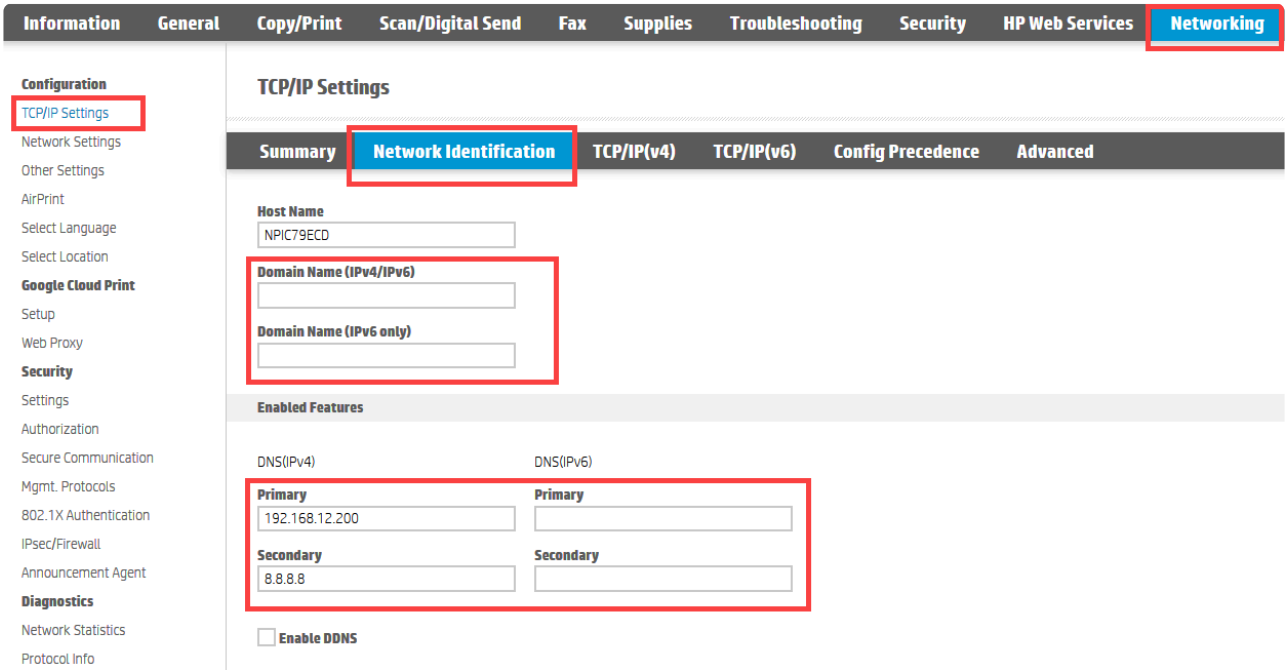
1. Log in to the EWS page of the device.
2. Go to **Networking** tab and select **Mgmt. Protocols** on the left menu.

3. Select **SNMP** tab.
4. Select **Enable SNMPv1/v2 read-write access** option.
5. You can also configure the Community Name. By default, the Community Name is set to 'public'.



To configure the Network setting:

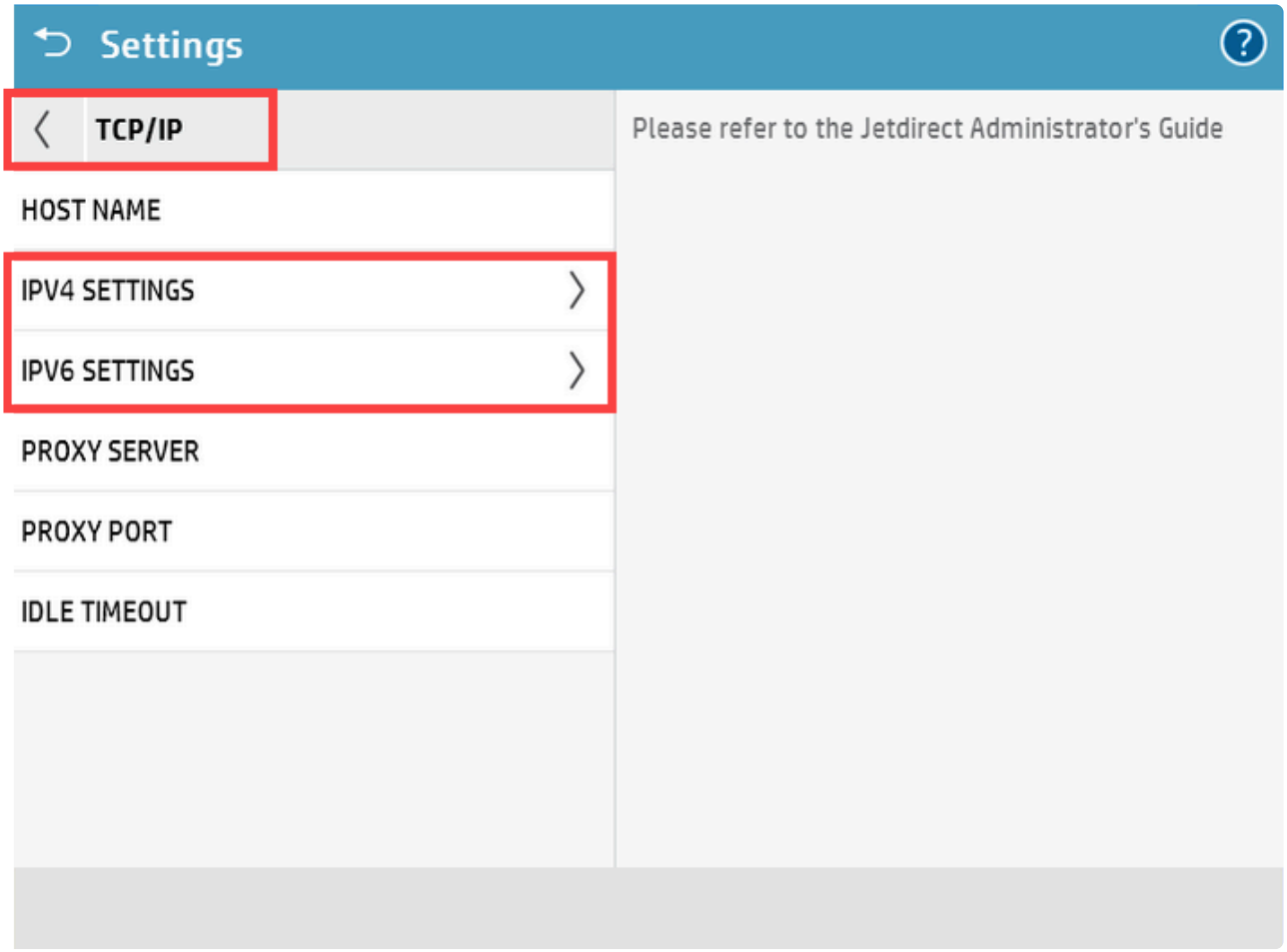
1. Under **Networking** tab, go to **TCP/ IP Settings > Network Identification** tab.
2. Set the **Domain** name and **DNS** for the device. Click **Apply**.



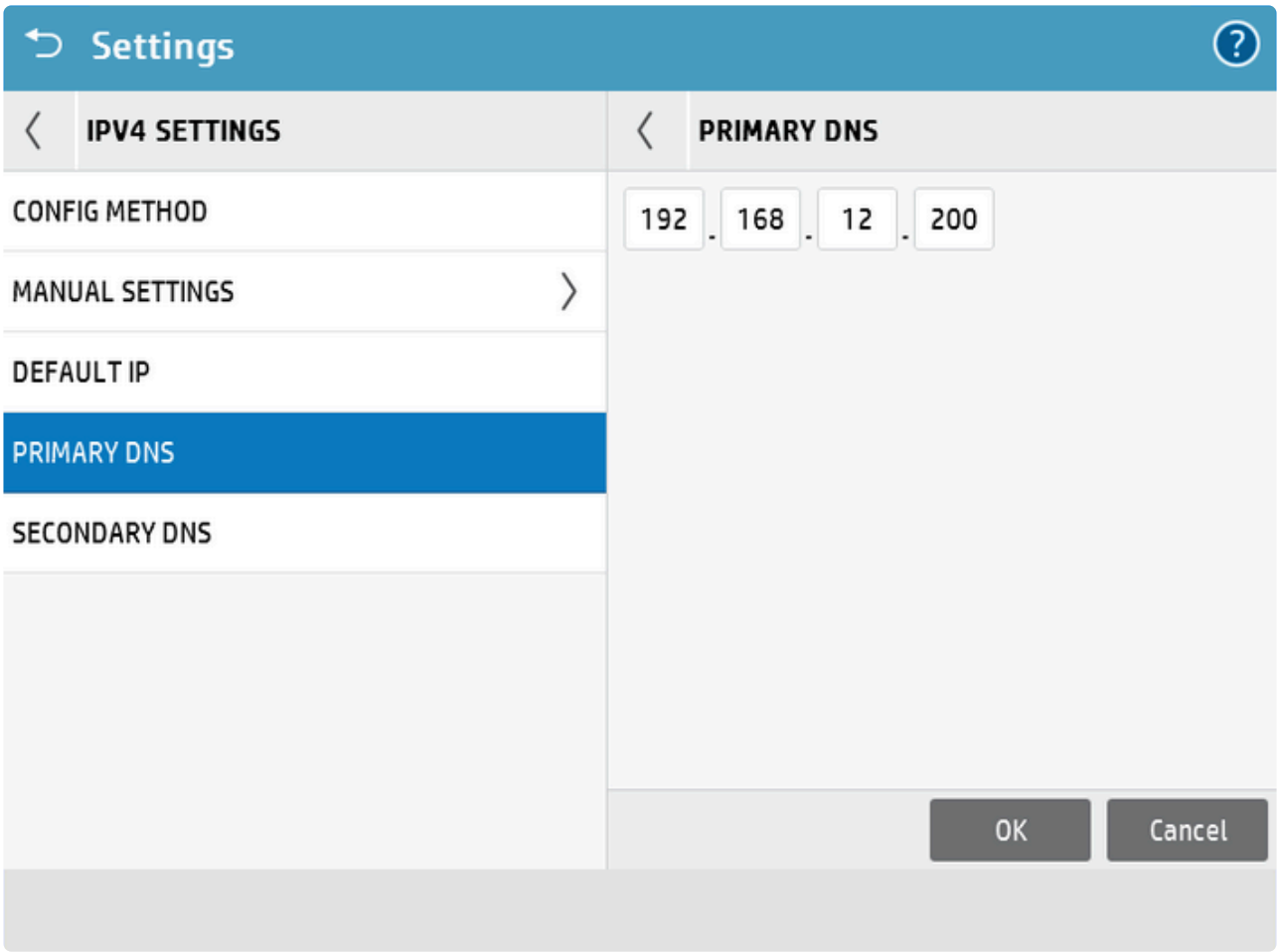
You can also configure the network settings using the device control panel.

To set the network configuration through device panel:

1. On the device control panel, press **Settings > Networking > Ethernet > TCP/IP**
2. Select appropriate IP settings (IPV4 or IPV6) to configure.



3. Enter the **Primary DNS** and **Secondary DNS** for the selected IP settings.
4. Press **OK**.



More Information:

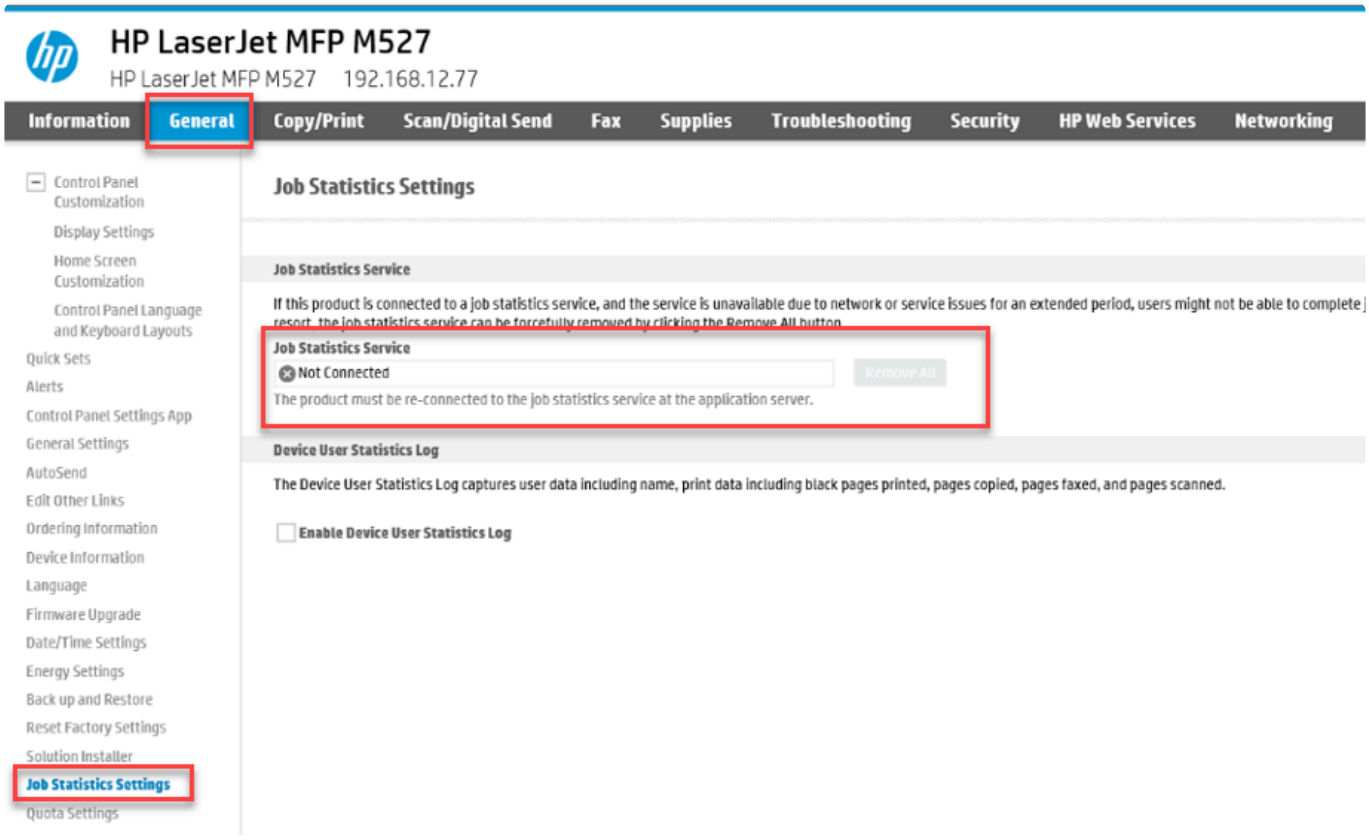
Configuring Scan to Email/ Scan to Sharepoint for Office365 account

For users using Office 365 account, HP provides instructions on how to configure the cloud-based Microsoft Office 365 Outlook email system on HP LaserJet Enterprise/ HP PageWide Enterprise (with firmware version 3.4 and newer) MFPs for **Scan to Email/ Scan to Sharepoint** options.

Follow the steps provided here: https://support.hp.com/in-en/document/c05920994

Note regarding the Jobs Statistics Service:

Celiveo Embedded Agent registers the Tracking service as a non-critical service so it would not appear on the below Jobs Statistics Service:



Last modified: 29 September 2022

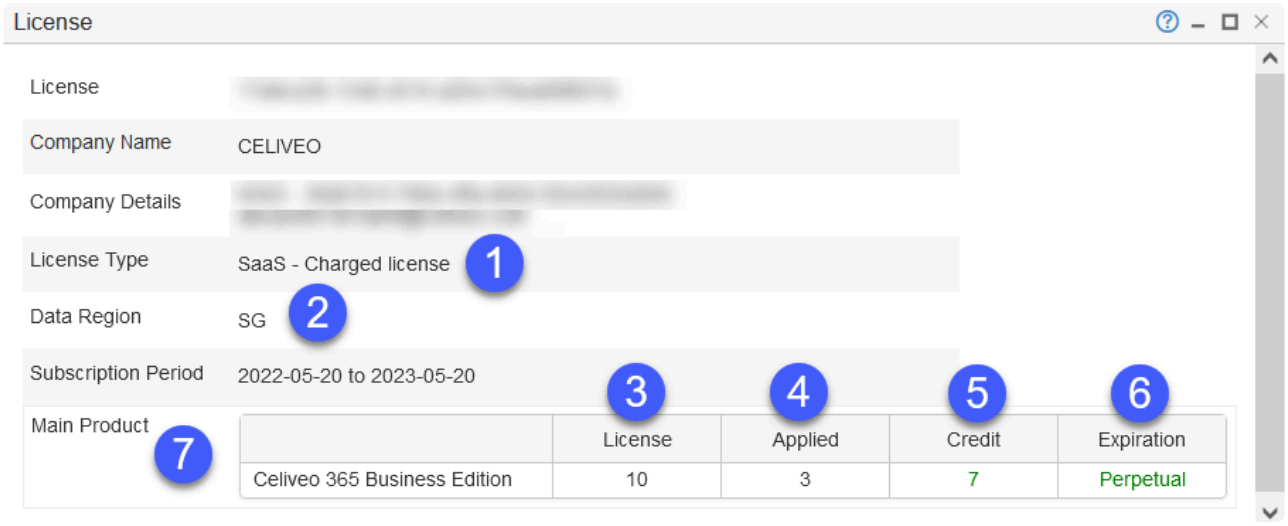
8.12. Viewing and Updating Your Celiveo License

The license defines what features you are authorized to use, and how many printers you can use them on. When you install the Web Admin on a Server for the very first time, you receive a trail. The trial license provides the features of Celiveo Business for 10 printers for a period of 30 days. You can upgrade your trail license to a full license by uploading a license file, which your Celiveo representative will provide.

If you upgrade your license to have more features or to support more printers, you will be provided with another license file. You upload the license file on top of your existing license and your license upgrades.

To check details of your license

1. Start and Login to the Web Admin.
2. On the Home tab, click . The License details display.



Legend

1 - Indicates how many licenses have been purchased
2 - Indicates how many licenses are in use. Each Celiveo enabled printer consumes one license.
3 - Indicates how many licenses are remaining.
4 - Identifies the edition of Celiveo you have purchased.
5 - Identifies the optional add-ons you have purchased (on top of the main product).

To Upload a License File

1. Start and Login to the Web Admin.
2. On the Home tab, click . The License details display.
3. Click the **[Upload License]** button.
4. Click **[Select Files]** and select the license file (*.*lic*) provided by your Celiveo Representative.
5. Click **[Upload]**. The file uploads, and the license details update.

Note: If you upgraded your license, you must sync all physical printers for the upgrade to take effect.

What if I purchase a Connector License later?

If you purchase an optional connector after you have installed and licensed your main Celiveo Product, Celiveo will provide you another license file. You can upload the new license file on top of your existing license. This license will unlock the feature you purchased, on top of your existing list of features.

Note: Before purchasing an optional connector, check with your Celiveo representative if the Celiveo edition you are using supports the desired connector.

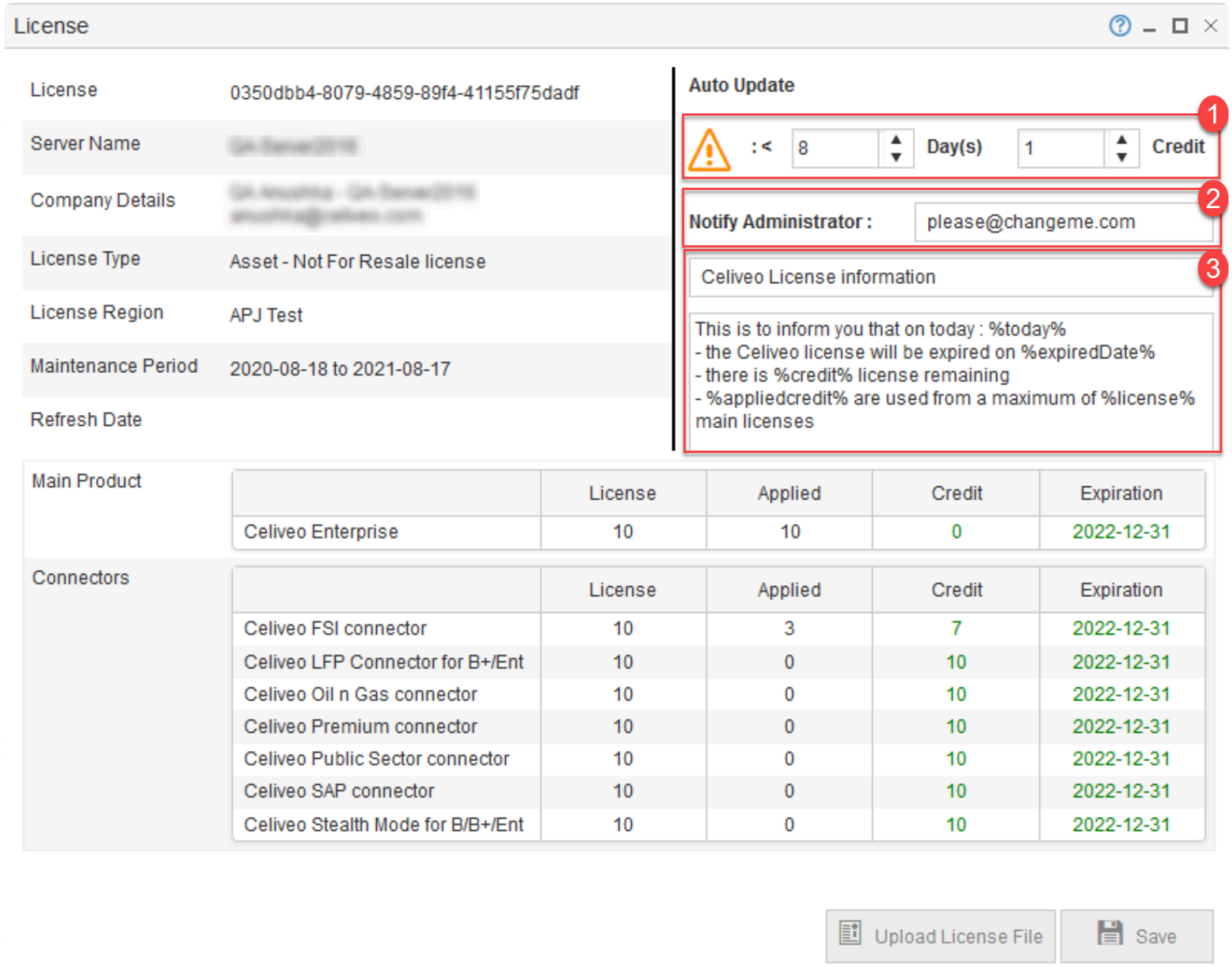
What information must I provide Celiveo to generate a license file for me?

Your Celiveo representative may ask for details pertaining to your account. Additionally, you must provide the host name of the server that Web Admin runs on.

Automatic License Update

The Celiveo Web Admin can automatically get updated from Azure, where the licenses are kept, so that it never stops, without any administrator work. Clients without Internet access will not benefit from that feature.

Configure Automatic License Update



1. Using the arrows, define the number of days or credits that will trigger the warning email to the administrator.
   If the license type is RENTAL, the number of days cannot be changed.
2. Enter the administrator's email address.
3. (Optional) Customize the text that will be sent to administrator. Please do not change the variables.

Manual Update

To manually update your license, click the **Refresh** button.

Last modified: 29 September 2022

9. SAP Connector Configuration

Configuration on TLS 1.2 disabled environments

By default, the Celiveo Print-ERP Unified Print Queue is supporting TLS1.2. If the environment is not supporting TLS1.2, follow the steps below:

1. Navigate to *C:\Program Files\Celiveo\Celiveo Print-ERP Unified Print Queue\Celiveo Print-ERP Communication Server\conf*.
2. Open the **server.xml** file.
3. Remove **protocols=”TLS1.2** and save the file.

Before Removal

```
<SSLHostConfig clientAuth="false" sslProtocol="TLS" protocols="TLSv1.2">
```

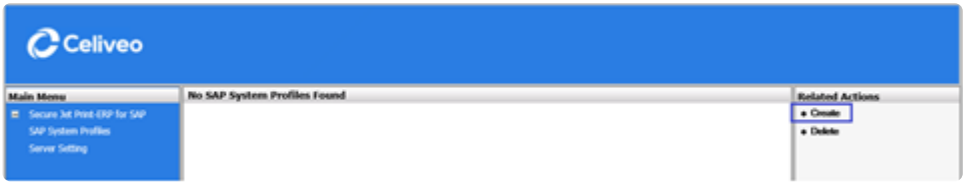
After Removal

```
<SSLHostConfig clientAuth="false" sslProtocol="TLS" >
```

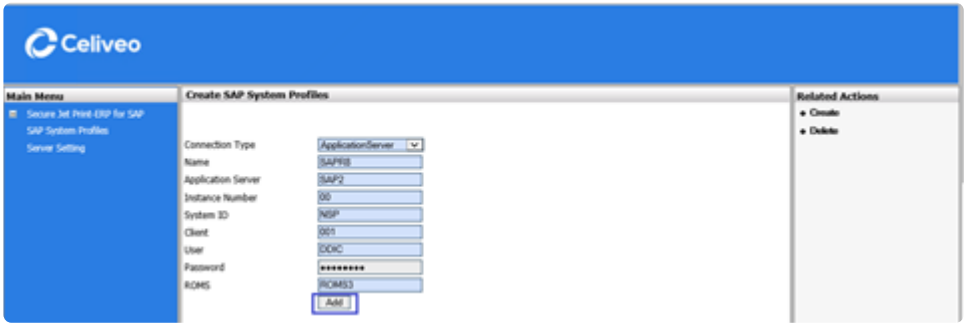
4. Open the Windows services and Restart the **Celiveo Print-ERP Communication Server** Service

Configure the sapconfig-ui utility

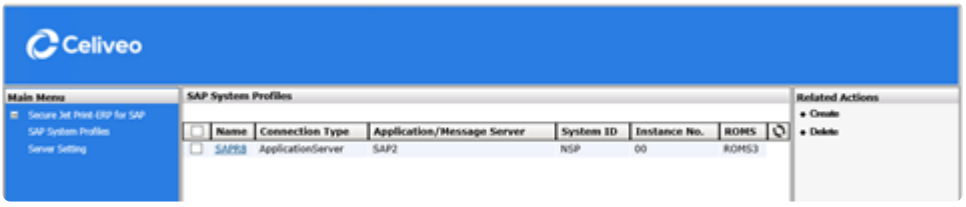
1. Navigate to “https://[IP_ADDRESS]:8443/sapconfig-ui/”
IP_ADDRESS = Existing server IP where the Celiveo Print-ERP Unified Print Queue is installed.
2. Click **Create**.



3. Fill in all the details as in the backup configuration and click **Add**



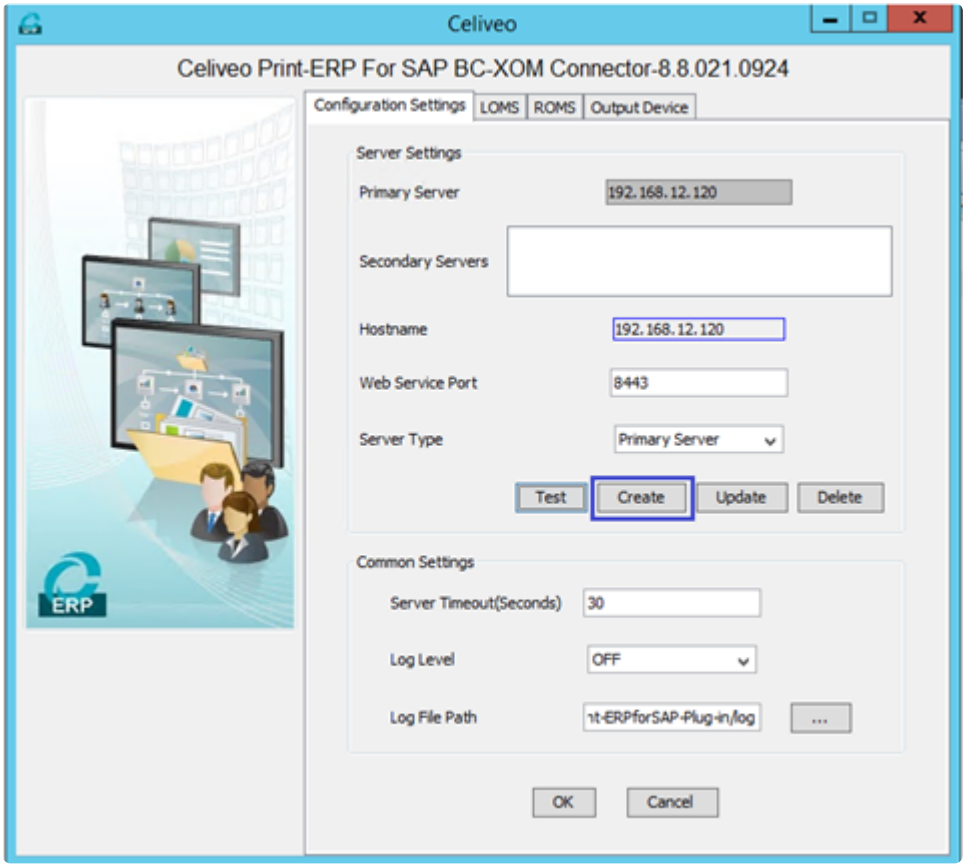
4. The profile is added under **SAP System Profiles**



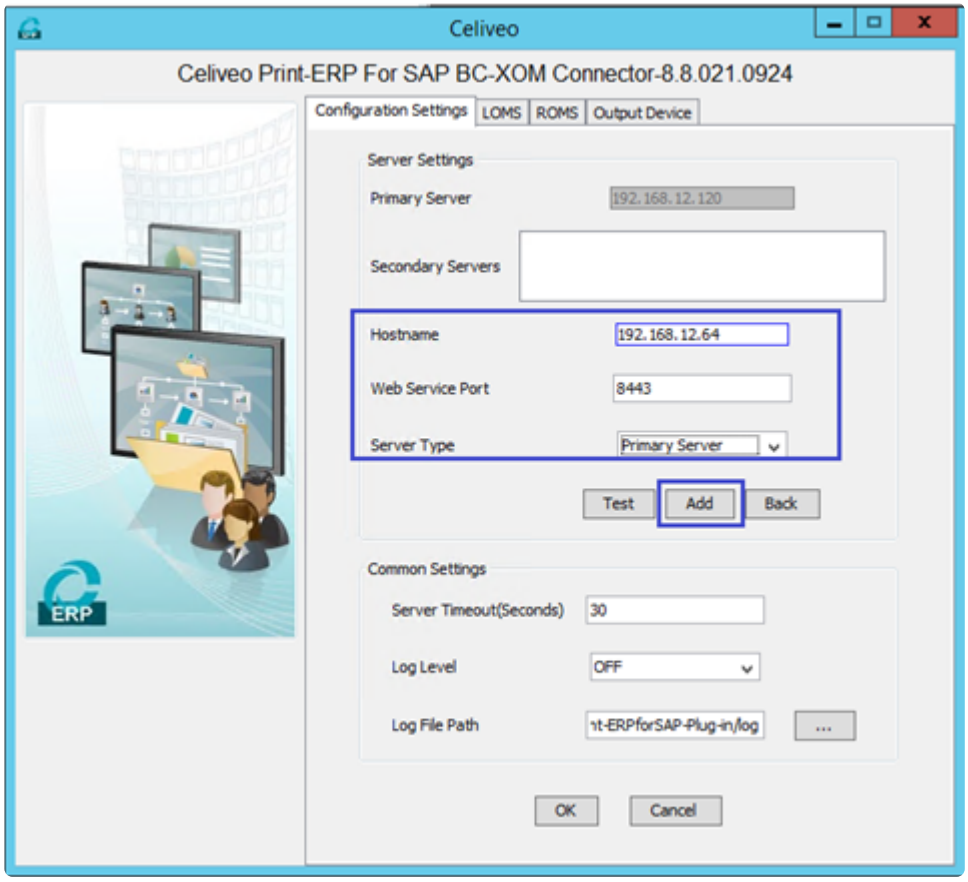
Configure the Celiveo BC_XOM Connector to point the Celiveo 8 Server

> Note: If you use the current Celiveo 8.0.x version, you will see your Celiveo 8.0.x server configurations as the primary server. If you install the new Celiveo 8 connector, you will not see any configurations after installing it.

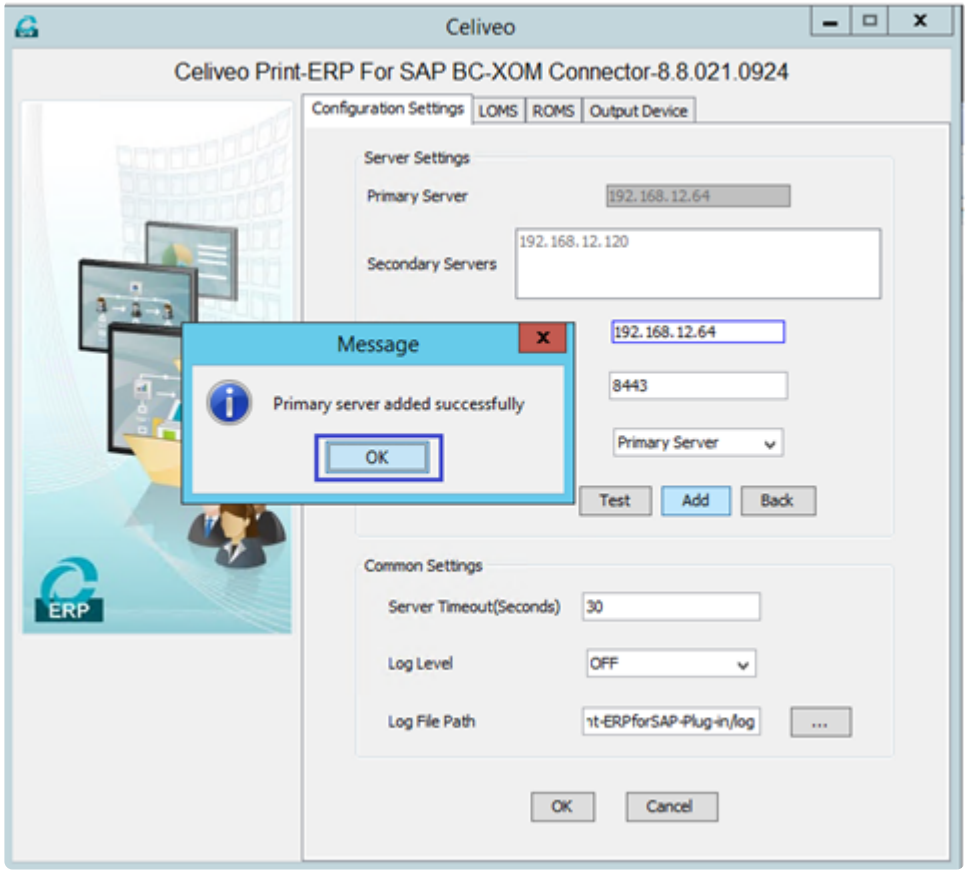
1. Click **Create**.



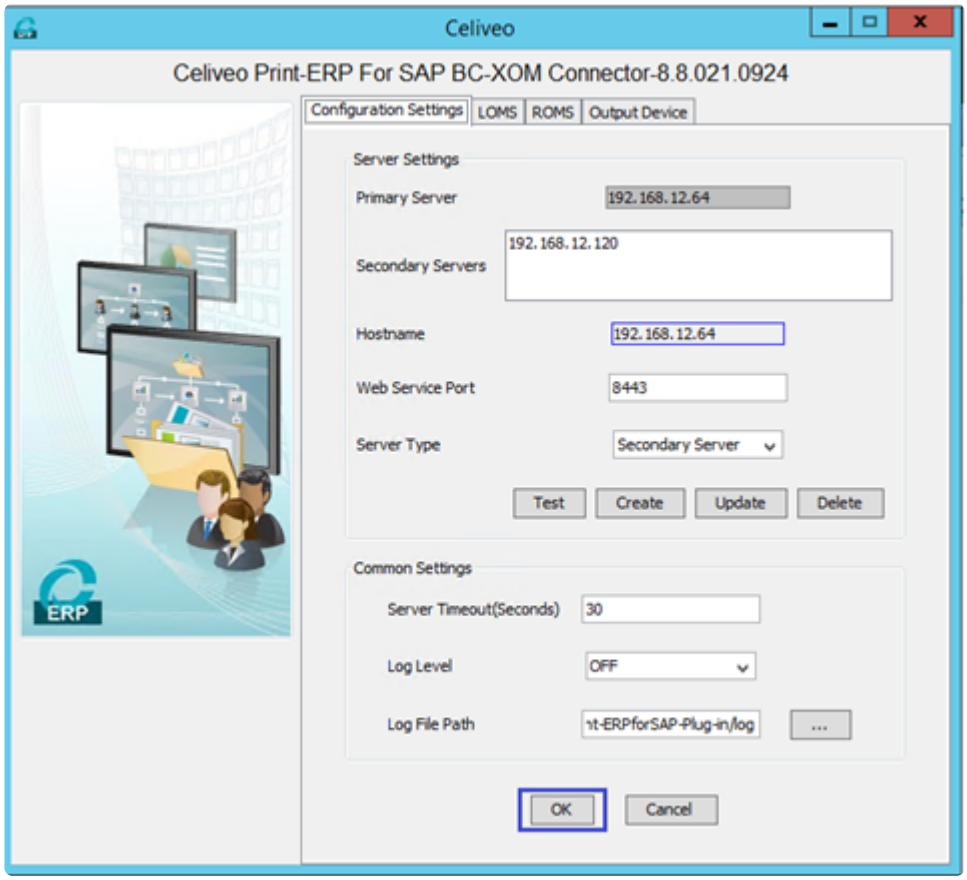
2. Enter the following details and click **Add**.
- Hostname —> Hostname of the Celiveo 8 server.
- Web Service Port
- Server Type —> Select **Primary Server**



3. Click **OK** to confirm and add the Celiveo 8 server as the primary server.

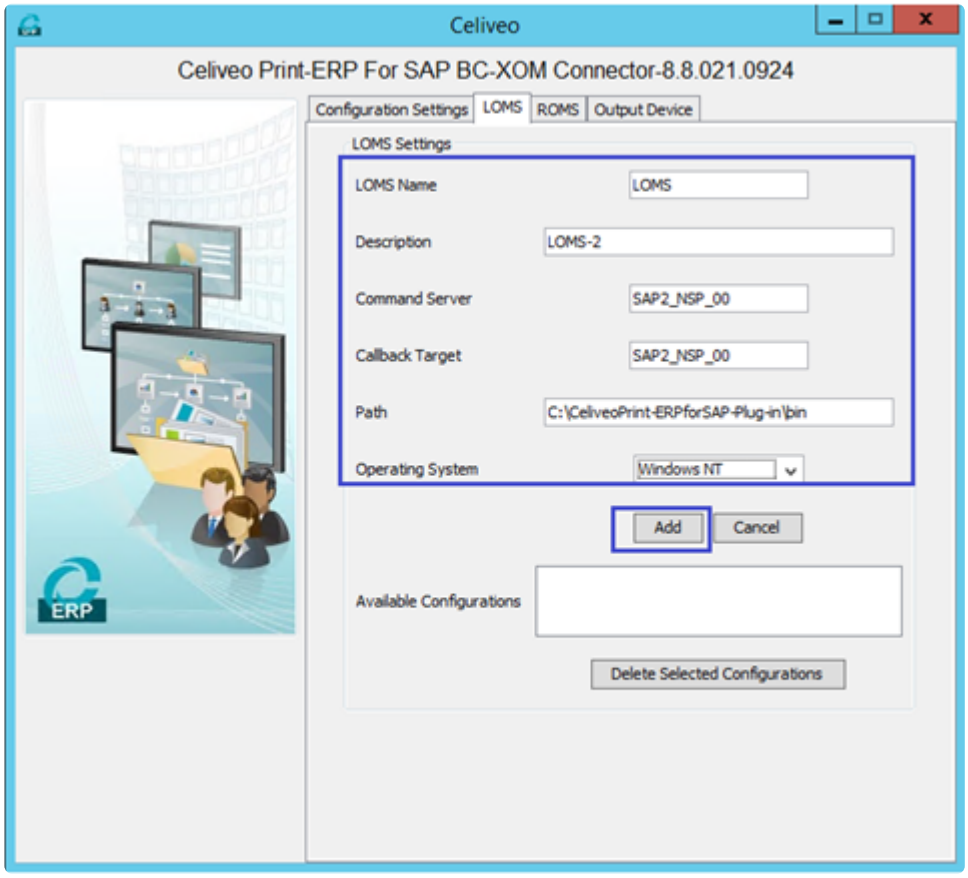


4. Click **OK** on the bottom to save the changes.

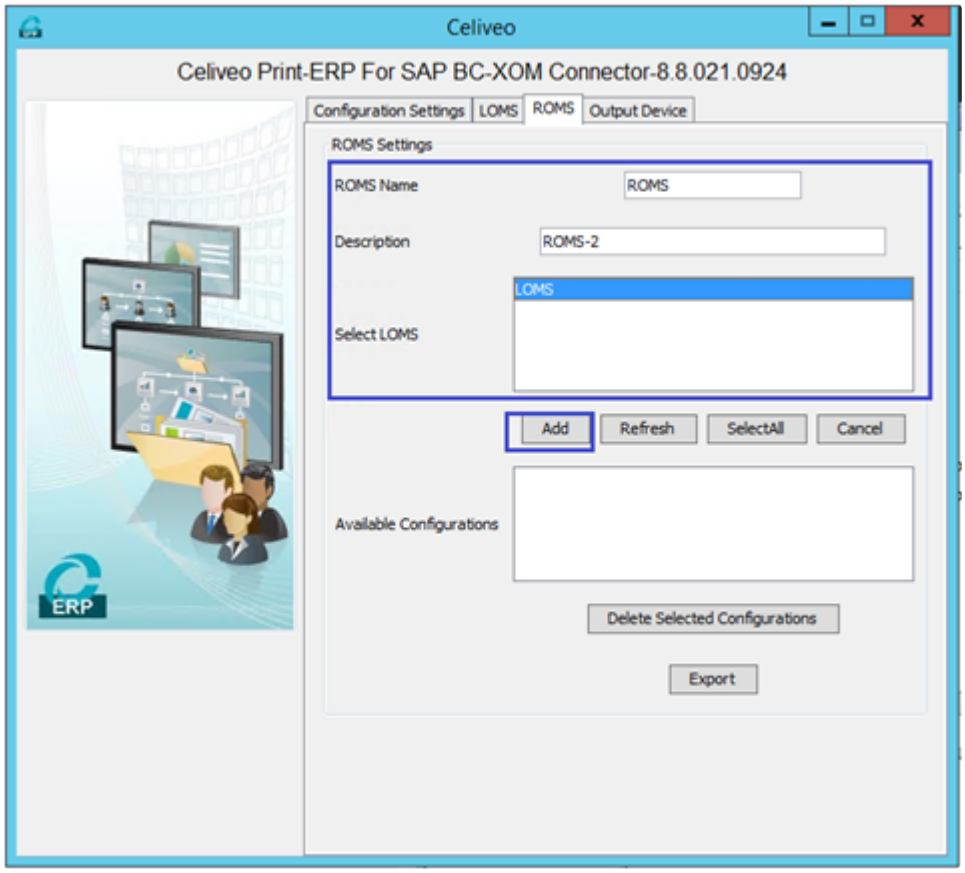


Configure LOMS/ROMS/Output Devices

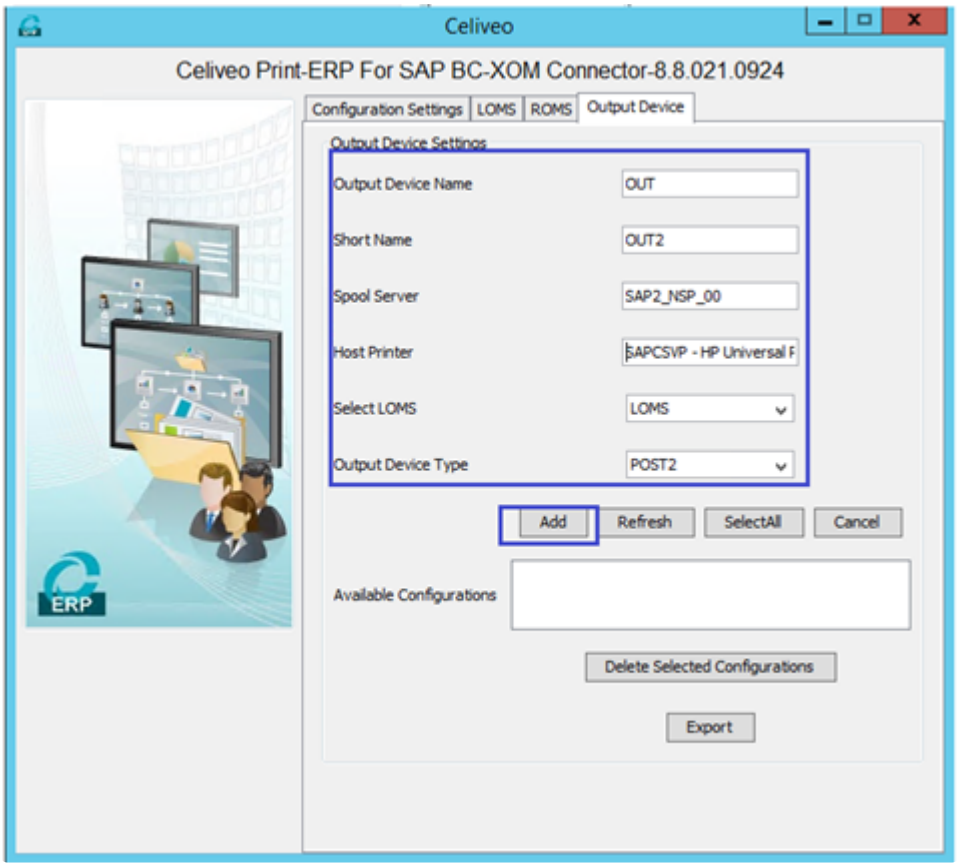
1. Enter the LOMS details



2. Enter the ROMS details



3. Enter the Output Device details.



Last modified: 29 September 2022

10. Using Celiveo

Learn how to use the Celiveo Solution on a daily basis!

Enroll a Card on a Celiveo-Enabled Printer
Tag Printers and Users
Place or Locate Printers on a Floor Plan
Print from a Workstation
Print Using Print Direct

Last modified: 29 September 2022

10.1. Enroll a Card on a Celiveo-Enabled Printer

When authenticating for the first time on a Celiveo-Enabled Printer, you need to enroll your card in the printer, i.e make your card recognizable by the machine. Once you have done this, authentication will only require a simple gesture.

To enroll your card:

1. Swipe your card over the reader.

2. When prompted, enter your Windows credentials.
3. Wait for the confirmation message. Your card is now enrolled.
4. To authenticate, simply swipe the card over the reader.

Last modified: 29 September 2022

10.2. Tag Printers and Users

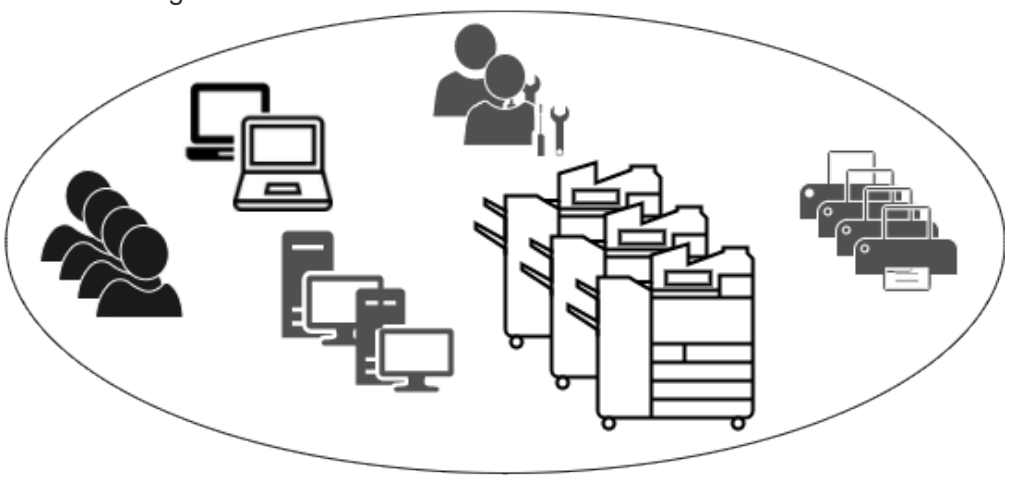
Use Tags to Define Communities

Contents

1. What is community?
2. Why use Tags/Communities?
3. Examples
4. Use Bookmarks to access communities quickly
5. How to…
    a. Label a Tag
    b. Tag Printers
    c. Tag Users
    d. Tag User Groups
    e. Tag IP Address Ranges

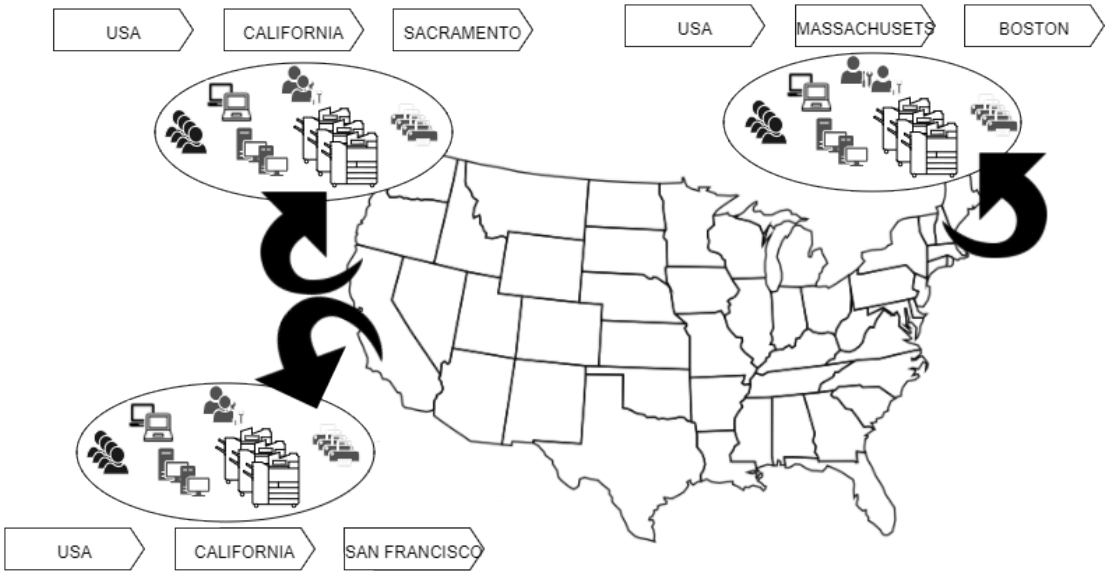
What is a community?

A community is a group of users, workstations, printers, and administrators that have a common characteristic. For example, a group of users, workstations, printers, and administrators, located in the same building.



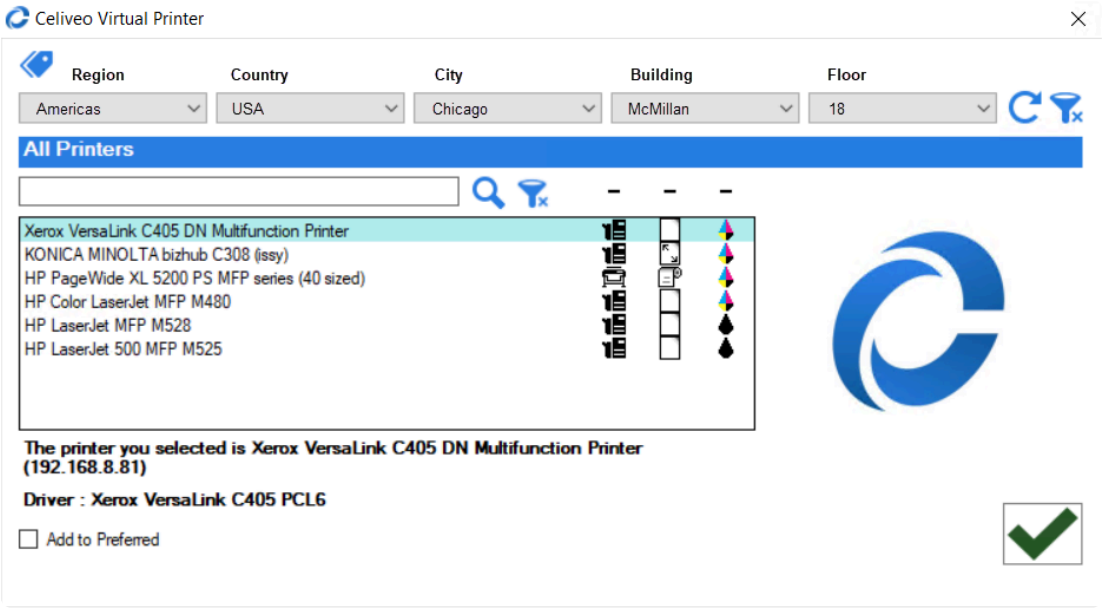
The community that a user or device belongs to is determined by the tags assigned to them.

Why use Tags/Communities?



The example shown above illustrates a company distributed across several cities. The company uses tags to identify places. Although Celiveo supports up to five tags, they use only three, which identify Country, State, and City. A user tagged *USA*, *California*, *San Francisco*, belongs to the San Francisco community. A user tagged *USA*, *California*, *, belongs to the California community, which is a superset of San Francisco and Sacramento.

When you use Print Direct, tags filter the available printer list to display only those printers that are part of your community, thus minimizing screen clutter.

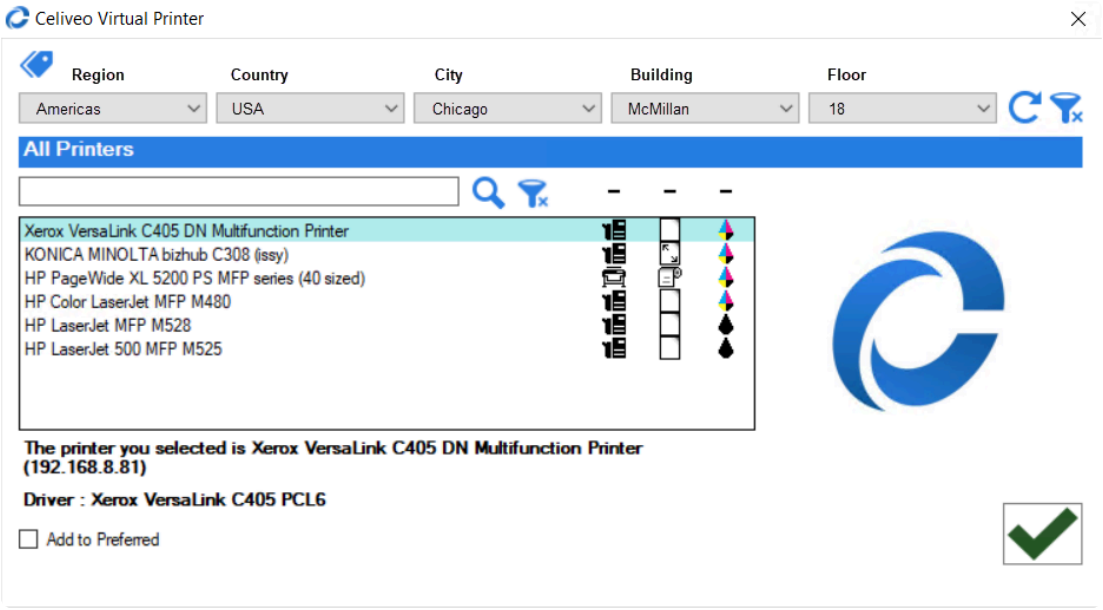


You can also use tagging to delegate the system administration of a community to a user who belongs to that community. (See Managing System Administrators for more information)

Examples

Example 1 : Your Company is distributed across multiple cities (Sacramento, San Francisco, and Boston). You don't want to clutter a Boston user's screen with Sacramento and San Francisco Printers (and vice versa). Hence, you create three separate communities for Sacramento, San Francisco, and Boston. You then tag the printers and IP Address ranges so that the printers and IP Addresses used in

each geography will belong to the same community. When a user connects to the network from the Boston office, the user is assigned a Boston IP Address. Because this IP address is tied to the Boston Community, Print Direct filters the list of Printers to show only the Boston Printers. If this same user visits the San Francisco office, and plugs into the San Francisco network, the list of printers will automatically show the San Francisco printers.



Example 2: Your Company occupies a large multi-story building, and each organizational unit is housed in a different zone in the building. You want to provide users' access to printers within their zone. Hence you create communities for each zone. You tag printers so that they belong to the zone they are placed in. Thereafter you tag Active Directory organizational units (using authentication profiles), such that users who belong to an organizational unit will belong to the zone they are seated in. When these users log in to Windows, the system interacts with the Active Directory and filters the list of available printers to those in the zone they are seated in.

Use Bookmarks to access communities quickly

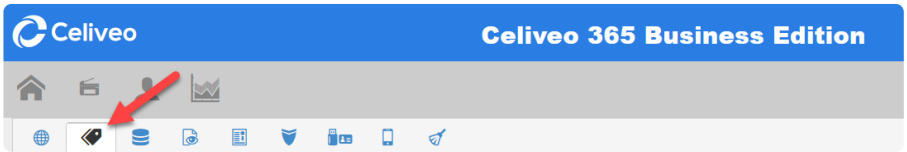
In the Web Admin, you can save a tag combination as a bookmark. Thereafter when you load the bookmark, the tag combination loads. Thereby, a bookmark serves as a shortcut to a community.

How to…

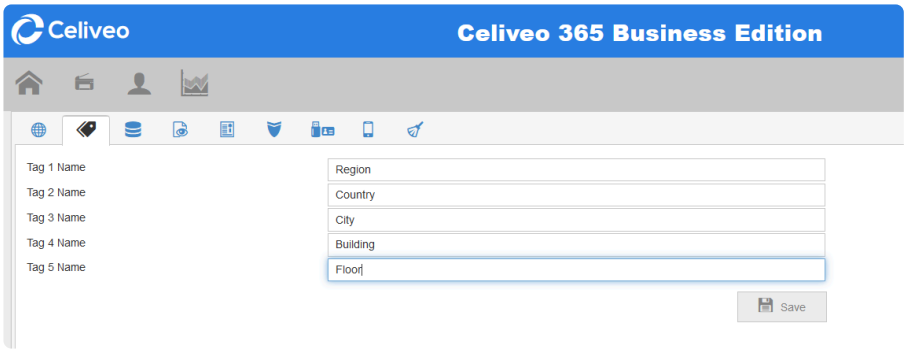
Label a Tag

1. Click ⚙.

2. Click 🏷.

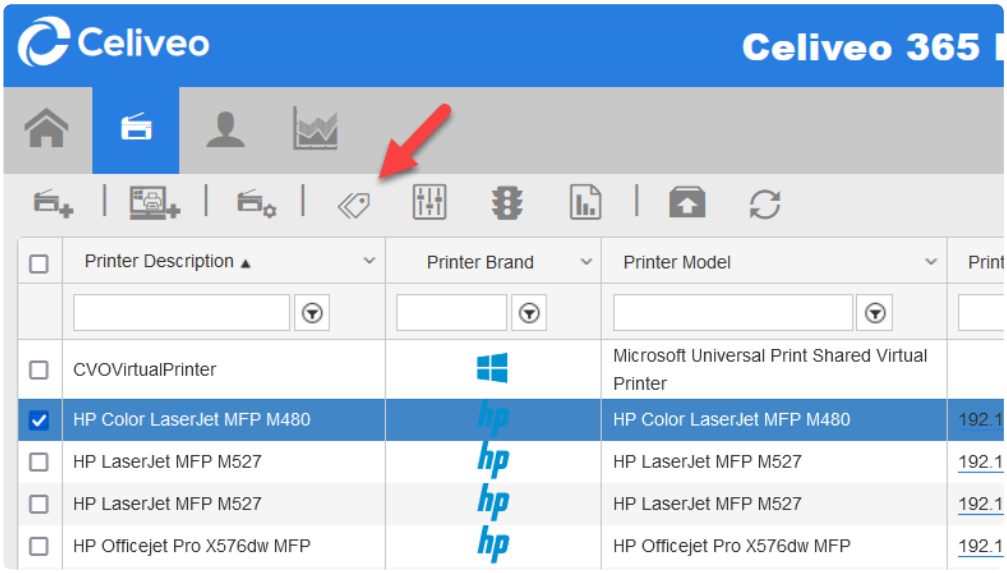


3. Label the tags as required and click **[Save]**.

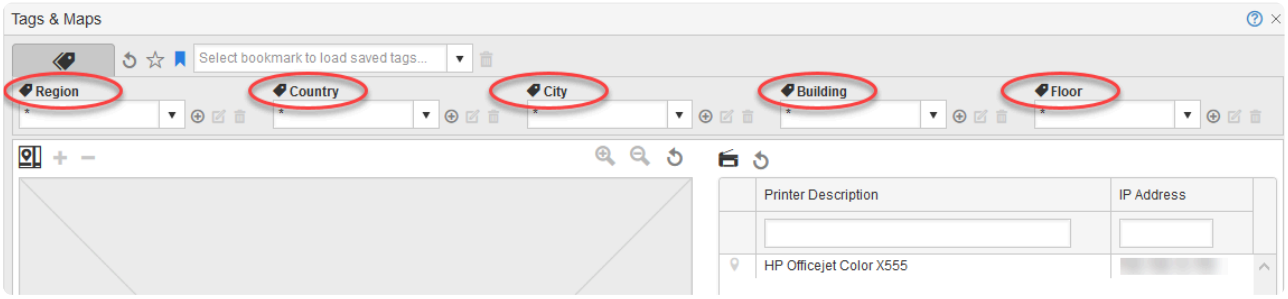


Tag Printers (Add Printers to a Community)

1. From the List of Printers, select the printers you want to specify tags for and click .



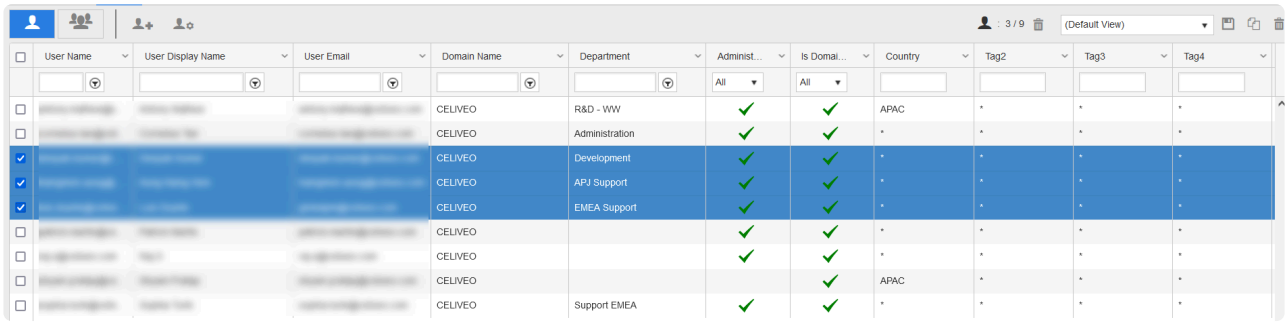
2. Select the tags for the printers.



3. If any tag drop-down list is empty, or does not contain the value you need:
   a. Click ⊕ next to the drop-down.
   b. Specify the new value for the tag and click **[Save]**.
4. Click **[Save]**. The tags are assigned to the printers.

Tag Users (Add Users to a Community)

1. From the List of Users, select the users you want to specify tags for and click .

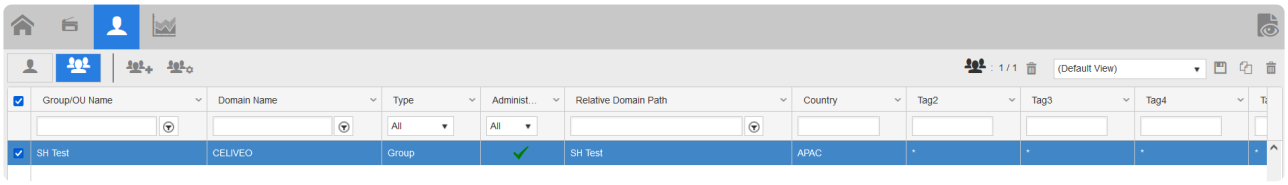


2. Select the tags for the users.

3. If any tag drop-down list is empty, or does not contain the value you need:
   a. Click ⊕ next to the drop-down.
   b. Specify the new value for the tag and click **[Save]**.
4. Click **[Save]**. The tags are assigned to the users.

Tag User Groups (Add user groups to a community)

1. From the List of User Groups, select the groups you want to specify tags for and click .

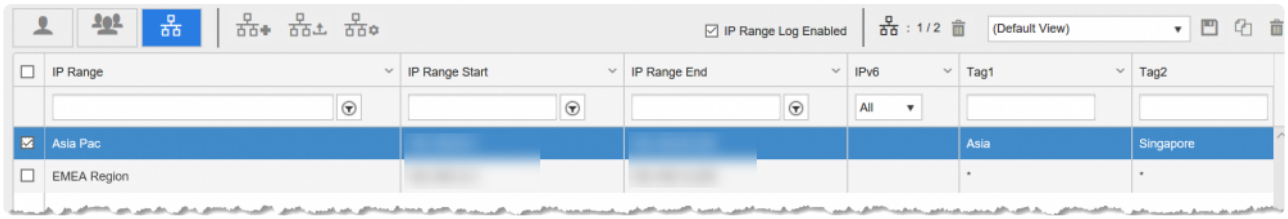


2. Select the tags for the user groups.

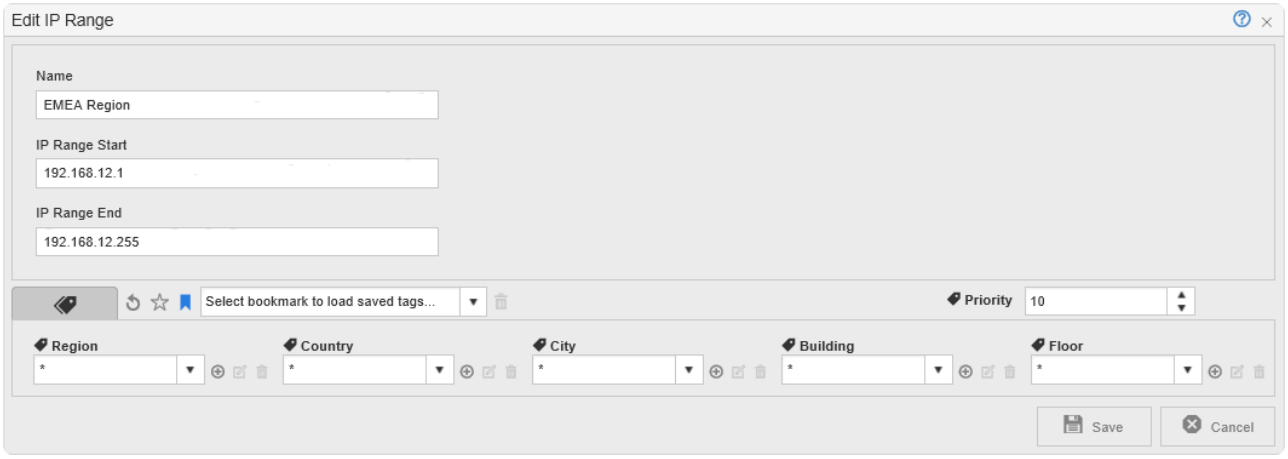
3. If any tag drop-down list is empty, or does not contain the value you need:
   a. Click ⊕ next to the drop-down.
   b. Specify the new value for the tag and click **[Save]**.
4. Click **[Save]**. The tags are assigned to the users.

Tag IP Address Ranges (Add IP Address Range to a Community)

1. From the List of IP Address ranges, select the range you want to specify tags for and click .



2. Select the tags for the IP Range.



3. If any tag drop-down list is empty, or does not contain the value you need:
   a. Click ⊕ next to the drop-down.
   b. Specify the new value for the tag and click **[Save]**.
4. Click **[Save]**. The tags are assigned to the users.

Enable IP Range Log (Generate log messages in System Log)

Select this checkbox to generate (warning) messages in Web Admin System Log if the user tries to connect from IP addresses that are not configured/ enlisted under the defined IP Address Range list. This option takes effect (i.e., log messages are generated) only if at least one IP Address Range is defined.

Last modified: 29 September 2022

10.3. Place or Locate Printers on a Floor Plan

The Floor Plan is tied to the combination of settings that are current at the time the Floor Plan is imported.

As such, ensure that tags are defined before you begin this exercise.

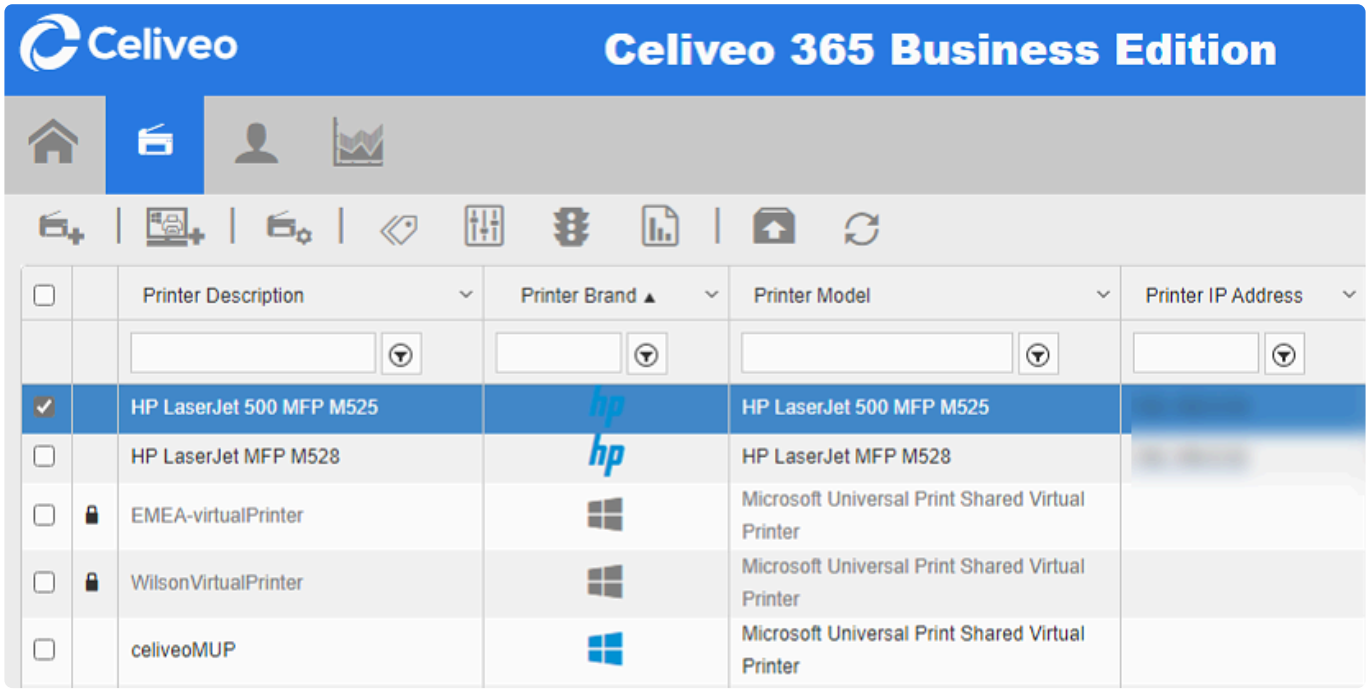
Contents

1. Why Floor Plans?
2. Import a Floor Plan and Place a Printer on It
3. Place Another Printer on the Floor Plan

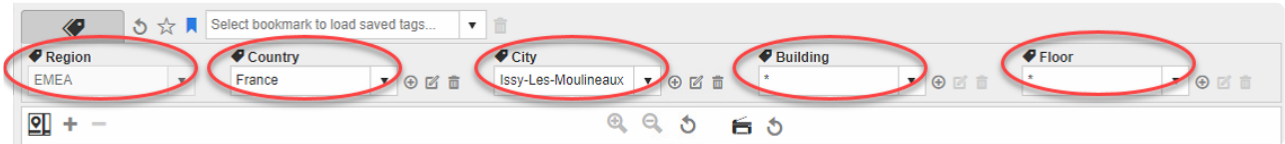
1. Why Floor Plans?

https://player.vimeo.com/video/240127463

2. Import a Floor Plan and Place a Printer on It

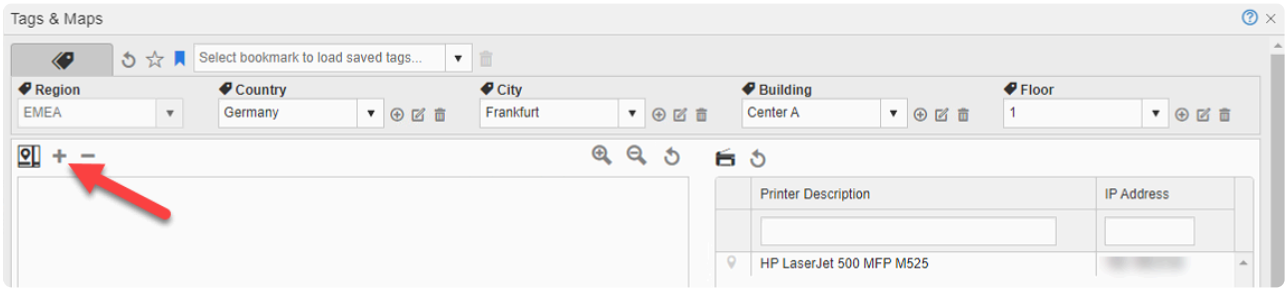


1. In the Printers List, select the printer you want to place on the Floor Plan.
2. In the Printer Menu, click . The Tag/Map displays.

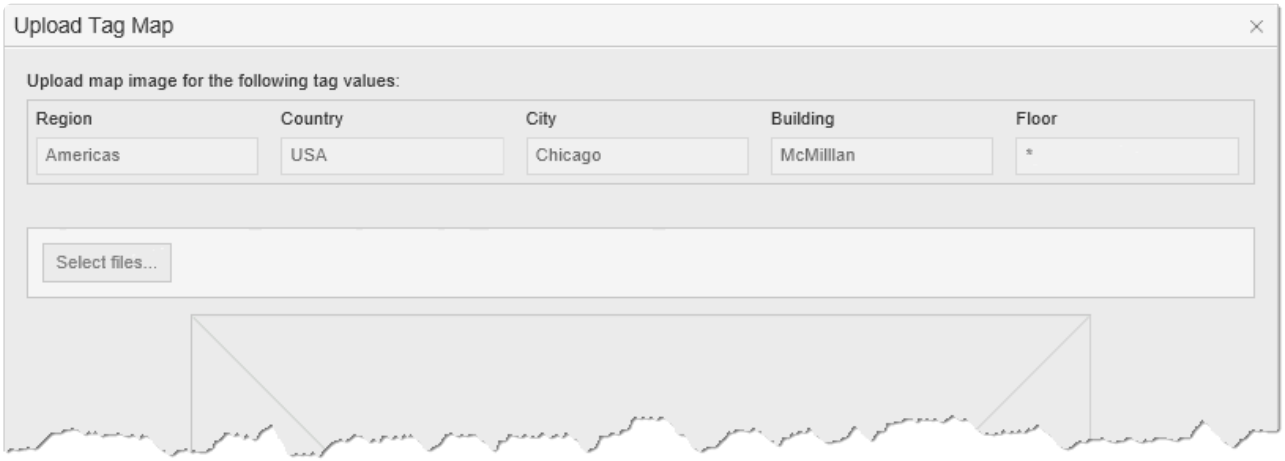


3. Specify the tags for the printer.

4. Click + below the first tag. Upload Tag Map displays.



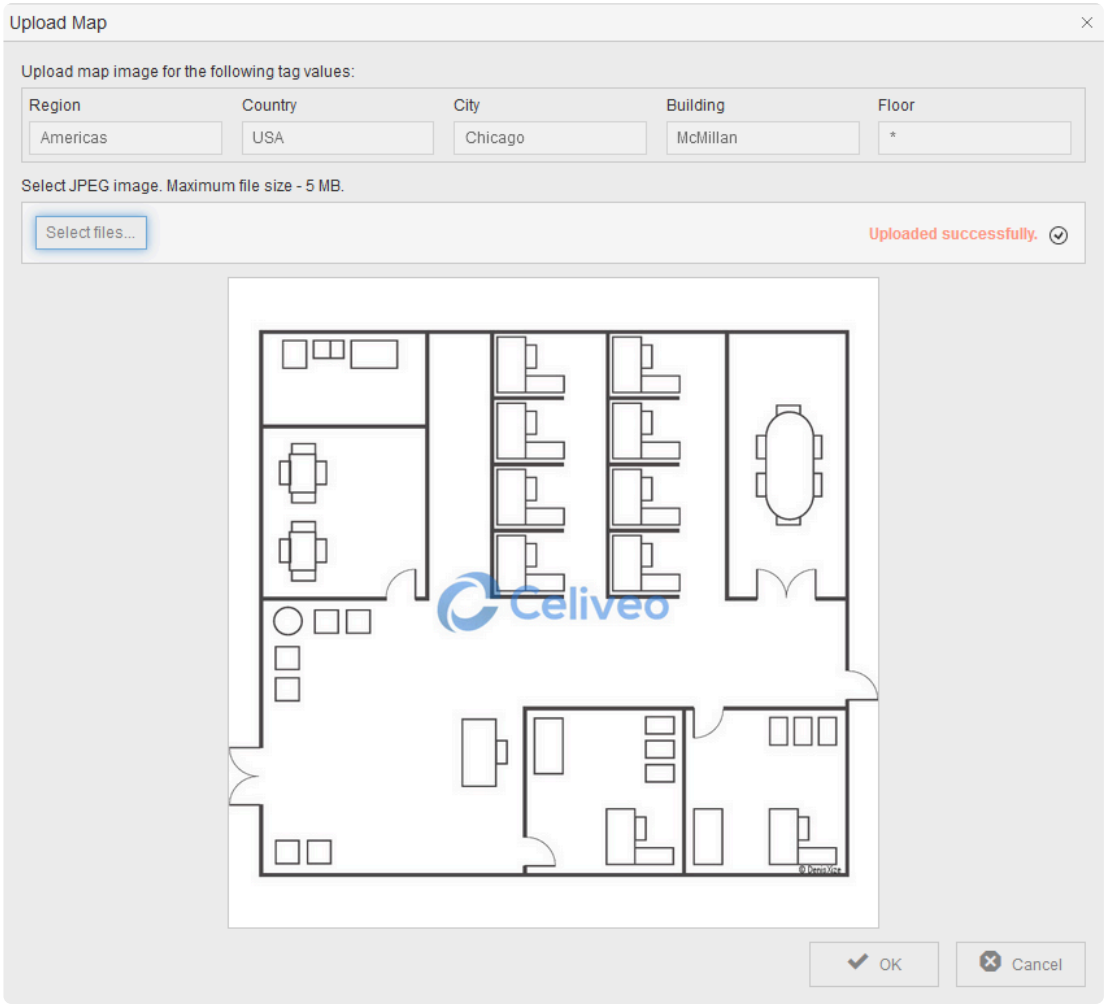
5. Click **[Select files]** and pick the image file that contains the floor plan.



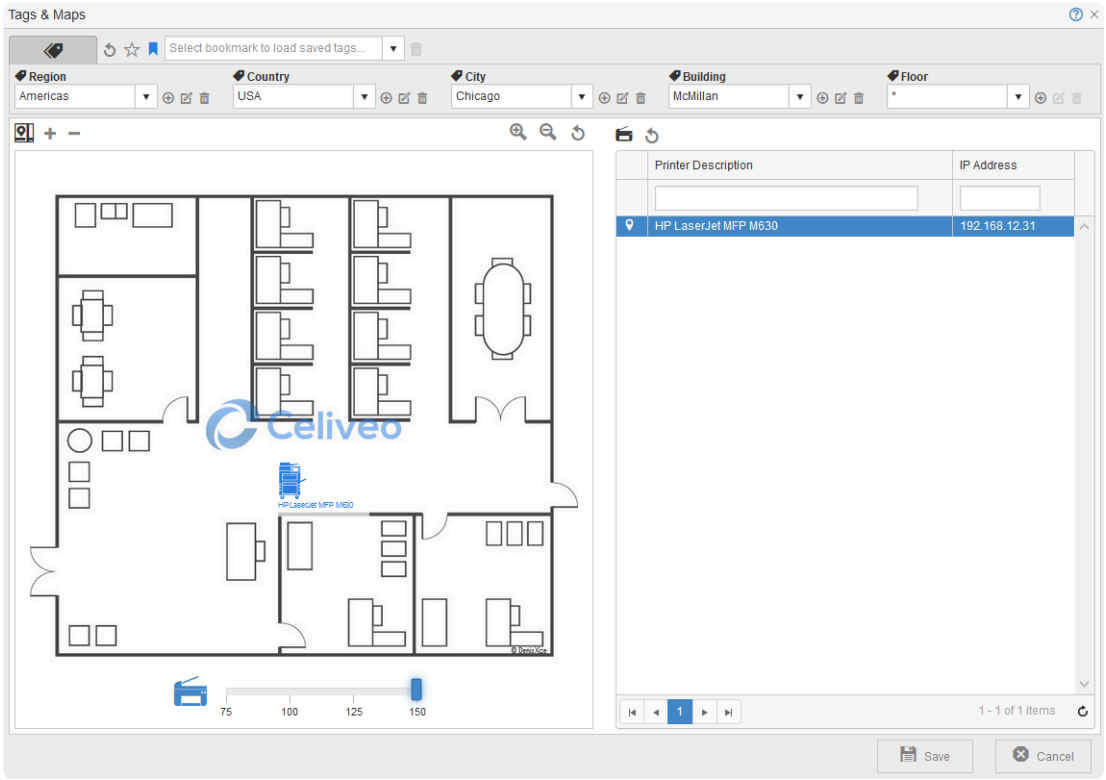
Note:

a. The image should be in JPEG format.
b. The image file must at least be 600px X 600px.
c. If the width is not the same as the height, the floor plan may become distorted.
d. The image file must be smaller than 5MB.

6. Click **[Save]**.

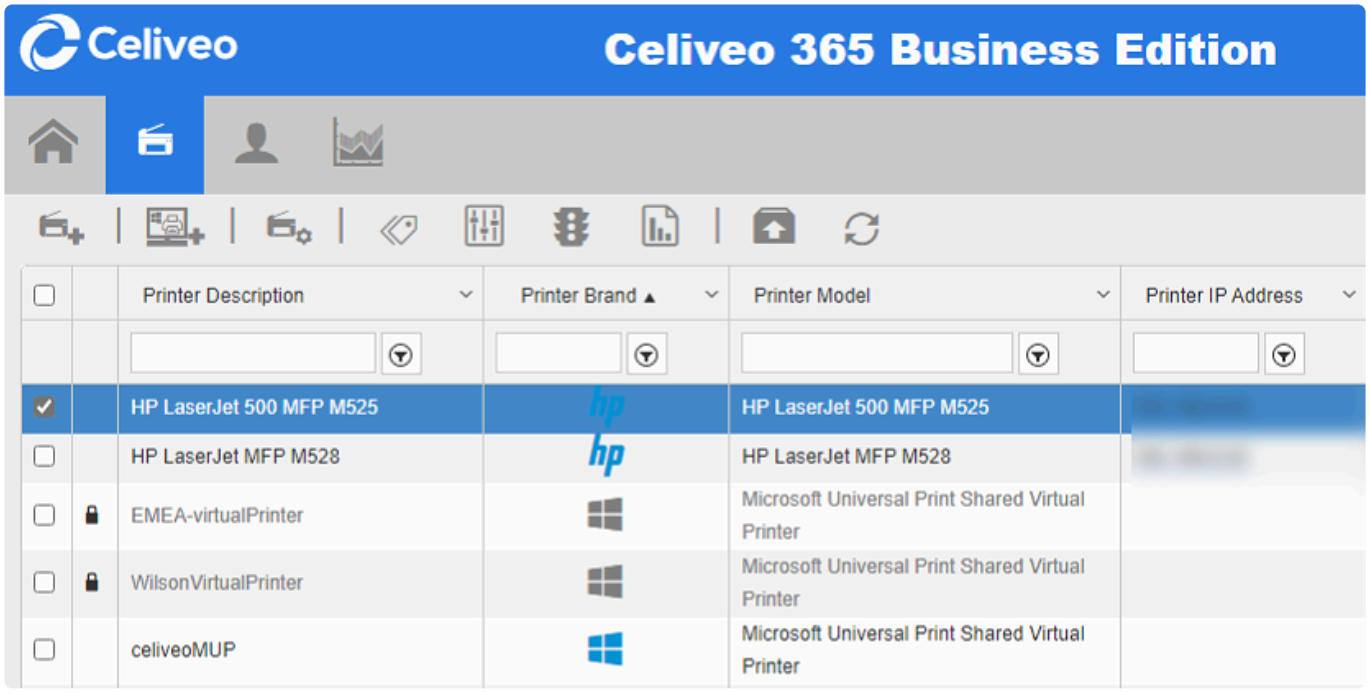


7. Drag the printer from the printer list on the right to its location on the Floor Plan.

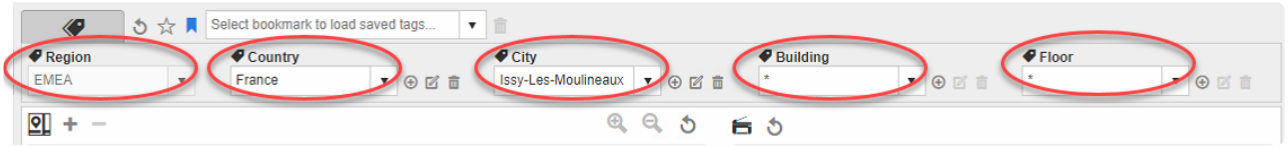


8. Use the cursor to increase or decrease the size of the printer icon.
9. Click **[Save]**.

3. Place Another Printer on the Floor Plan



1. In the Printers List, select the printer you want to place on the Floor Plan.
2. In the Printer Menu, click . The Tag/Map displays.



3. Specify the tags for the printer. When you specify the tags, the floor plan displays automatically.
4. Drag the printer from the printer list to its location on the floor plan.
5. Click **[Save]**.

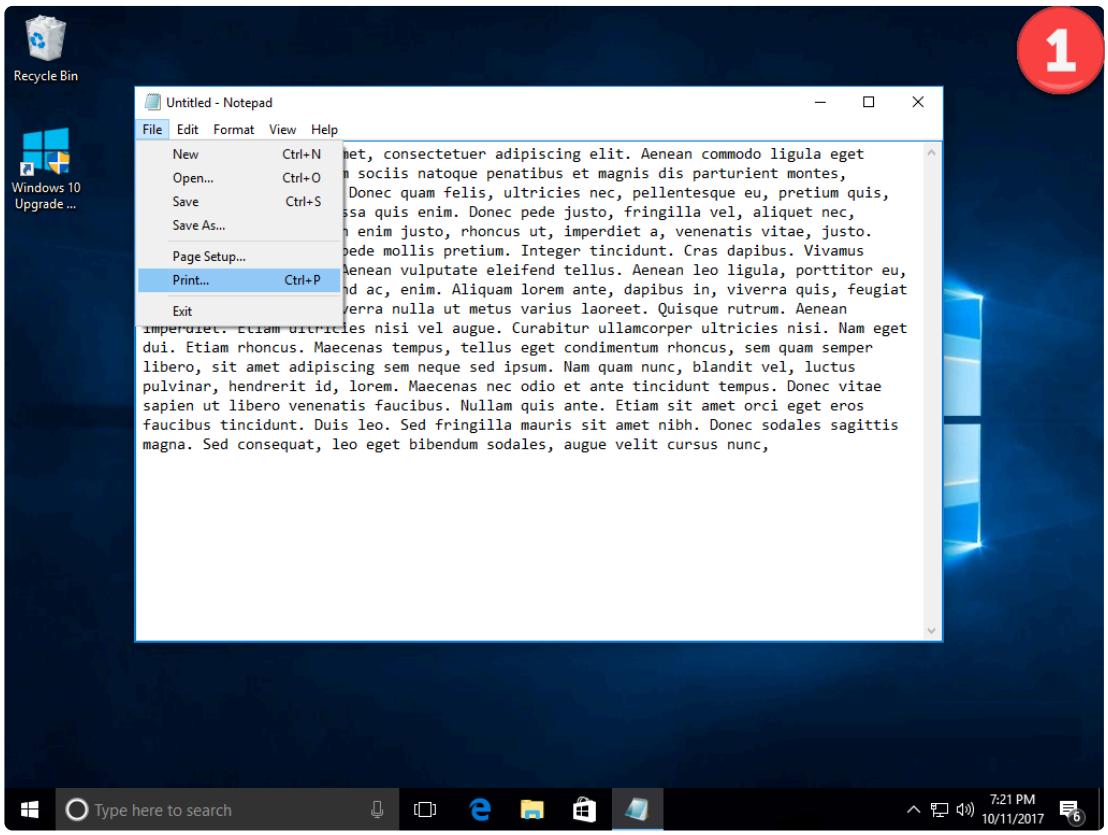
You can find Sample Floor Plans in our Downloads section (requires a Celiveo Portal Account).

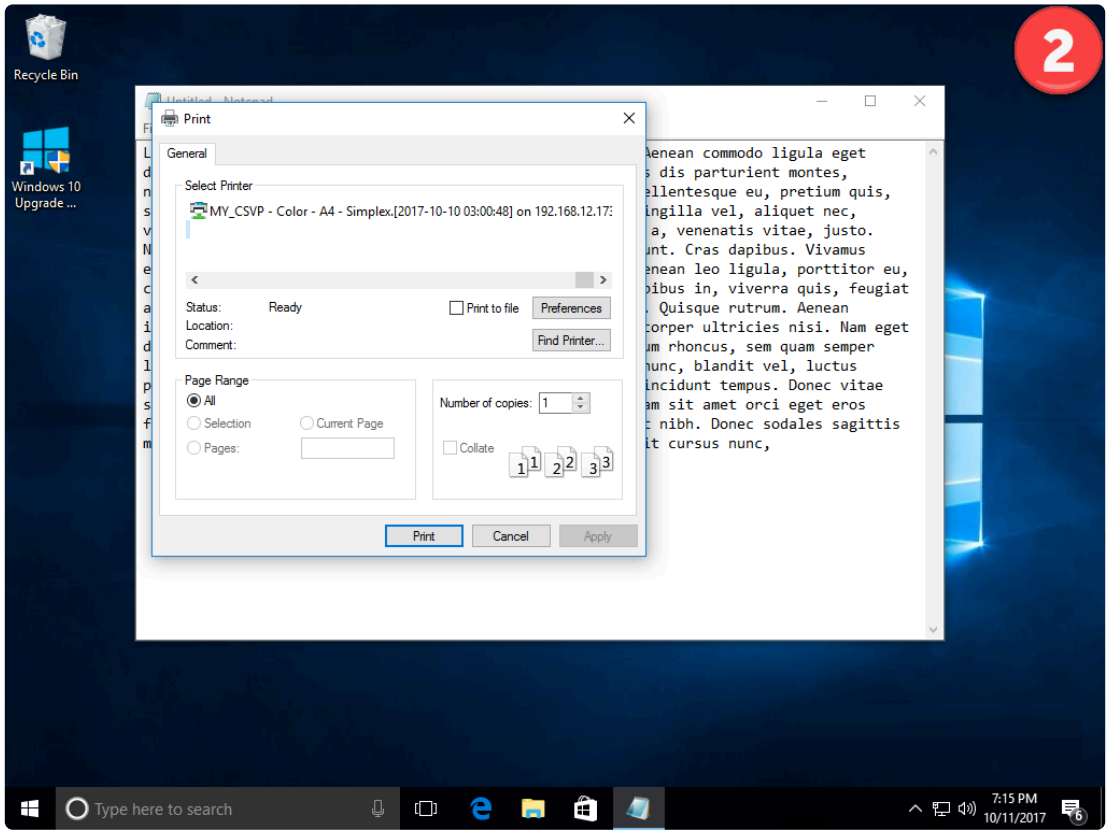
Last modified: 29 September 2022

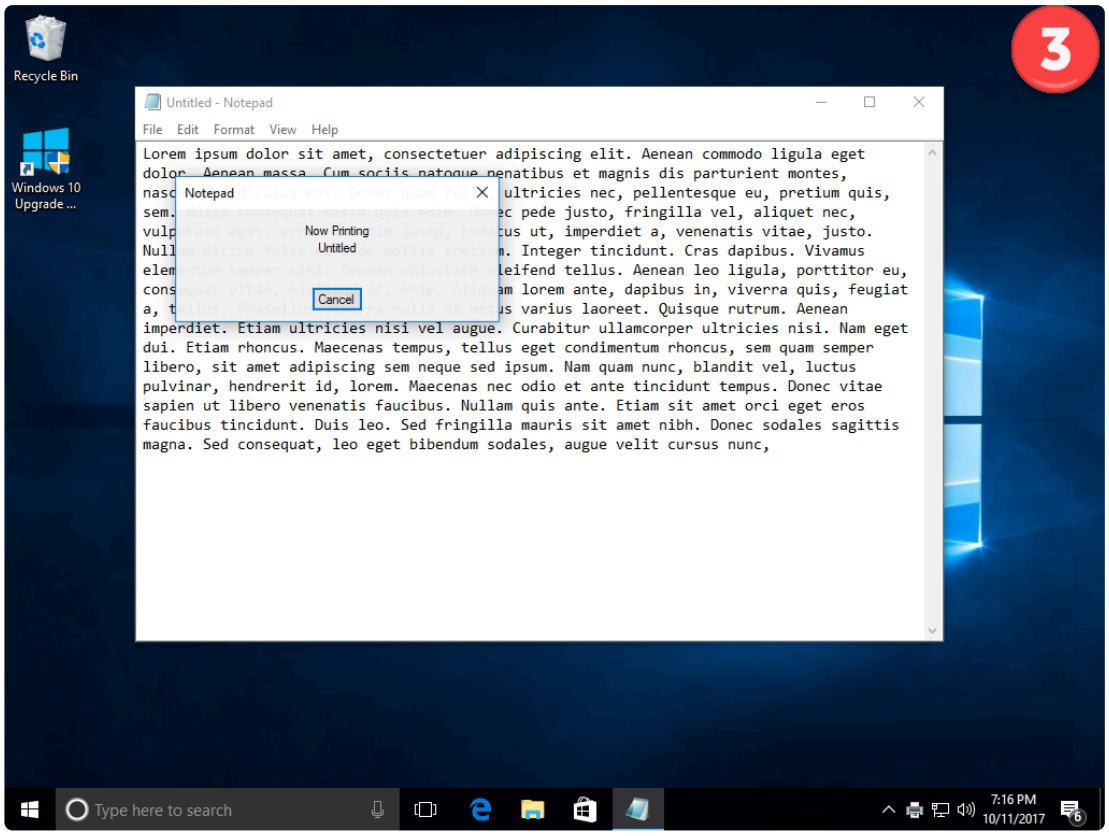
10.4. Print from a Workstation

1. On the User's Workstation…

When you print from a user's workstation,you print to the Celiveo Shared Virtual Printer, just like how you would print to any other printer. After that, you go to the nearest Celiveo-enabled printer.







Notes:

- In Print-Direct mode, the virtual printer on user workstation dynamically takes the [name + driver] of the physical printer that is selected, so that the user knows which printer is addressed and with what driver nickname.
- If both Pull Printing and Print-Direct are configured for the virtual printer, make sure the Celiveo Smart Appliance is attached to the printer and synchronized (in case of HP FutureSmart printers,

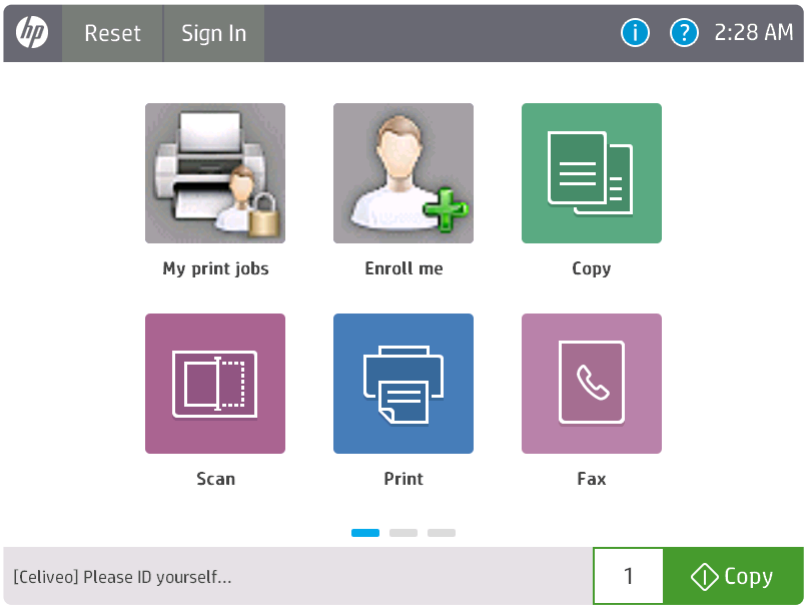
only synchronization is required) before printing, for Track-GreenSaver tracking to work properly.

2. At the Printer…

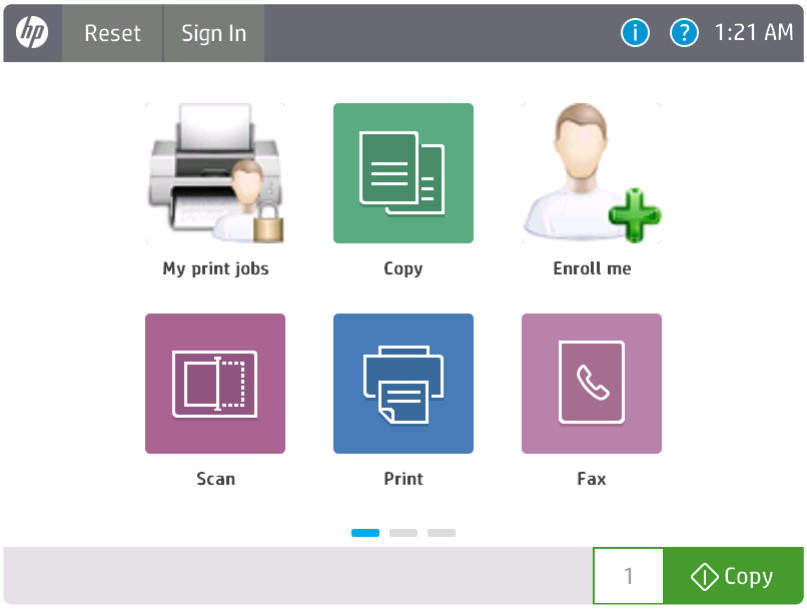
> **Note**: The screens you see at the printer and the workflow for releasing print jobs differ from one brand to another. The mock-ups shown below are for the purpose of illustrating the workflow, and can be different from actual screens.

2.1 HP Printers

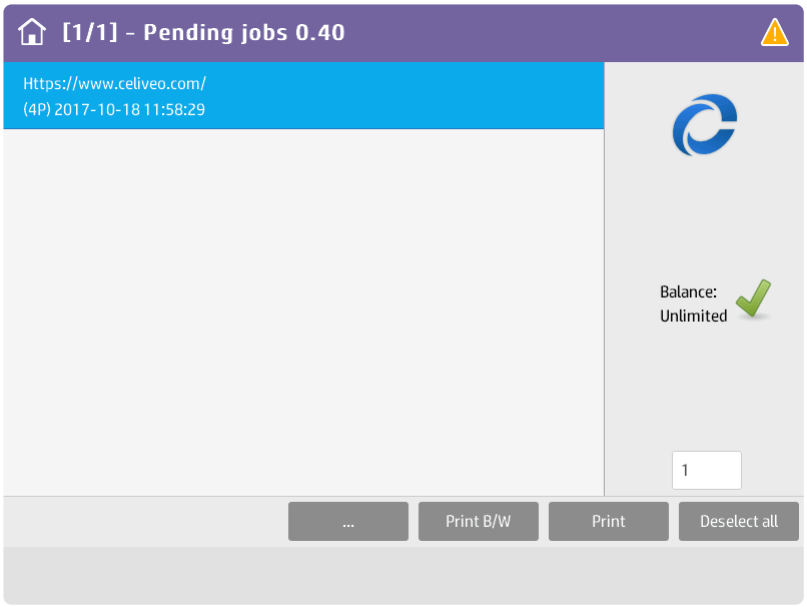
1. Tap your access card on the card reader.

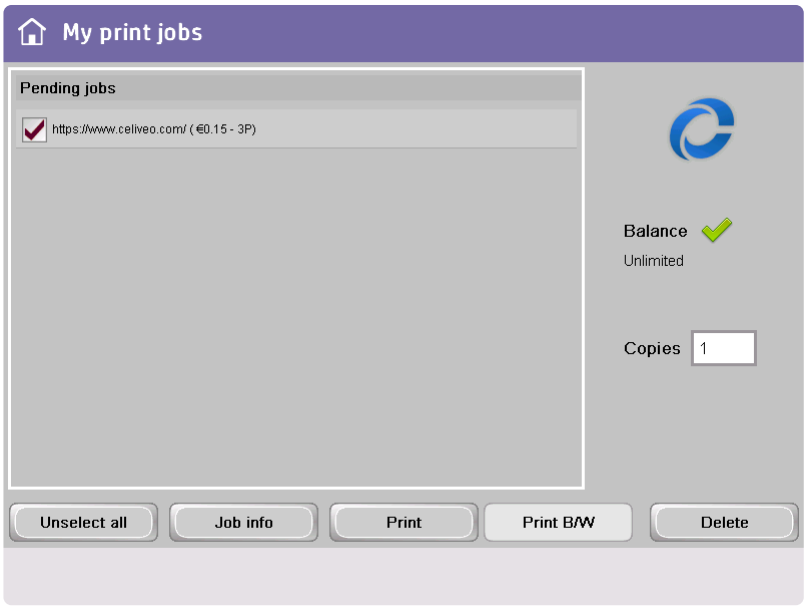


2. At the Home Screen tap **My Print Jobs**.



3. From the Print Job list, select the print jobs you want to release and tap **Print**.



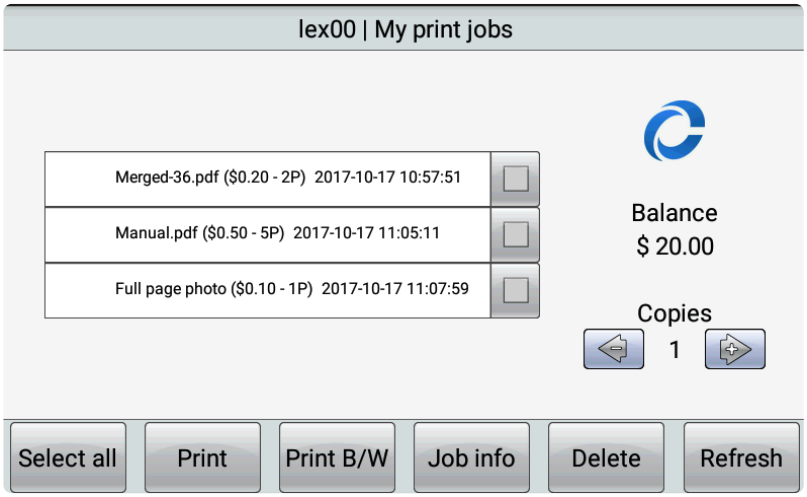


Note: The number of copies that can be printed for a print job is limited from 1 to 99 in HP printers.

2.2 Lexmark Printers

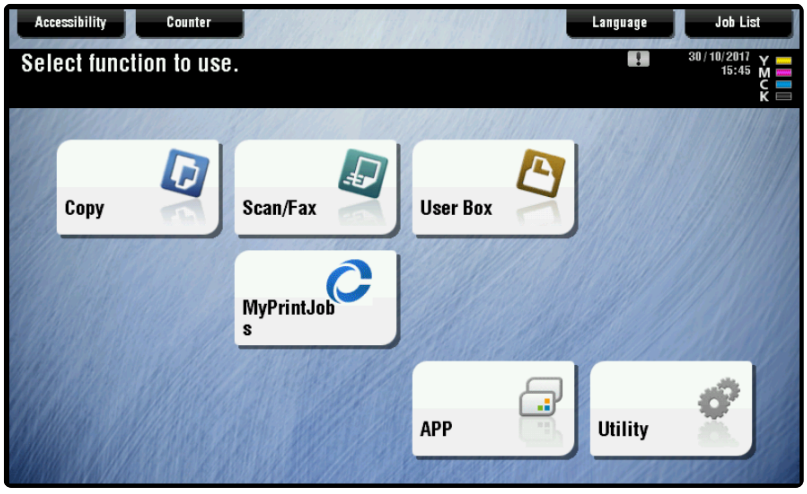
1. Tap your access card on the card reader.
2. At the Home Screen, tap My Print Jobs.

3. Select the print jobs to release and tap Print.

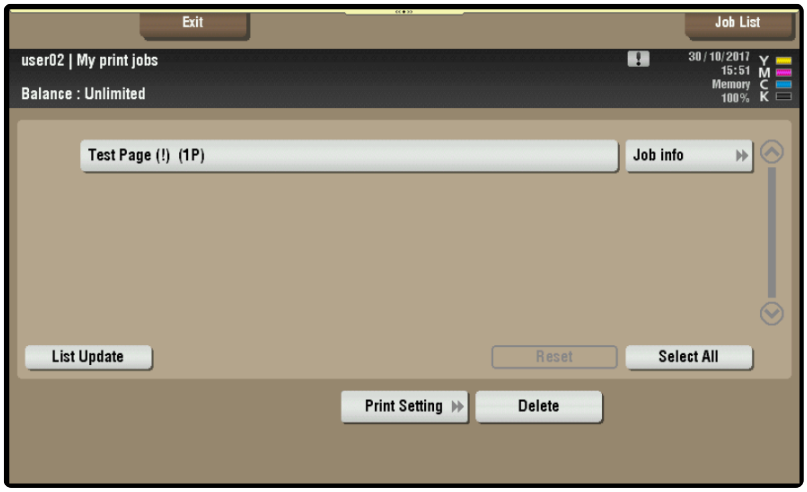


2.3 Konica Minolta Printers

1. Tap your access card on the card reader.
2. At the Home screen, tap the My Print Jobs icon.



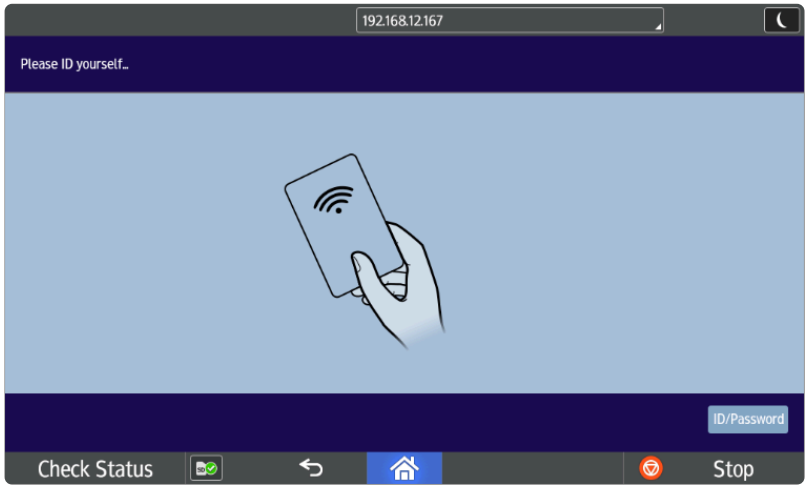
3. In the Print Jobs list, tap the print jobs you want to release.



4. Press the Start button on the Printer.

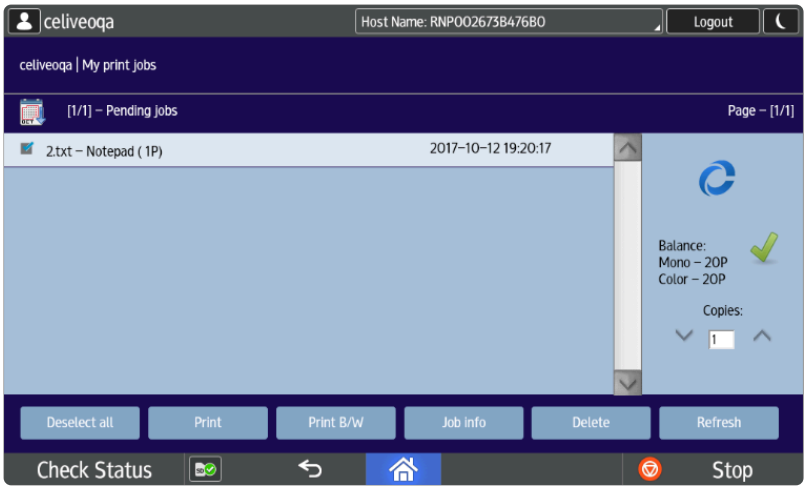
2.4 Ricoh Printers

A screen similar to the mock-up shown below is displayed when no one is logged into the printer.



1. Tap your access card on the card reader.
2. Tap **My Print Jobs**.

3. When the Print Job list is displayed, select the print jobs to release and tap Print.



Printing in a few seconds.

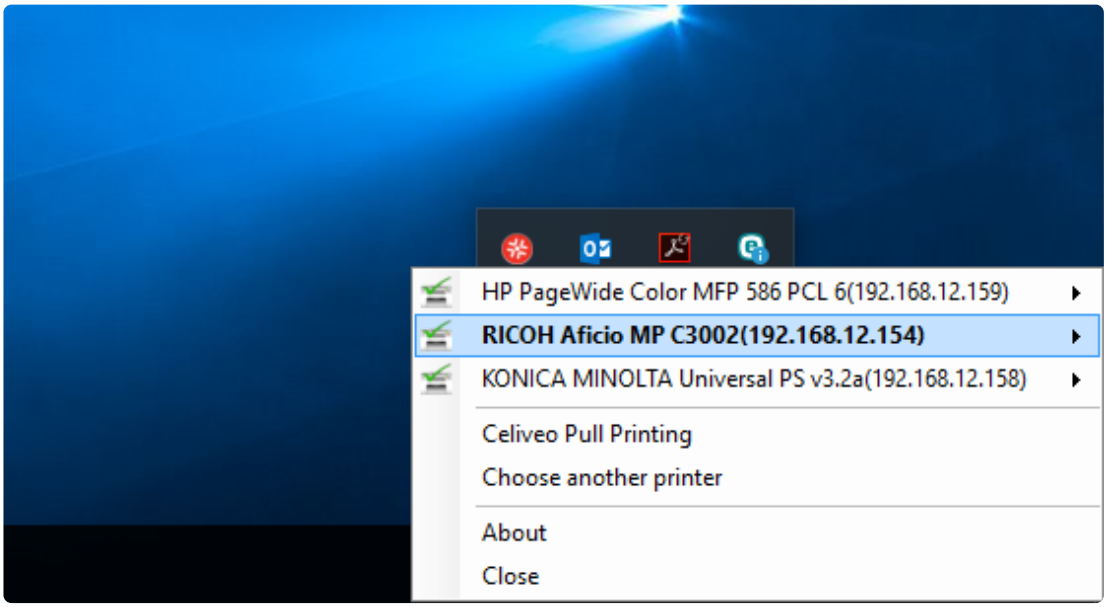
Last modified: 29 September 2022

10.5. Print Using Print-Direct

- Select Default Printer and Print
- If the Printer You want to Use is not on the Menu
- Change Default Printing Preferences

Select Default Printer and Print

1. Right-click the Celiveo Virtual Printer system tray icon ( ). A menu displays.



> **Notes**:
> - The printers you installed are listed at the top of the menu. Their status is displayed in real-time. A green tick mark indicates that the printer is available. A red x mark indicates that the printer is unavailable.
> - In Print-Direct mode, the virtual printer on PC dynamically takes the name + driver of the physical printer that is selected, so that the user knows what printer is addressed and with what driver nickname.

2. Click the printer you want to print from and then click **[Select]**. The printer is set as the default printer for Windows.

> **Note**: If the printer driver for the printer you selected is shared with another printer, the name of the printer driver is displayed in a sub menu after **[Select]**. If so, click the driver.

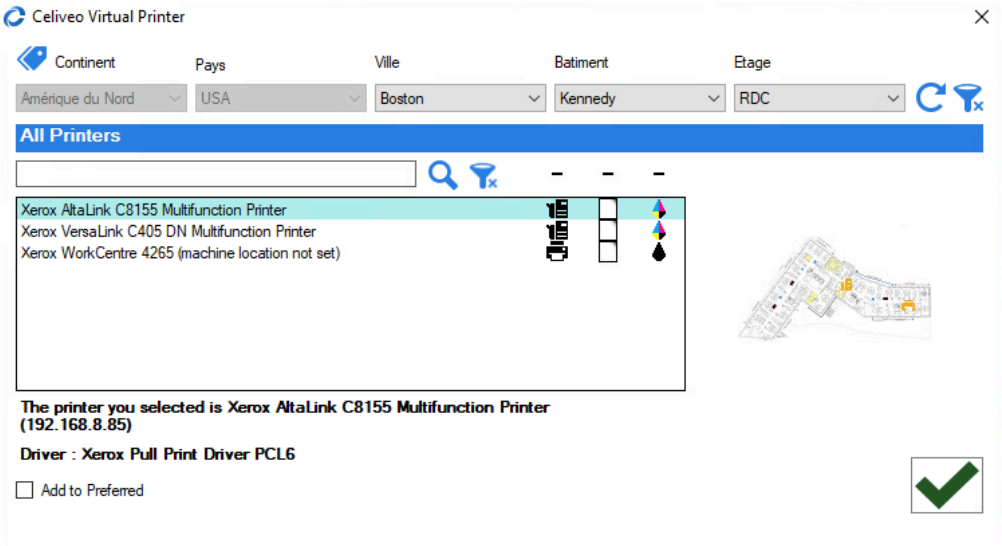
3. In the application to print from, print via the default printer.

> **Note**: For a Virtual printer, where both Pull printing and Print-Direct printing are configured, always make sure that the CSA is attached to the printer and synchronized (in case of HP printers, only syncing is required) before printing, for Track-GreenSaver

tracking to work properly.

If the Printer You want to Use is Not on the Menu…

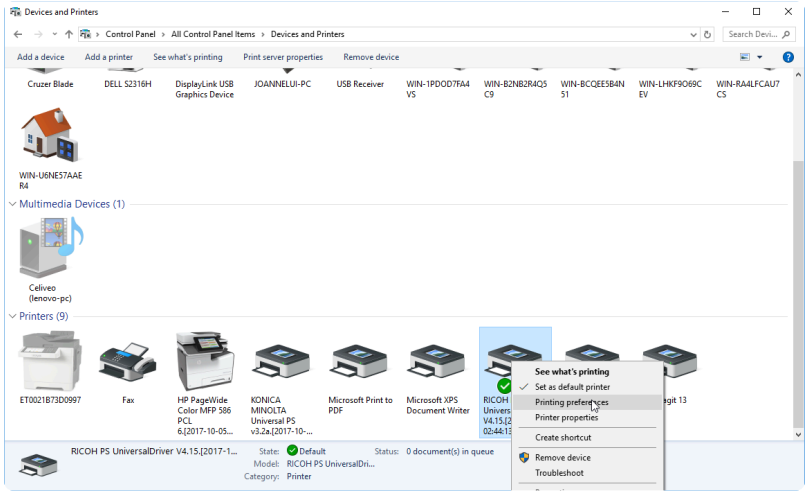
1. Right-click on the system tray. A menu displays.
2. Click **[Choose another printer]**. The Celiveo Virtual Printer screen displays.



3. Select the printer to use on this workstation and click .
   A vertical yellow bar starts running on the Celiveo Virtual Printer system tray icon while the printer is installed on the workstation.

Change Default Printing Preferences

The procedure for changing default printing preferences listed here applies to Windows 10. The procedure for other versions of Windows may differ slightly.



1. Start the **[Devices and Printers]** control panel applet.
2. Right-click the driver corresponding to the printer you want to configure. A menu displays.
3. Click **[Printing Preferences]**.
4. Specify the settings and click **[OK]**.

Note: The settings you specify are used as the default preferences for all printers that use that driver. If you install another printer that uses the same driver, the settings may be overwritten.

Last modified: 29 September 2022

11. Authentication

This section details how to configure the Celiveo authentication feature.

Access Control Rules
Authentication Profiles
High Availability
Enable ID Code Authentication for Printers
Save Card Number and ID code on Active Directory
Configure BLE RF IDEAS Readers for Smartphone Authentication with Orange Pack-ID Application
Configure ID Mask
Custom Access Control for HP FutureSmart Printers

Last modified: 29 September 2022

11.1. Access Control Rules

Contents

1. About Access & Control Rules
    a. What are Access Control Rules?
    b. Unlock a Function for Unrestricted Access
    c. Authorize a Function for a Specific Group of Users
    d. Combining Access Control Rules and Assigning them to Printers

2. How to…
    a. Create a New Access & Rules Profile
    b. Add a Rule to Unlock a Function
    c. Authorize a Function for Smartcard/Card or PIN Authentication
    d. Set Up ID Mask and Dual Factor Authorization for Card Authentication
    e. Enable Self-Enrollment for Card Authentication

About Access Control Rules

What are Access Control Rules?

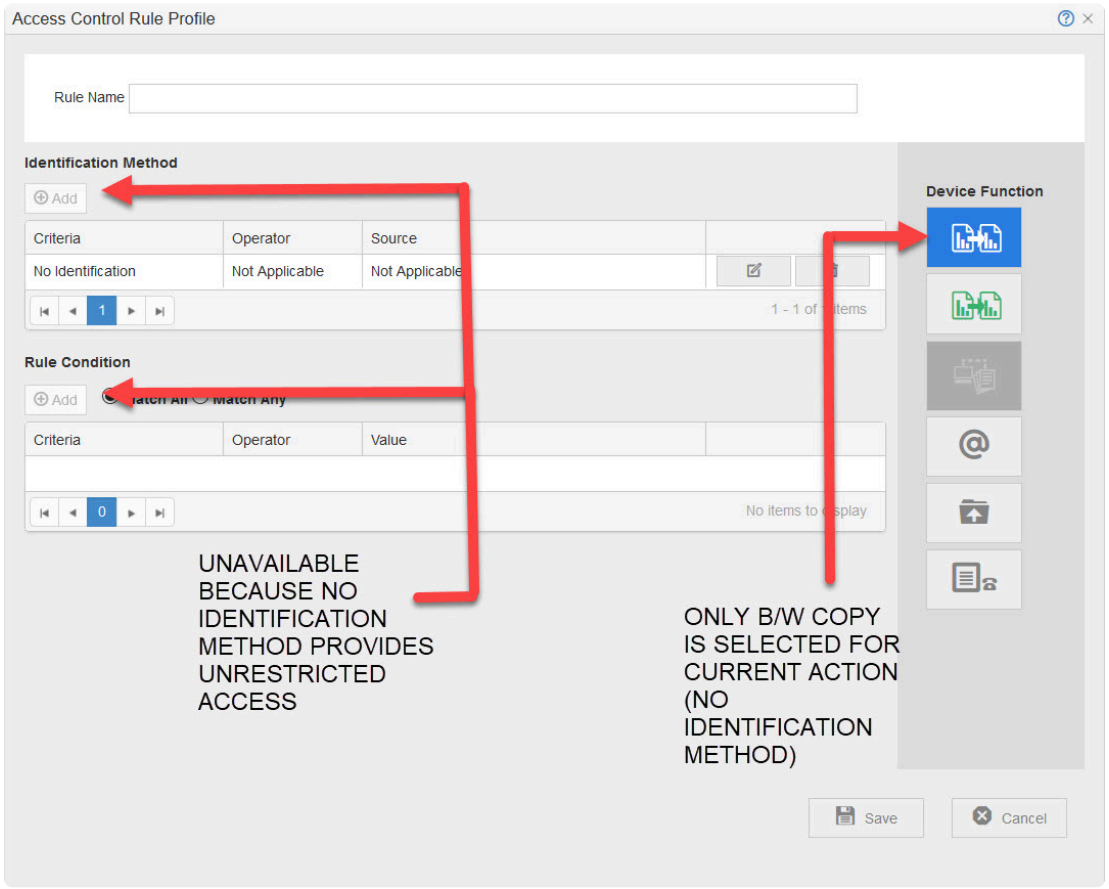
Access Control Rules define who can access which functions of a multi-function printer. Access Control Rules:

1. Unlock functions for unrestricted use, so that they can be used without authentication.
2. Enable functions you are authorized to use, when you authenticate at the printer.

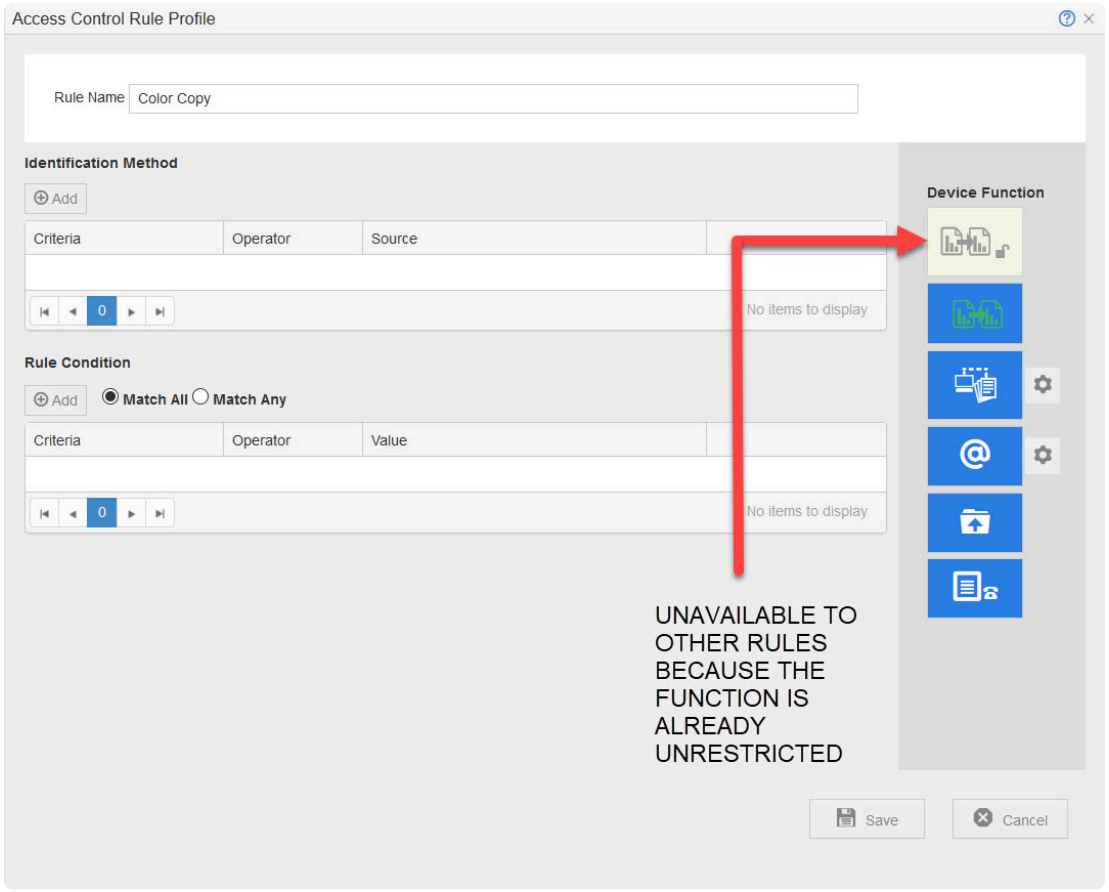
On a printer, the functions that are unlocked are available without you having to authenticate. Once you authenticate the functions you are authorized to use will also become available.

Unlock a Function for Unrestricted Access

In the example shown below, a company does not want to restrict black and white photocopying. The Access Control Rule unlocks the black and white photocopy function, making it unnecessary for anyone to authenticate at the printer for that function.



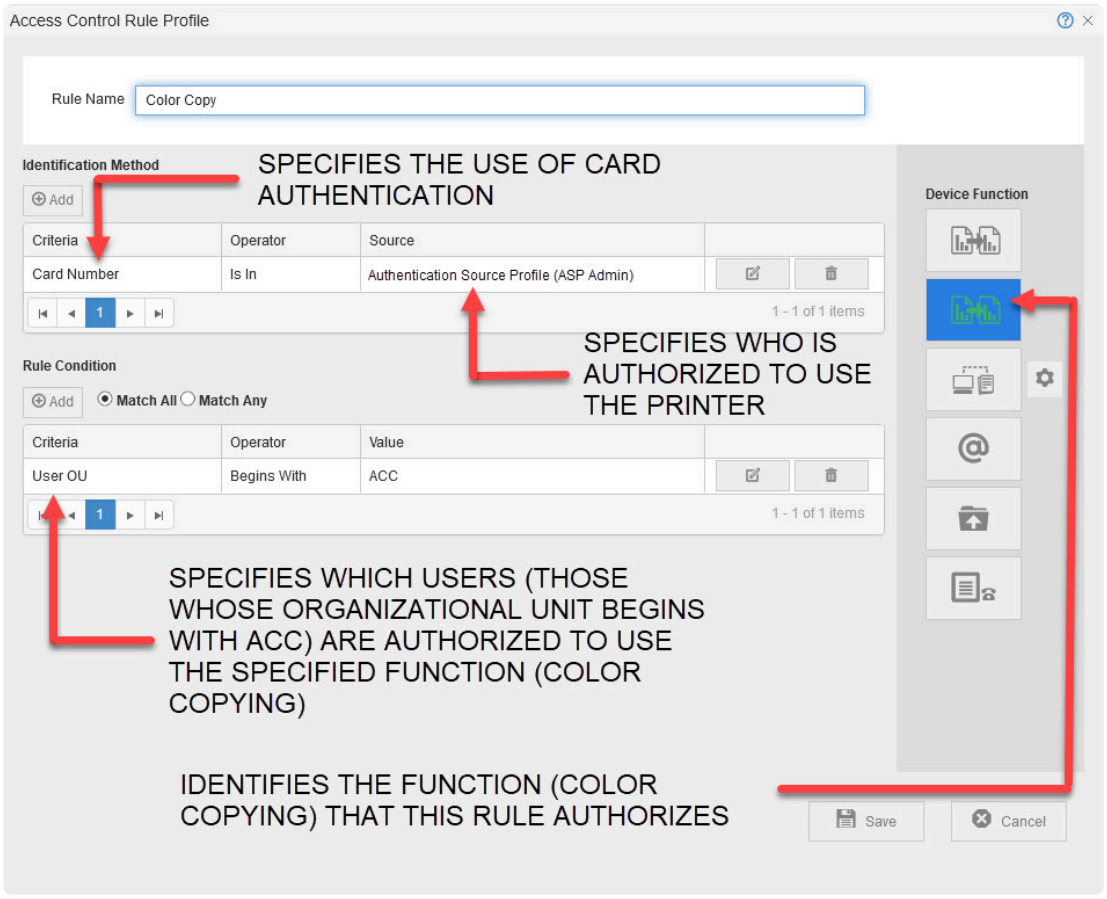
Any printer that this rule applies to does not restrict the black and white photocopy function. The other rules that apply to that printer (see the example below) cannot restrict the black and white copy function, because it is already unlocked.



Authorize a Function for a Specific Group of Users

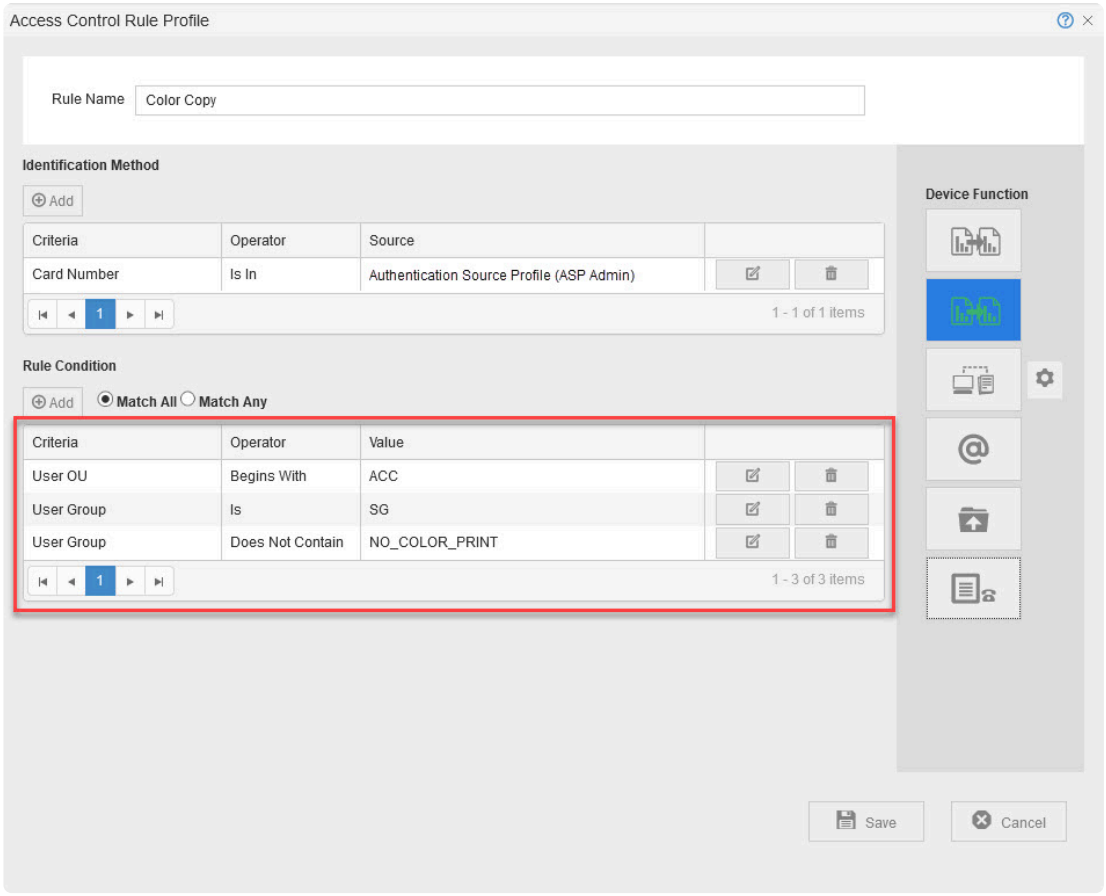
In the example shown below, the Access Control Rule specifies the following:

1. Use Card to authenticate at the printer.
2. Validate credentials against the identity management system(s) specified by *Authentication Source Profile (ASP Admin)*
3. Upon successful authentication, Authorize Color Copying only for those who belong to Organizational Groups that have names beginning with the letters ACC.



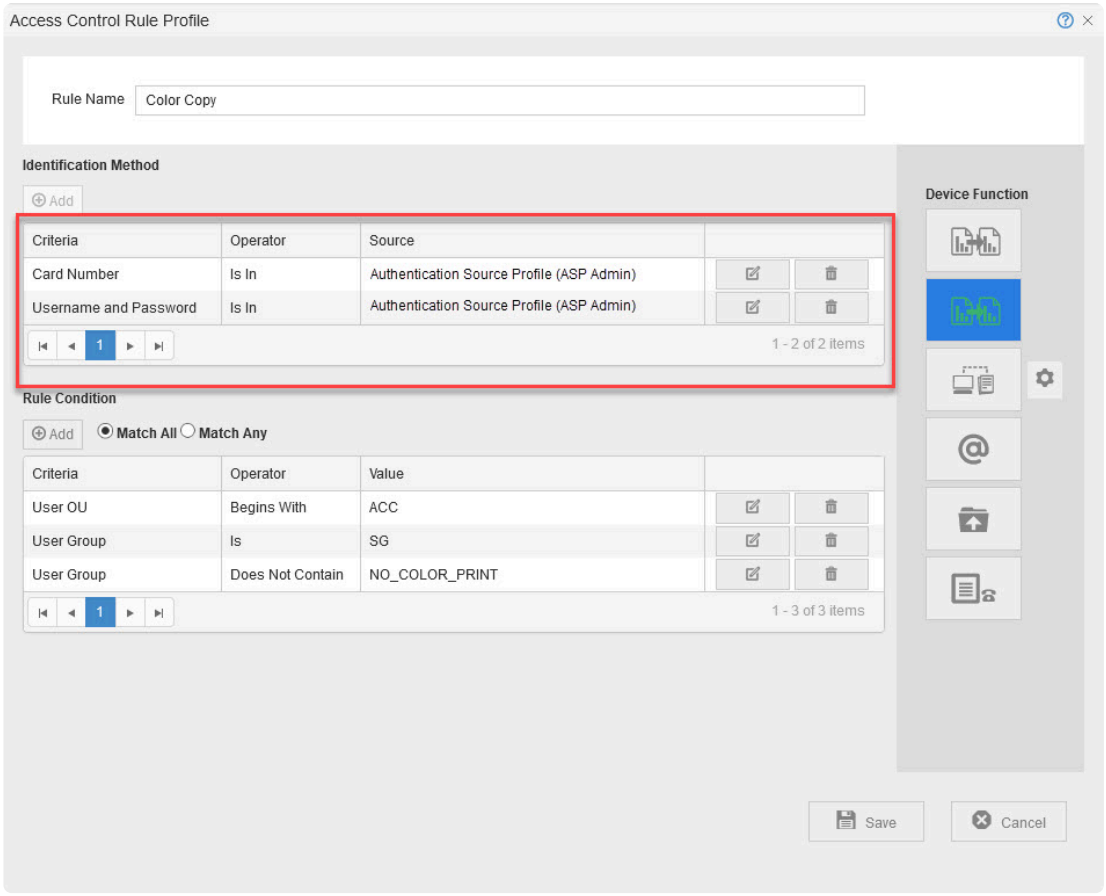
The rule can be expanded to enable more complex scenarios such as:

1. Enabling Color Copy for those who belong to Organizational Groups that have names beginning with the letters ACC, and belong to the User Group SG, but not to the User Group NO_COLOR_PRINT.

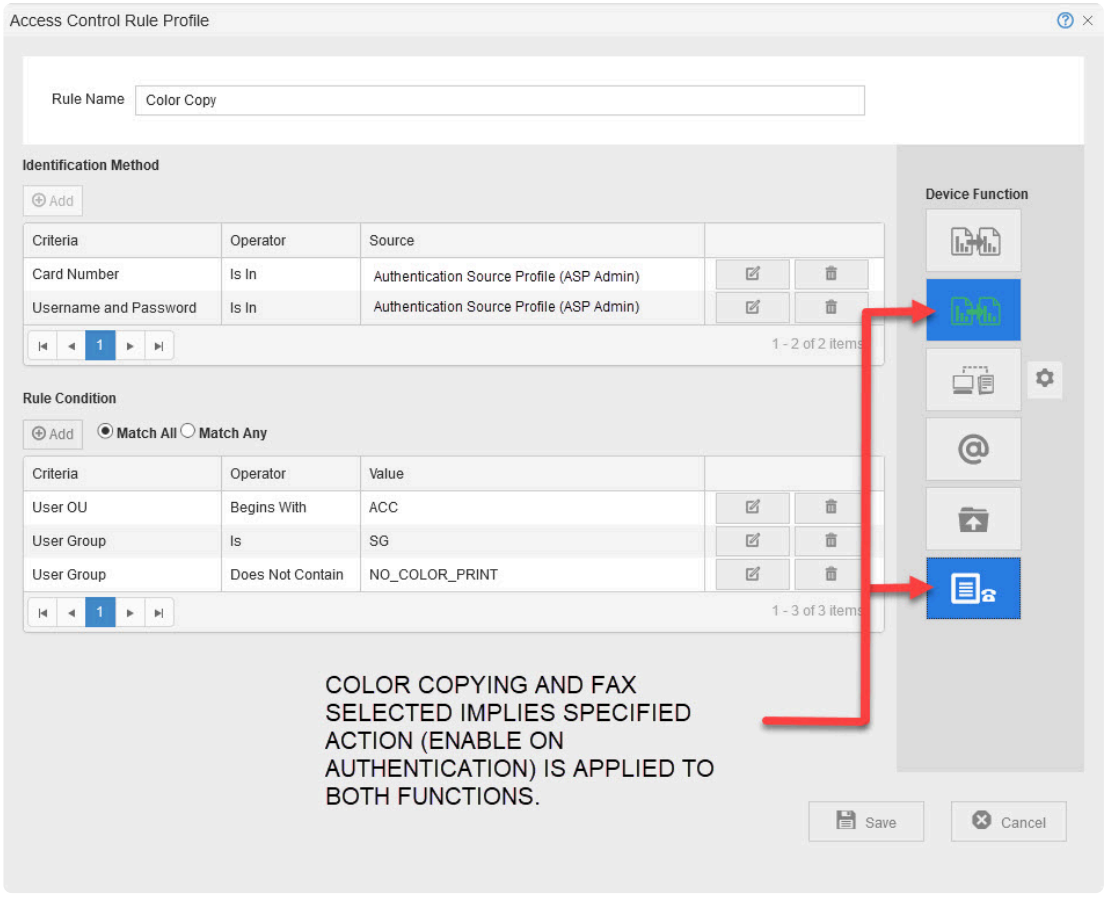


Changing the rule condition from **Match All** to **Match Any** allows for one who belongs to any one of the specified groups to have authorization to use the Color Copy Feature.

2. Allow for Card Authentication as well as User Name / Password Identification Method, so that users who forget their card can still authenticate at the printer.

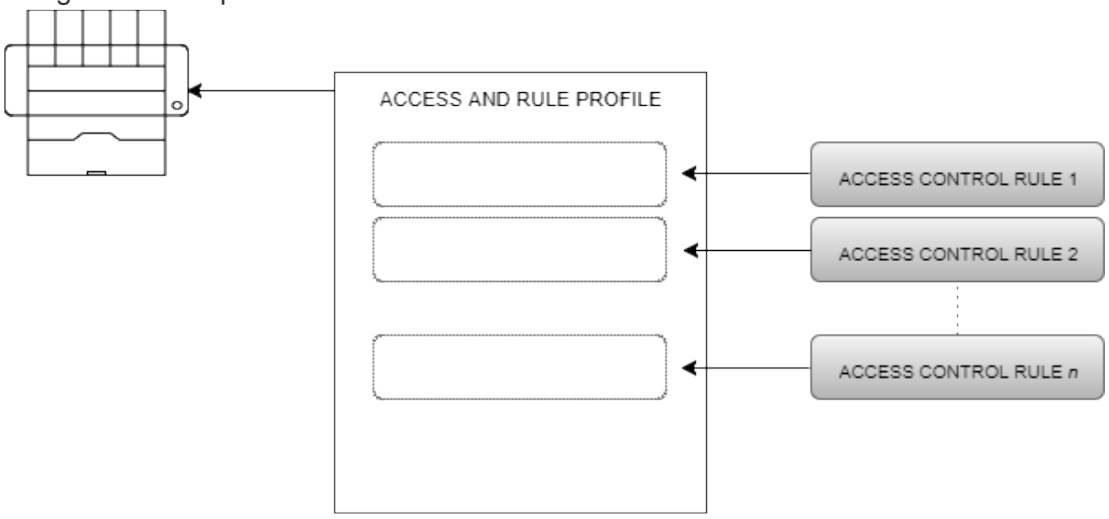


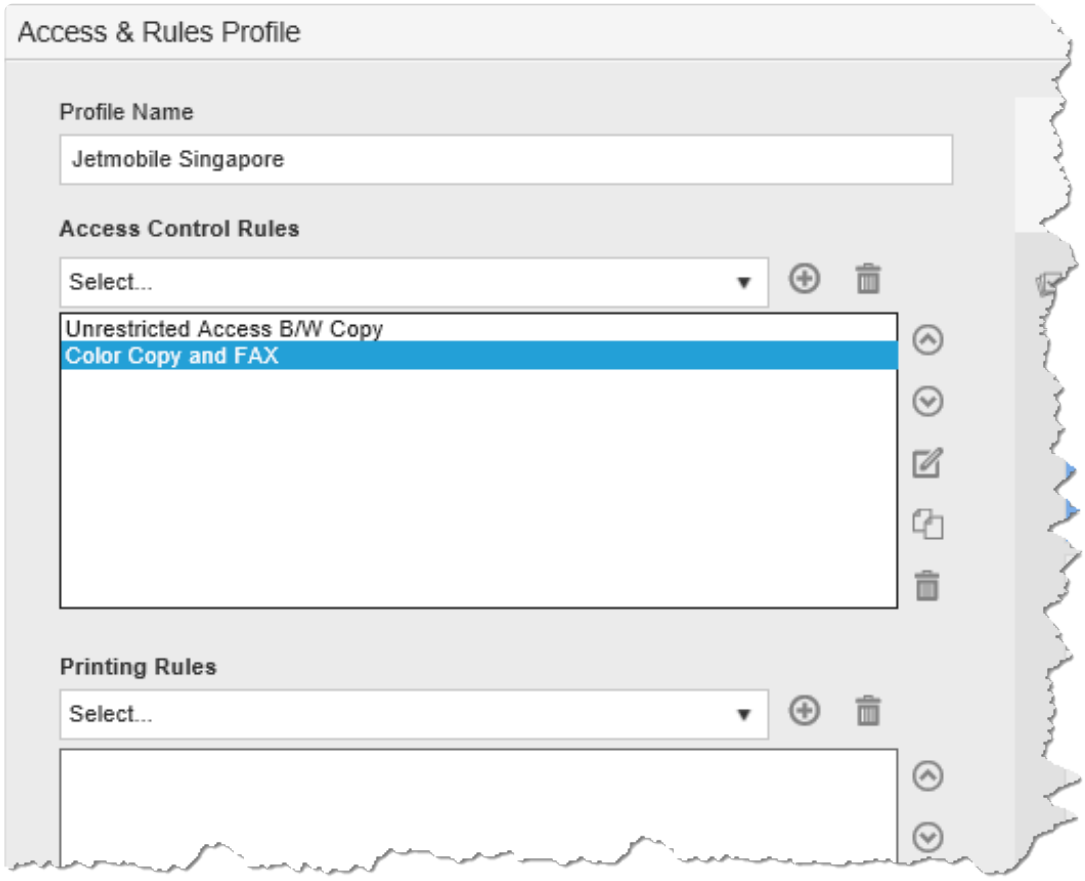
3. Enable more than one function within a single rule.



Combining Access Control Rules and Assigning them to Printers

You assign a rule to a printer by adding the rule to the Access & Rule Profile assigned to that printer. An Access & Rule Profile is a named collection of rules. When you authenticate at a printer, the availability of functions is determined by the combination of the Access Control Rules in the Access & Rule Profile assigned to that printer.

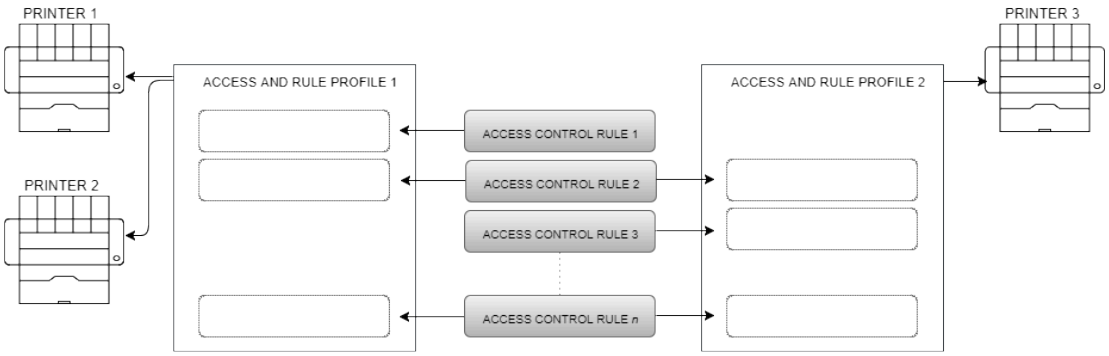




One Access & Rule Profile can be assigned to many printers. This eliminates the need to set rules for each printer individually. Furthermore, if you add, remove or change a rule, all printers controlled by that Access and Rule Profile are updated.

Similarly, one Access rule can be assigned to more than one Access & Rule Profile. Changing the rule will update all such Access & Rule Profiles, and hence, all printers that use those Access & Rule

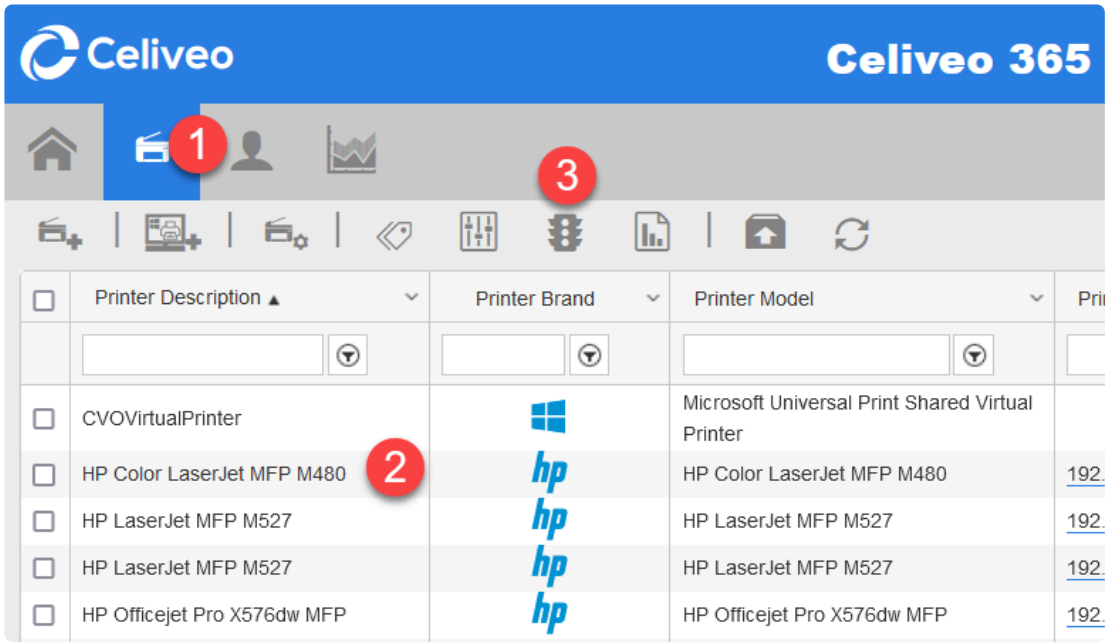
Profiles.



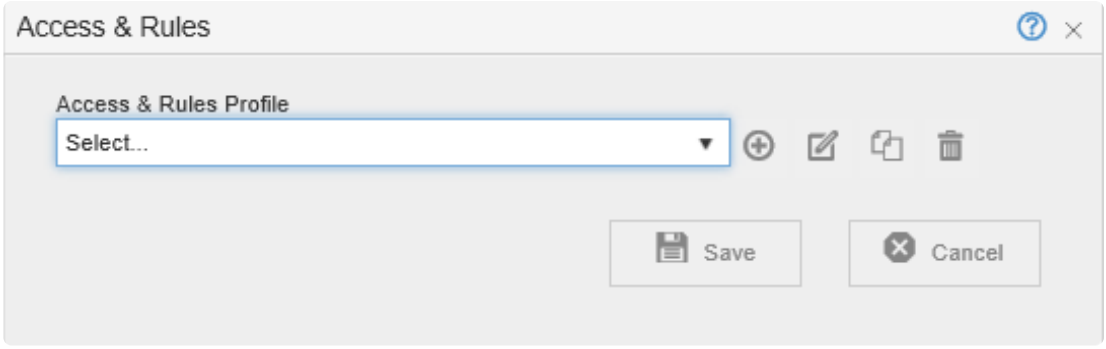
How to…

Create a New Access & Rule Profile

You create a new Access & Rules Profile while assigning it to a printer.

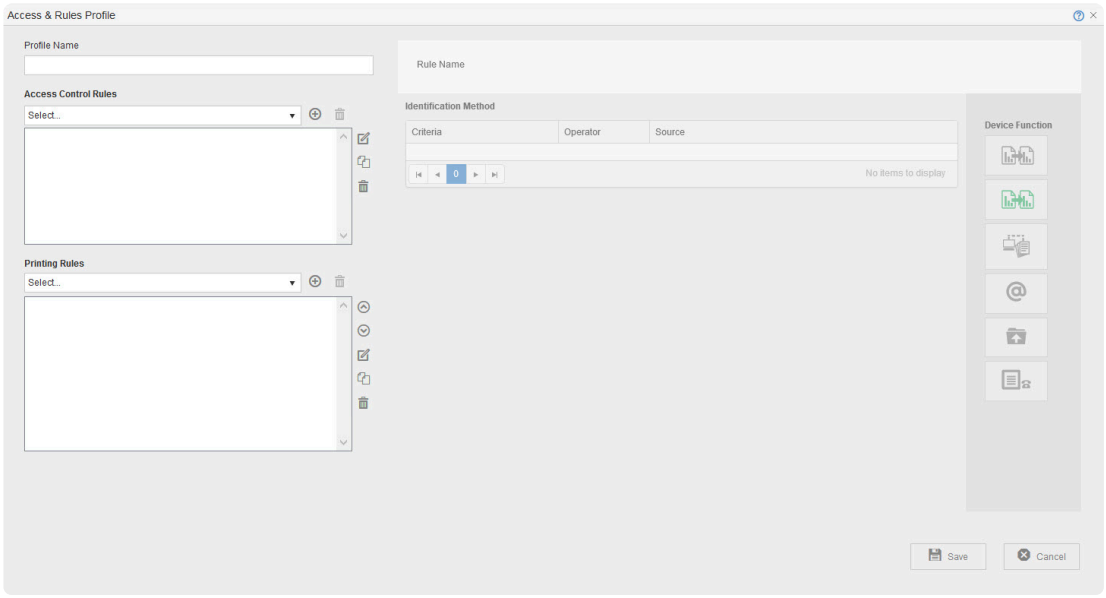


1. On the Celiveo Web Admin, at the main menu, click . The Printer List displays.
2. Select the Printer you want to add the new Access & Rules Profile to.
3. On the printer menu, click . Access and Rules is displayed.



4. To create an empty Access & Rules Profile, click .
   To create a new Access & Rules Profile by cloning an existing rule, select the existing rule from

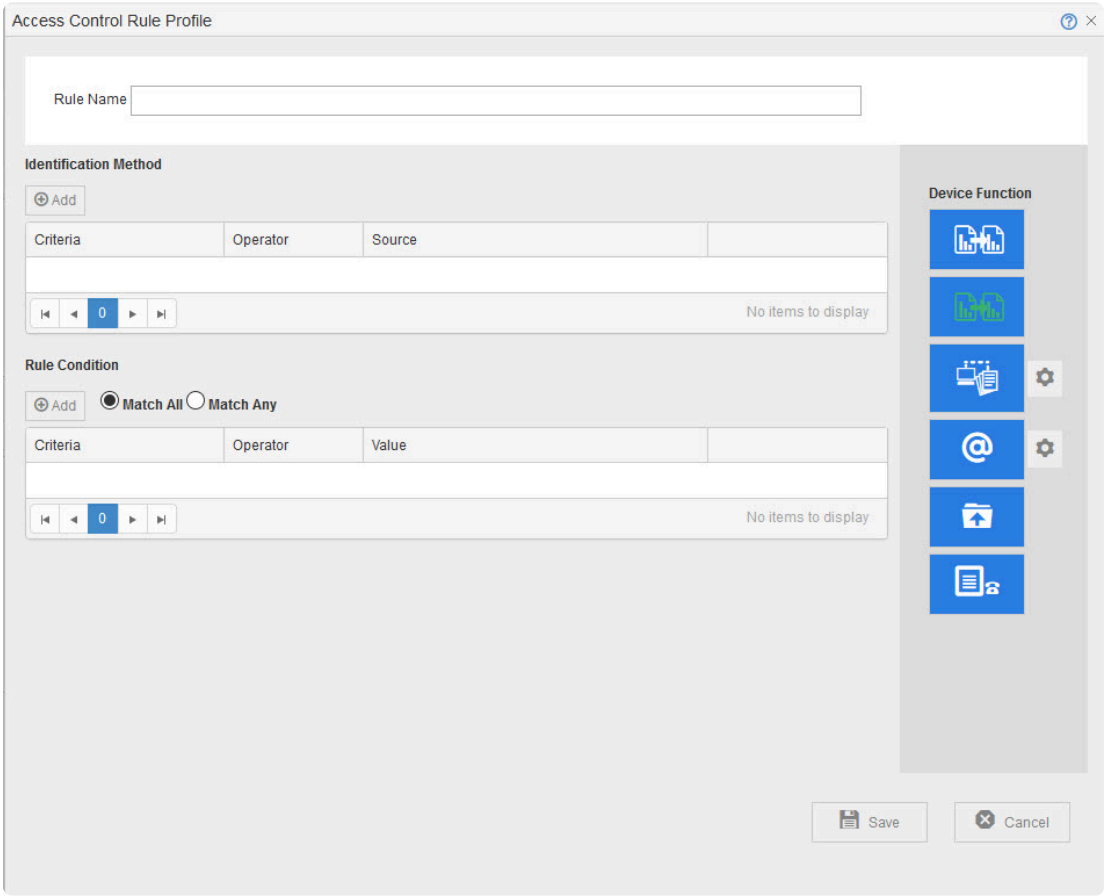
the drop-down and click . The Access & Rules Profile is displayed.



5. In the **[Profile Name]** box, specify a unique name for the Access & Rules Profile. The new Access & Rules Profile is created when you save it.

Add a Rule to Unlock a Function

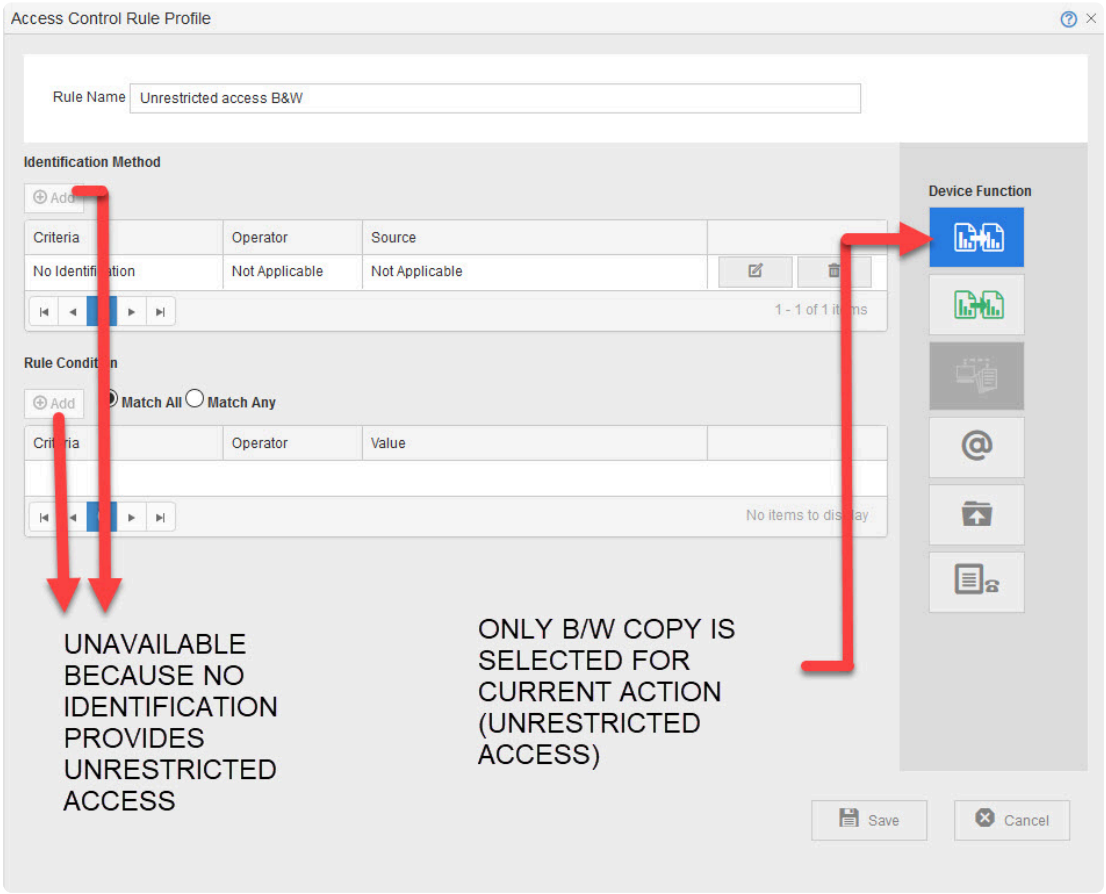
1. In Access & Rule Profile, click adjacent to **[Access Control Rules]** drop-down. A new rule displays.



2. At **[Rule Name]** specify a name for the rule.
3. In the **[Device Functions]** section, click the different buttons to deactivate all features but Black

and White Copy.

4. In the **[Identification Method]** section, select **No identification**.



5. Click **[Save]**.

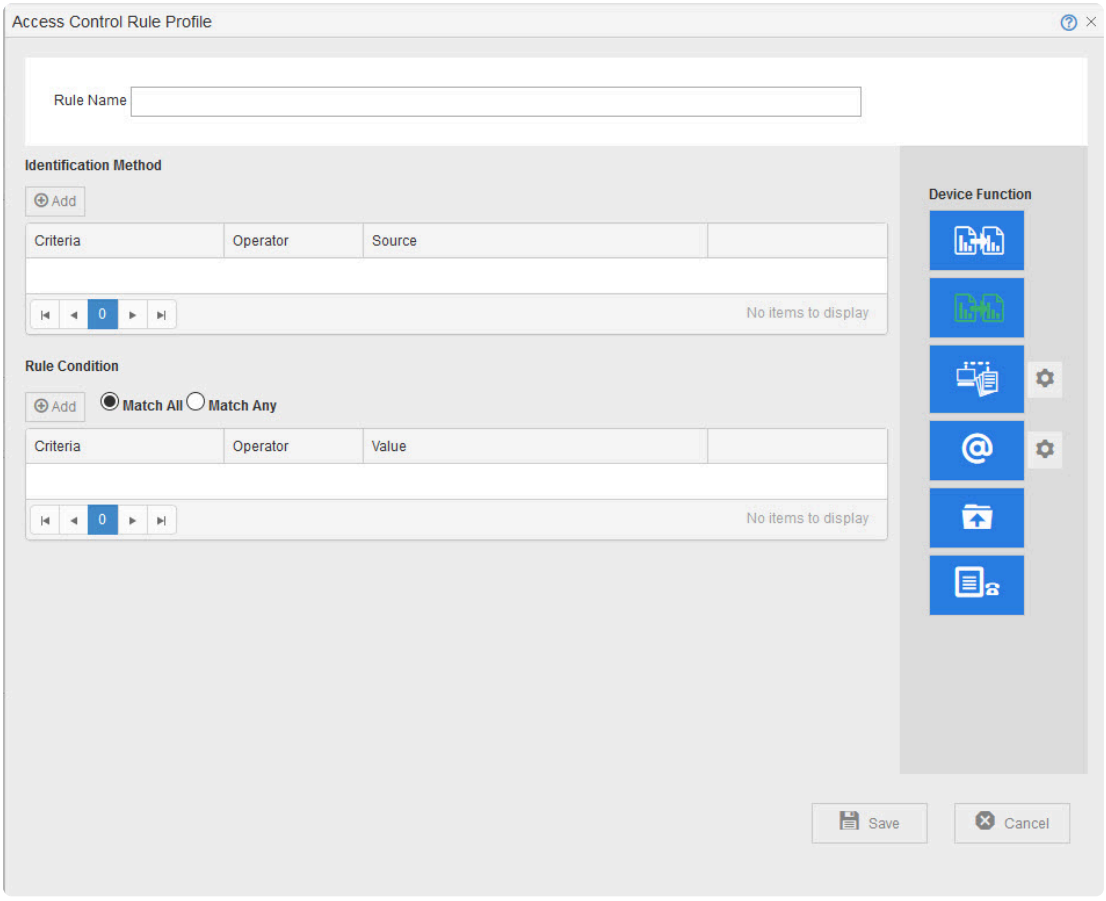
Authorize a Function for SmartCard/Card or PIN Authentication

Authorizing a function, is a 3 stage process.

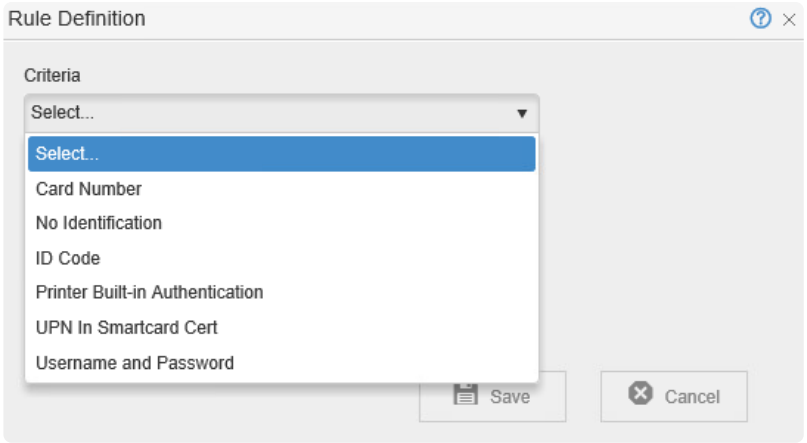
- Stage 1 – Enable Smartcard, Proximity card or PIN Authentication
- Stage 2 – Specify the function to authorize
- Stage 3 – Specify who is authorized to use the function (If all users who successfully authenticate are allowed to use the function, this stage can be skipped)

Stage 1:

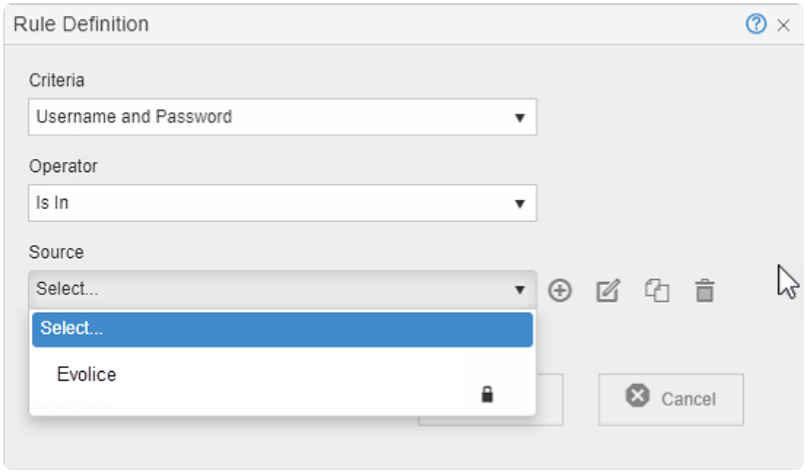
1. In Access & Rule Profile, click ⊕ adjacent to **[Access Control Rules]** drop-down. A new rule displays within the Access & Rules Profile.



2. At **[Rule Name]** specify a name for the rule.
3. In the Access Control Rule Profile, In the **[Identification Method]** section, click ⊕. The Rule Definition is displayed.
4. In the **[Criteria]** drop-down, select **[Card Number]** for Card Authentication, **[ID Code]** for IC Code Authentication or **[UPN in Smartcard Cert]** for Smartcard Authentication.



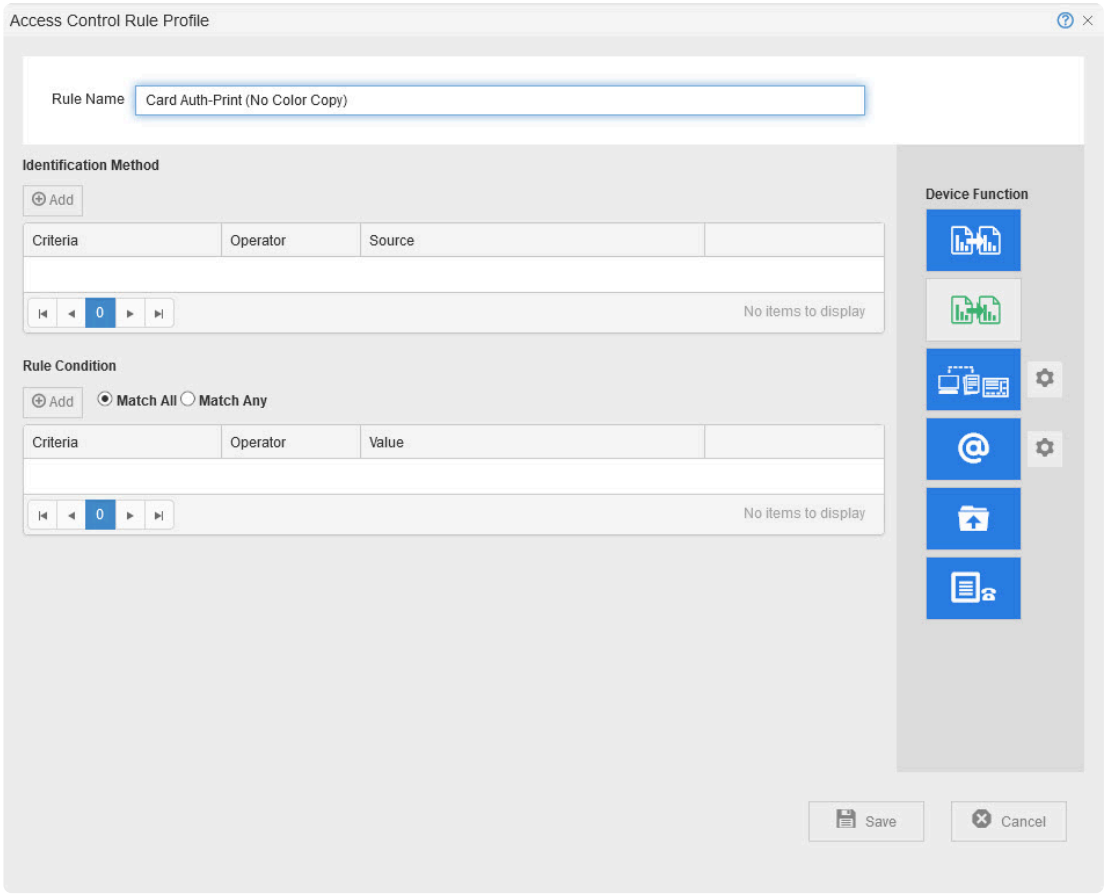
5. In the **Source** drop-down, select the Authentication Source Profile to authenticate against.



Notes:

- For information on Authentication Profiles, see the article on Authentication Profiles.
- The system ensures that all Card Authentication Access Control Rules for a given printer are authenticated against the same Authentication Profile.
- For more information about Authentication Profile, refer to About Authentication Profiles.
- You can combine Card Authentication with the User Name/Password method in the same Access Control Rule.
- A Smartcard license feature connector is required to use **[UPN In Smartcard Cert]**.
- **[UPN In Smartcard Cert]** rule can only be combined with **[Username and Password]**.
- **[UPN In Smartcard Certification]** rule cannot be used with the **[Celiveo Authentication Gateway]** authentication method.

6. Click **[Save]**. You return to the Access Control Rule Profile.



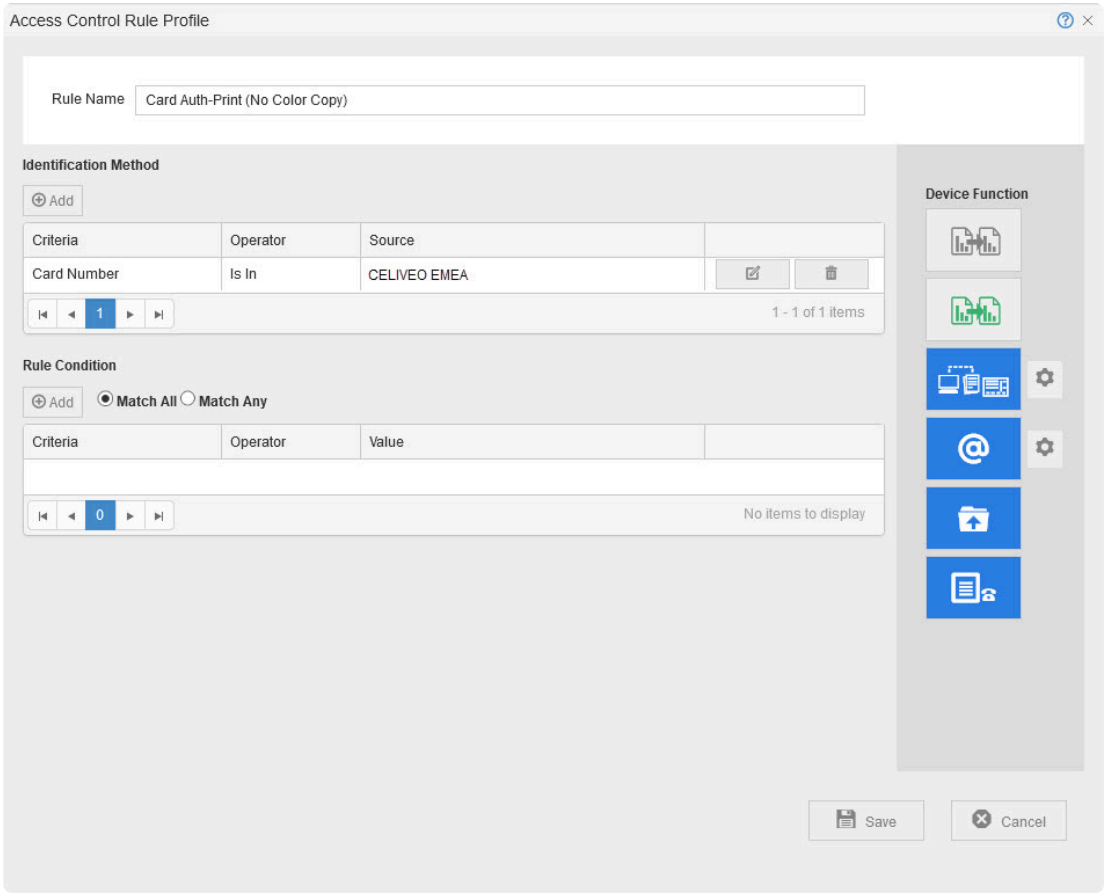
Stage 2

1. In the **[Device Functions]** section, select the features you want to authorize. The features you select are displayed as blue buttons.

Notes:

- If you selected Scan to Email, click ⚙ and specify who to send the scanned image to.
- If you selected Print, click ⚙ and specify the pull print settings.

Tip: Use the Celiveo CSS option only if you are upgrading from SecureJet 7.0.5/6 or Celiveo 8.0.x.



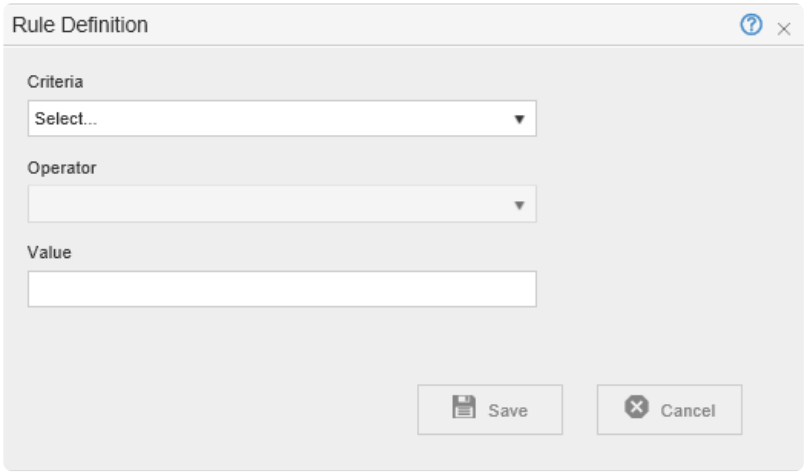
Stage 3

To grant permission for a user group or organizational unit:

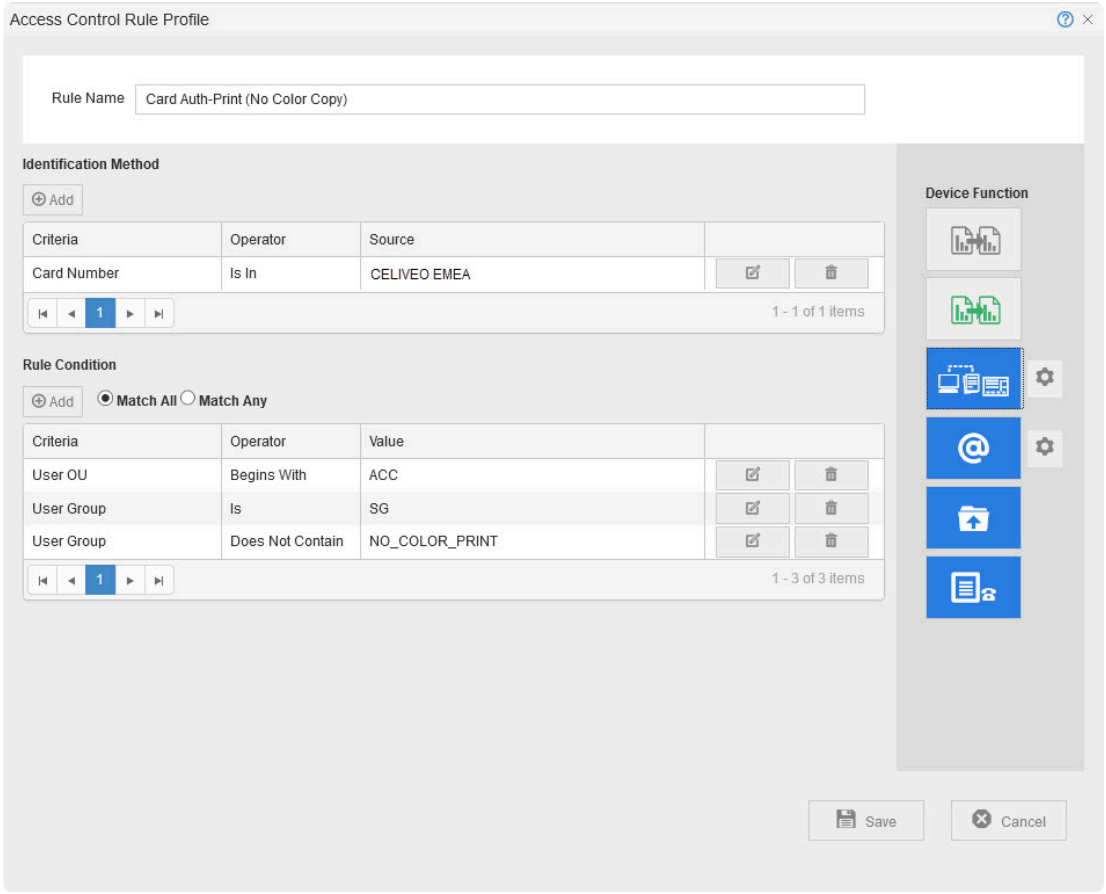
Note: Access Control Rules cannot be applied to a user group that is a Primary AD group.

IMPORTANT: Rules for a Celiveo Shared Virtual Printer must not have USER OU as a criteria.

1. Under **[Rule Condition]**, click ⊕. The Rule Definition is displayed.



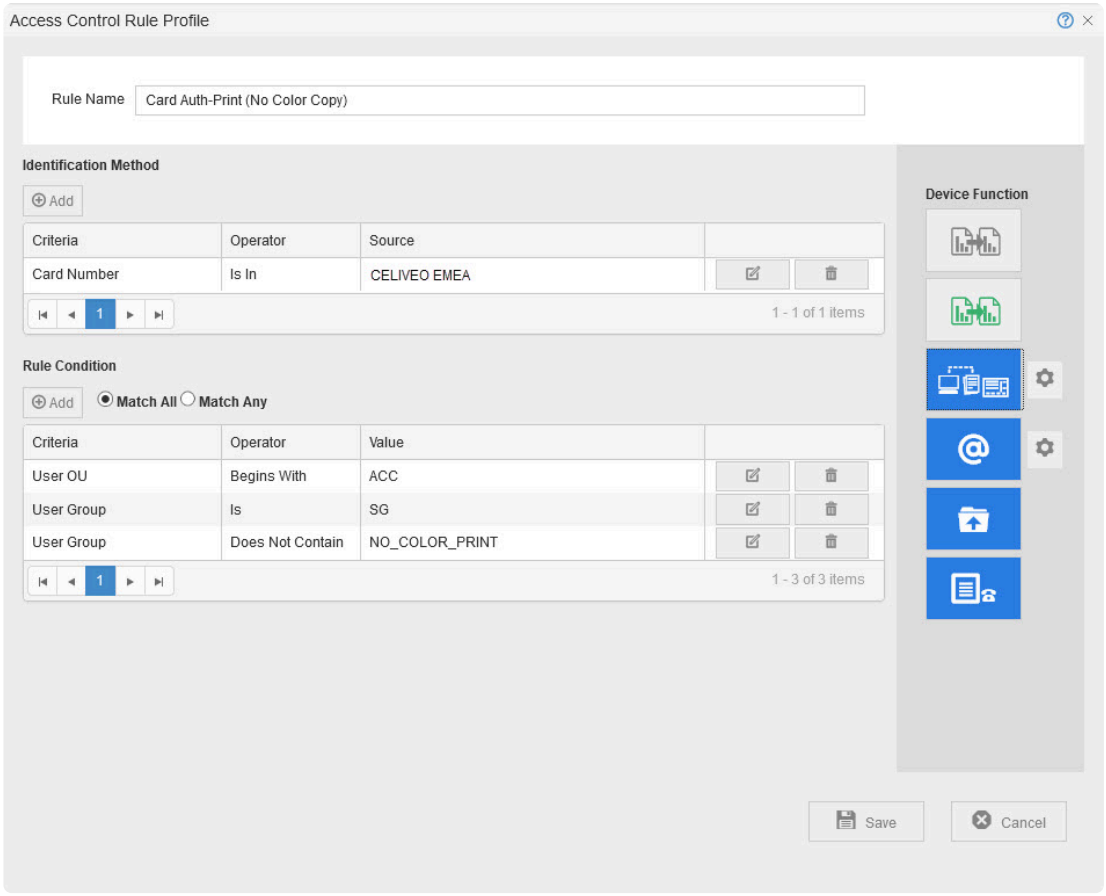
2. From the **[Criteria]** drop-down, select **User Group** or **Organizational Unit**.
3. In the **[Operator]** drop-down select the comparison criterion.
4. In the **[Value]** box, specify what to compare against .
5. **Note**: You can specify multiple rule conditions, and select **[Match Any]** to authorize the features if any one condition is met, or select **[Match All]**, to authorize the features if every condition is met.



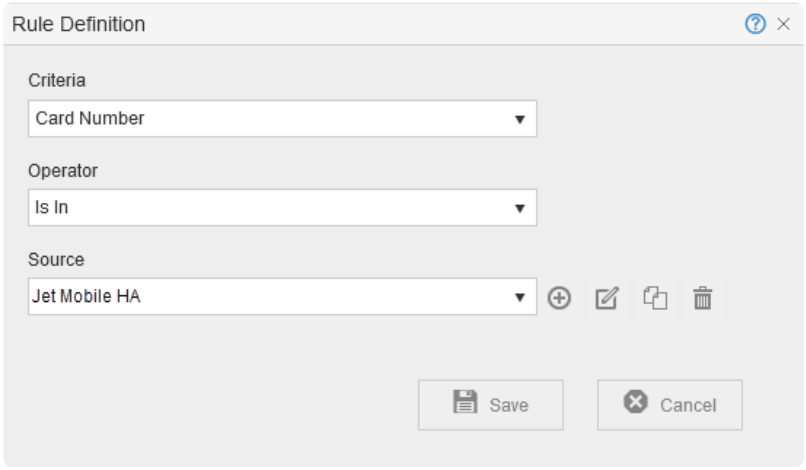
6. Click **Save** until all dialogs close.

Set Up ID Mask and Dual Factor Authorization for Card Authentication

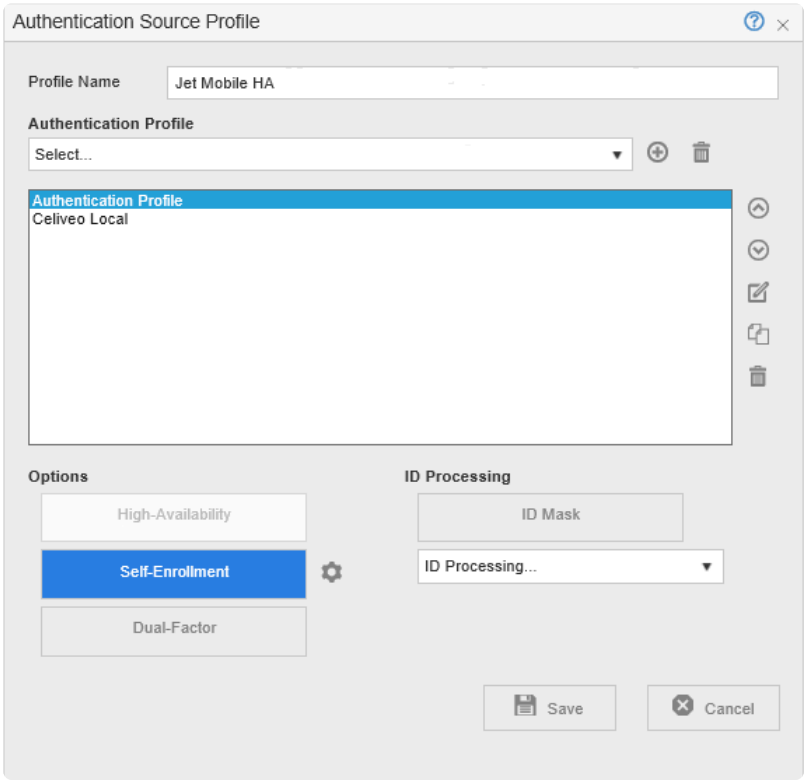
1. In Access & Rule Profile, in Access Control Rules, select the rule that implements card authentication.
2. Click ✎ under **[Access Control Rules]**. The rule displays for editing.



3. In the **[Identification Method]** section, click in the row containing the Card Number condition. The Rule definition displays.

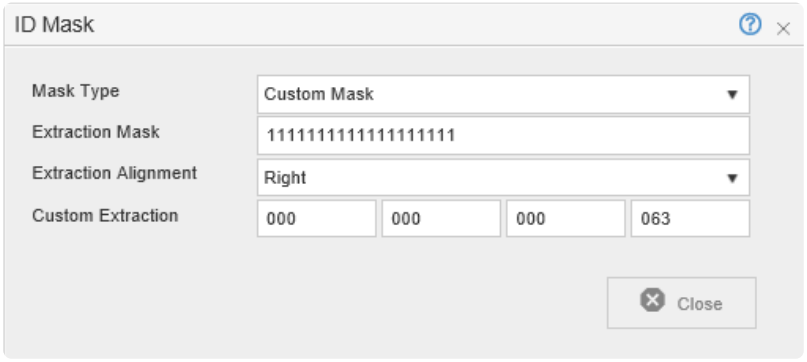


4. Click in the row containing the Source. The Authentication Source Profile displays.



To set up the ID Mask;

1. Click the **[ID Mask]** button to turn it on.
2. Click ⚙, which is placed next to **[ID Mask]**. The ID Mask displays.



3. Specify the ID Mask to use to extract the card number and click **[Close]**. See this article on how to configure ID mask.
4. From the **[ID Processing]** drop-down, specify how to process the extracted card number.

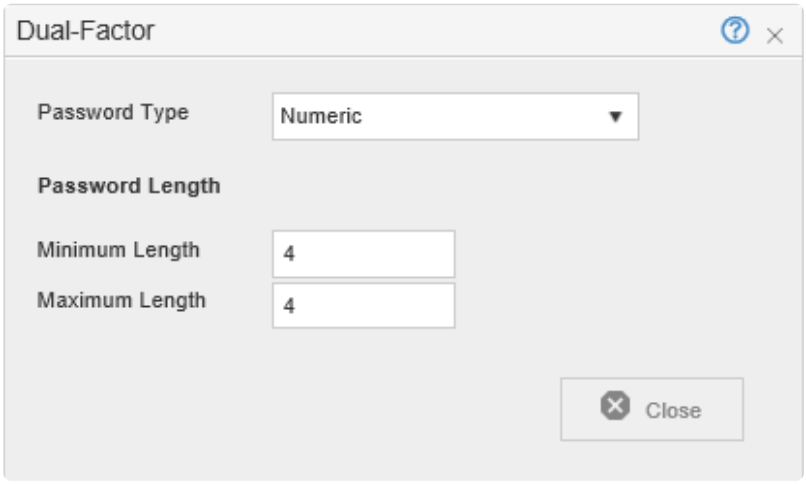
Information about ID Processing:

The ID Processing methods are used to match the number extracted from the card with the one that is written in the back of the card. These conversions are needed when the card ID in Celiveo has to match the numbers in the back of the card or if they need to correspond to an existing number in a database that would be imported to AD or Celiveo SQL DB.

To enable dual factor authentication;

1. Click the **[Dual Factor]** button to turn it on.

2. Click ⚙, which is placed next to the **[Dual Factor]** button.

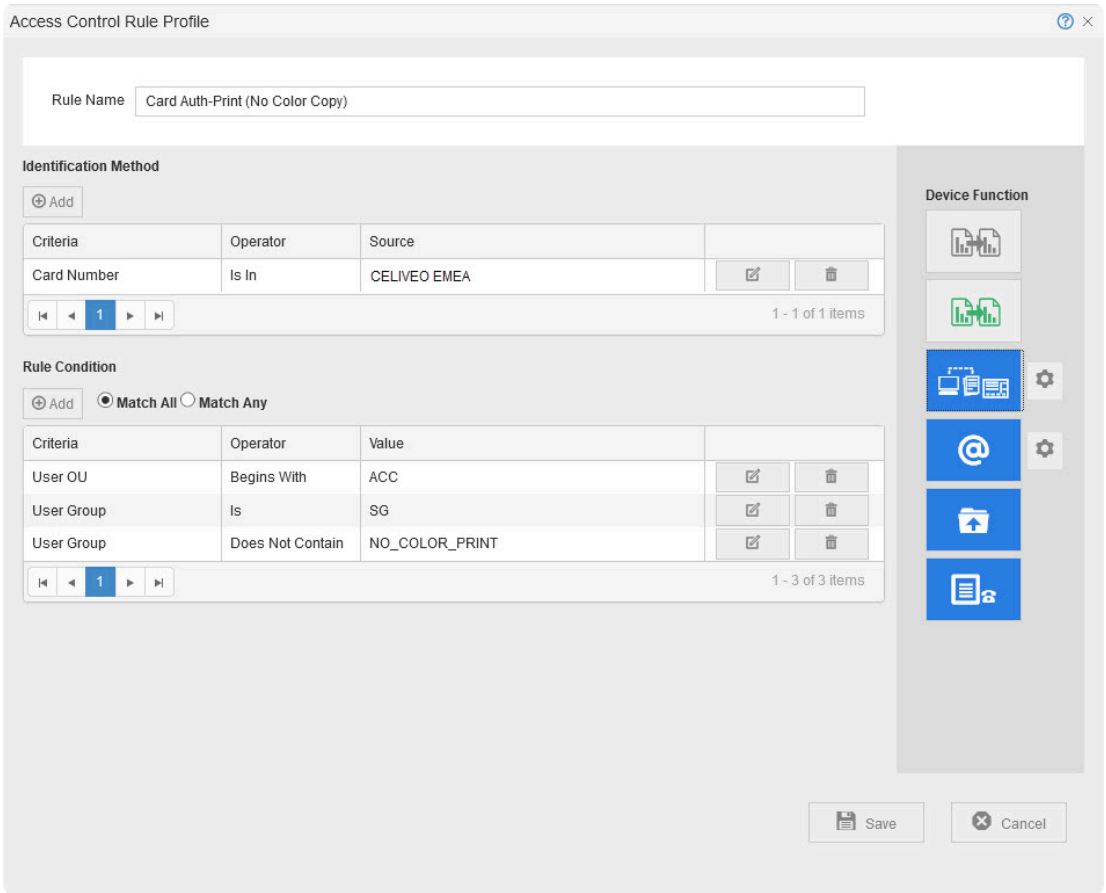


3. Specify properties of the password to use and click **[Close]**.
4. Click **Save**.

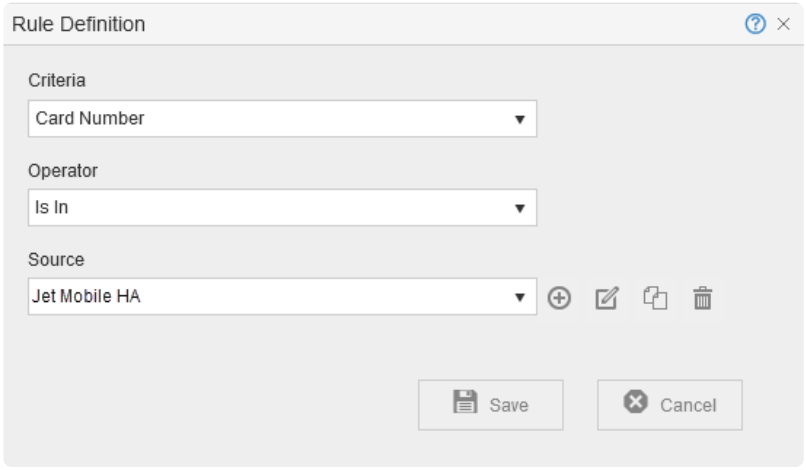
Enable Self Enrollment for Card Authentication

When self enrollment is enabled, you can log in at the printer using your Windows credentials. Thereafter you can save your card details to Celiveo, without the help of a Celiveo Administrator.

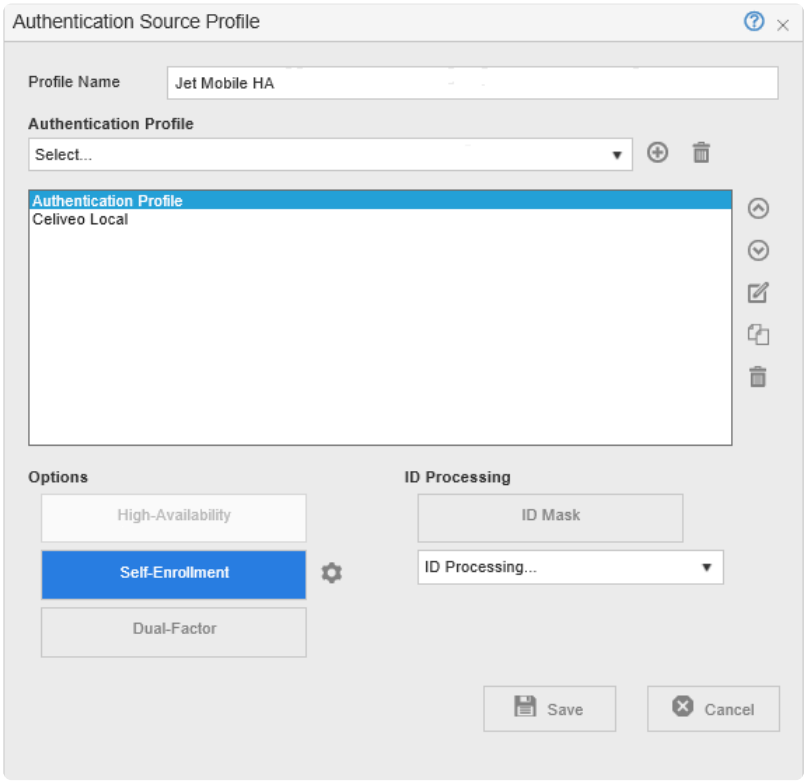
1. In Access & Rule Profile, in Access Control Rules, select the rule that implements card authentication.
2. Click ✎ under **[Access Control Rules]**. The rule displays for editing.



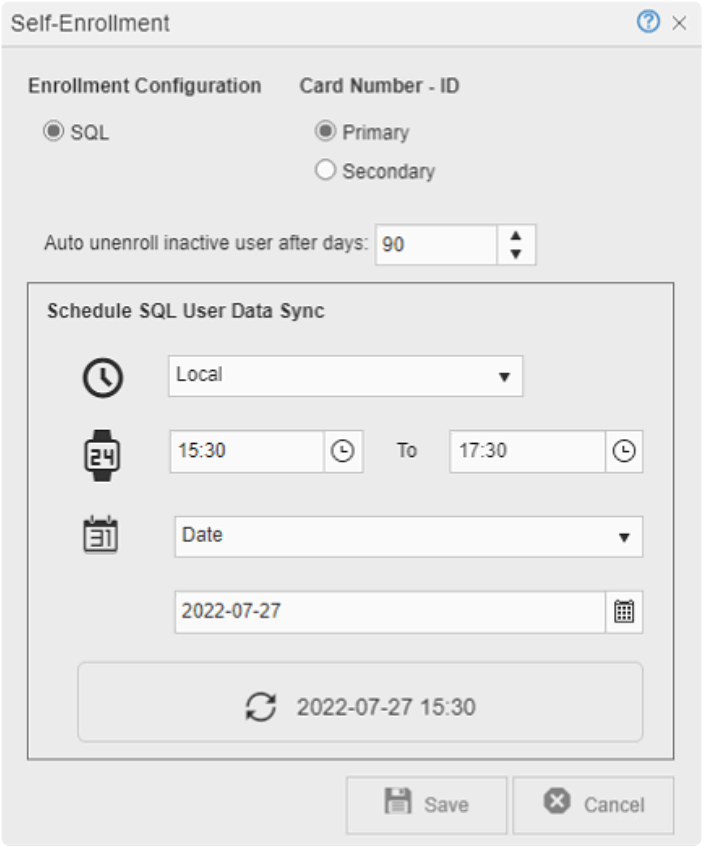
3. In the **[Identification Method]** section, click in the row containing the Card Number condition. The Rule definition displays.



4. Click in the row containing the Source. The Authentication Source Profile displays.



5. Verify that the Self Enrollment is turned on (The Self Enrollment button is highlighted in blue when Self Enrollment is on).
6. Click , which is placed next to the **[Self Enrollment]** button. The Self Enrollment settings display.



UNENROLL INACTIVE USERS

To help the IT administrator keep the database up to date, you can set a time frame to automatically remove an inactive user.

At **[Auto unenroll inactive user after days]**, enter the number of days.

An enrolled user who has not used the Celiveo system after the specified number of days is automatically removed.

Note: If enrollment into AD is selected, to avoid any error, make sure that the **Last Activity Field Name** of the Active Directory fields is documented and that the field has read/write rights for the indicated AD service account. This can be set up in the Advanced Section of the Authentication Profile settings. To learn more, see the information about the advanced settings of an authentication profile.

1. To save card info in the Celiveo database:
   a. Select **[SQL]**.
   b. In the **[Schedule SQL User Data Sync]** section, specify when and how often user information should be synced with the Authentication Server.
2. To save card information on the Authentication Server, select **[AD/LDAP]**.
   See the information about the advanced settings of an authentication profile to see where card information is saved.
3. Close all dialogs.

Last modified: 29 September 2022

11.2. Authentication Profiles

Contents

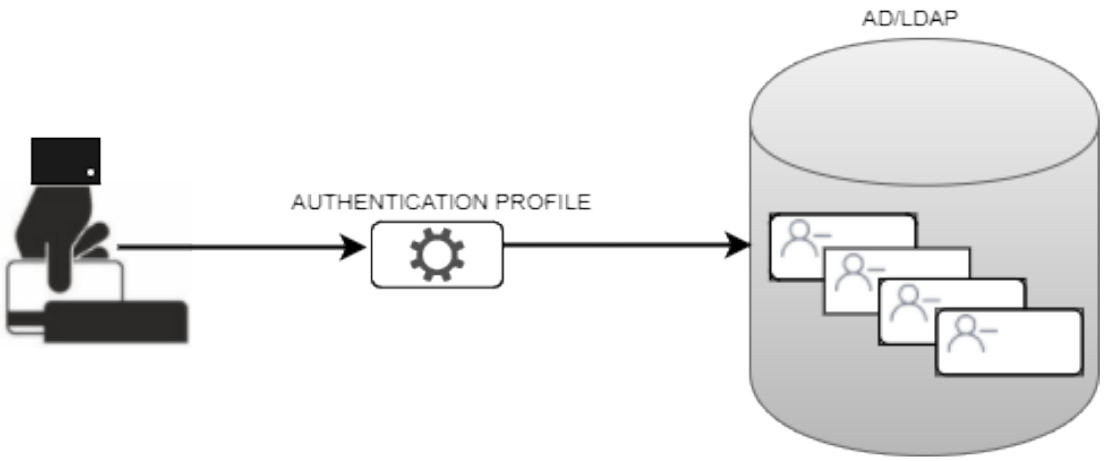
1. About Authentication Profiles
   a. What are Authentication Profiles?
   b. Settings Specified in an Authentication Profile
   c. Authentication Profiles in Access Control Rules
   d. Optimizing Authentication for Large Organizations
   e. Additional Settings in an Authentication Profile

2. How to…
   a. Create a New Authentication Source Profile
   b. Create and Add an Authentication Profile to an Authentication Source Profile
   c. Create a New Authentication Profile

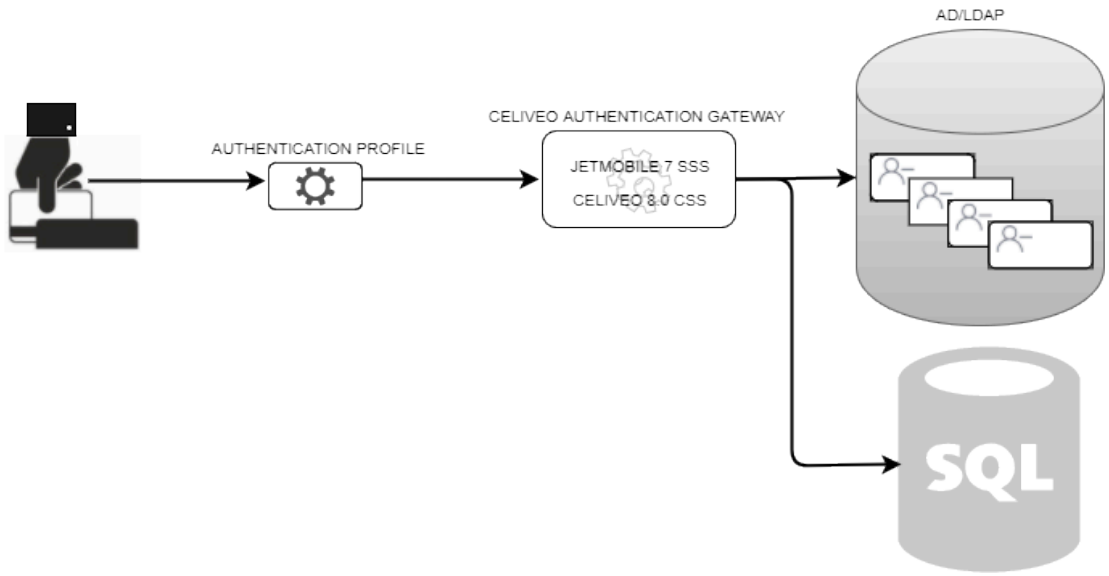
About Authentication Profiles

What are Authentication Profiles?

Authentication Profiles contain the settings that Celiveo uses to query an Authentication Server and retrieve a list of users (who typically are authorized to access Celiveo-enabled printers). Celiveo works with Microsoft's Active Directory (AD), the directory service used by Microsoft Windows for identity management, using the vendor neutral Lightweight Directory Access Protocol (LDAP).



If you already have a running installation of SecureJet 7 or Celiveo 8.0.x, you can connect to the Celiveo Authentication Gateway instead of connecting directly to AD/LDAP. By connecting to the Celiveo Authentication Gateway, you avoid having to set up the authentication mechanism all over again.



However, connecting to the Authentication Gateway deprives you of the performance improvements introduced with the current version of Celiveo. For example, the ability to optimize authentication for large organizations.

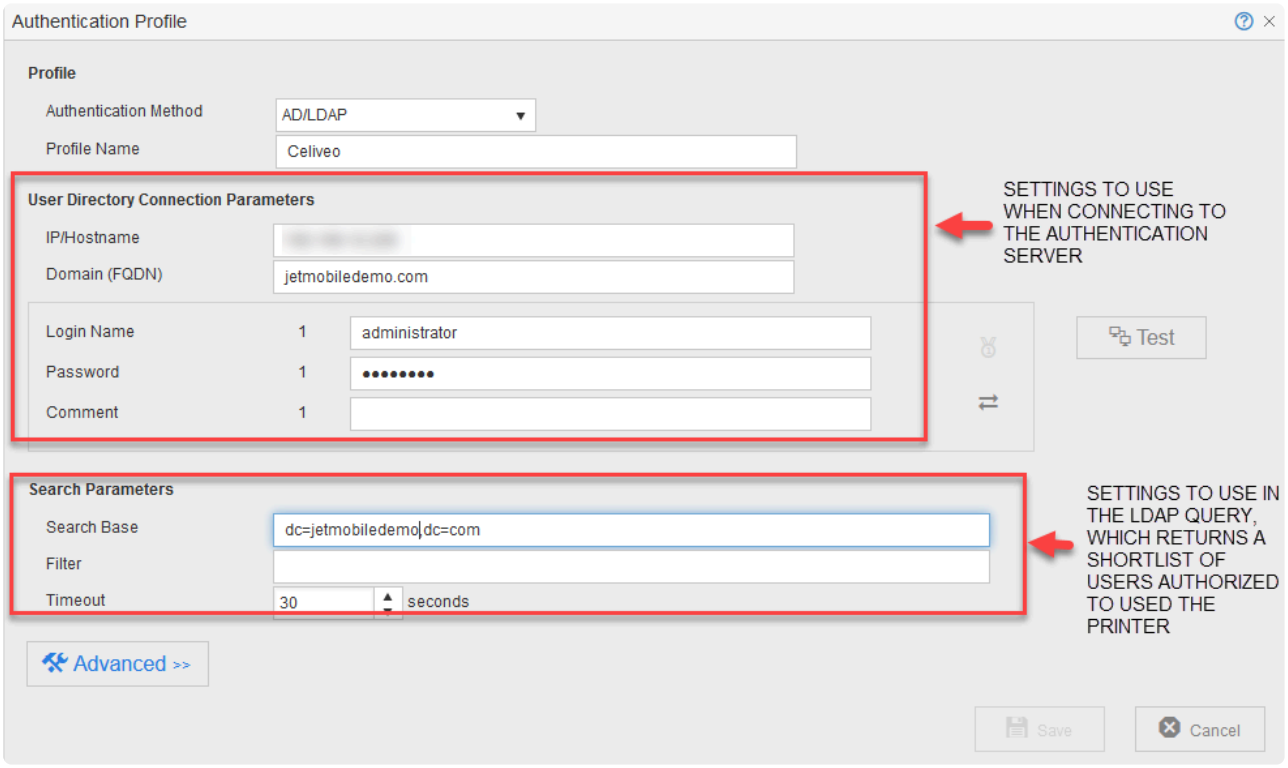
Settings Specified in an Authentication Profile

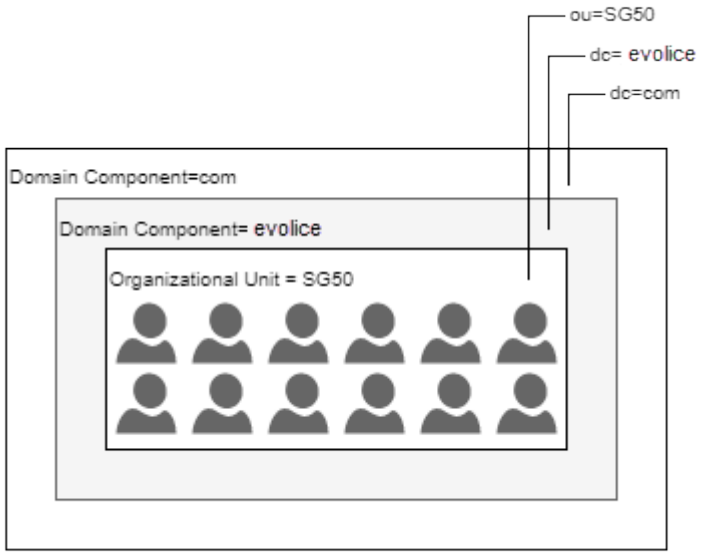
The basic settings of an authentication profile specify:

1. Settings to open a connection to an Authentication Server.
2. LDAP search parameters that results in a shortlist of authorized users.

The example shown below:

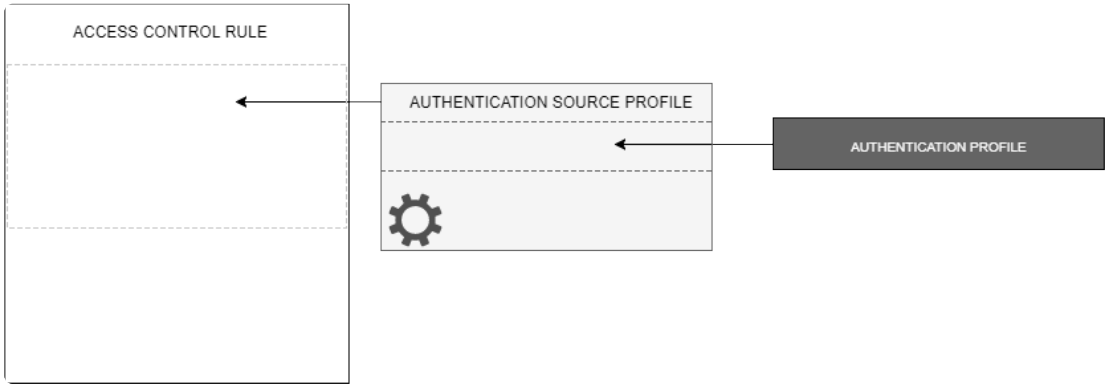
- Connects to 192.168.12.200 (the Authentication Server hosting the AD Database for the domain jetmobiledemo.com).
- Shortlist users who are part of the Organizational Unit SG50 (OU=SG50).





Authentication Profiles in Access Control Rules

Access Control Rules connect to Authentication Profiles through Authentication Source Profiles.



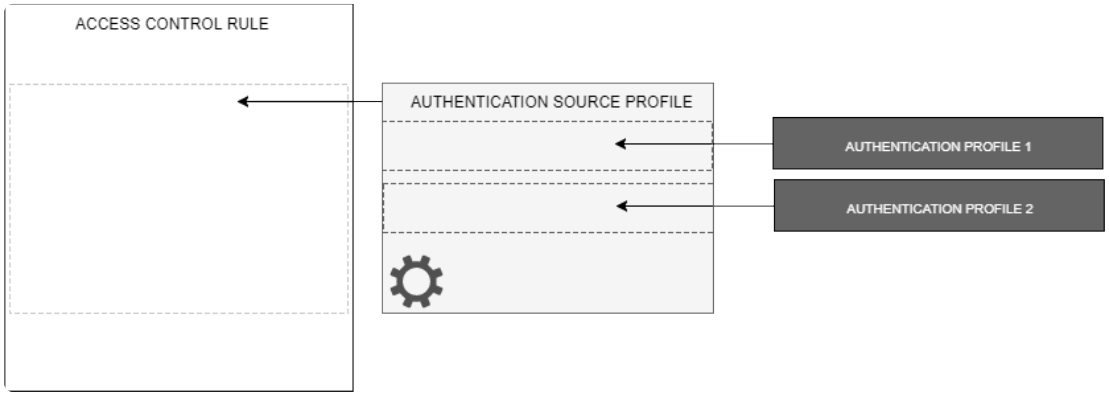
An Authentication Source Profile supplements Authentication Profile by carrying additional information

that may be required by an Authentication Profile. For example, the mask used to extract the employee id from an employee card.

Optimizing Authentication for Large Organizations

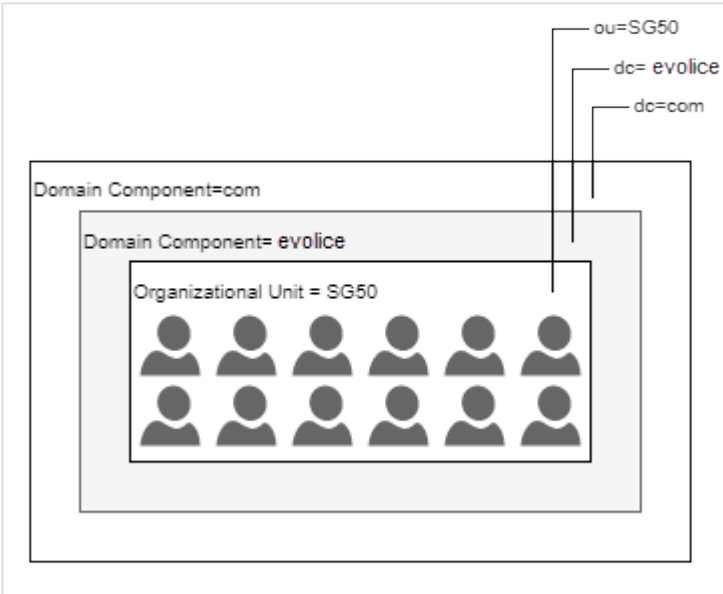
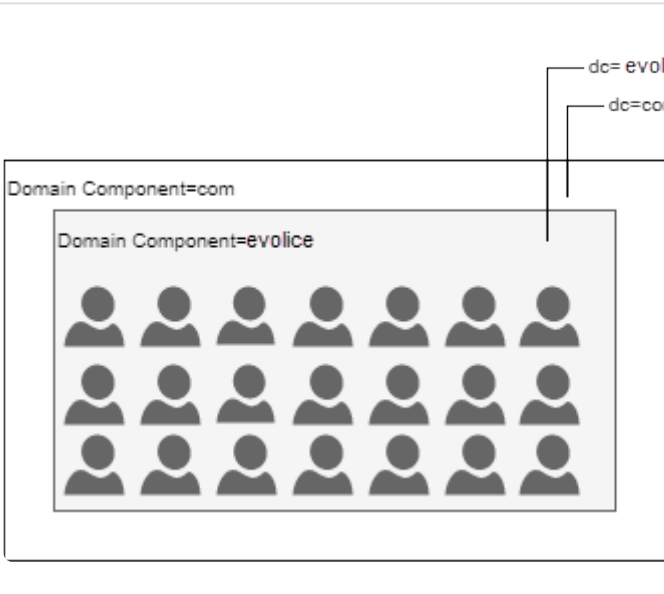
Enterprise

In large organizations, where the number of users is considerably high, or is geographically distributed, authentication may take time. The Enterprise Version of Celiveo provides a work-around for this bottleneck. The Enterprise Version supports the ability for an Authentication Source Profile to contain multiple Authentication Profiles.



If authentication fails on the first Authentication Profile, the system automatically falls back on to the next profile. By setting up more restrictive but faster Authentication Profiles to be processed before the less restrictive but larger ones, you can speed up authentication for regular users.

For example, supposing a large company has offices distributed across the globe, you can set up one authentication profile exclusively for employees of one office (OU=SG50 in the illustration below) and another less restrictive one for the entire company. Both Authentication Profiles are then assigned to the printers in that office.

	
Authentication Profile 1	**Authentication Profile 2**

When SG50 employees authenticate at a printer, Authentication Profile 1 is able to handle their authentication. Supposing a visitor from another office of the same organization visits the SG50 office,

Authentication Profile 2 is able to handle their Authentication. SG50 employees are able to authenticate faster than the visiting employee because Authentication Profile 1 ensures that the system has to deal only with the SG50 employees. The visiting employee will take longer to authenticate because Authentication Profile 2 results in a larger number of users to look up. This technique (of falling back on a secondary authentication profile when authentication against a main profile is unsuccessful) helps to cover all of the company's employees, while allowing the SG50 office employees enjoy faster authentication.

Additional Settings in an Authentication Profile

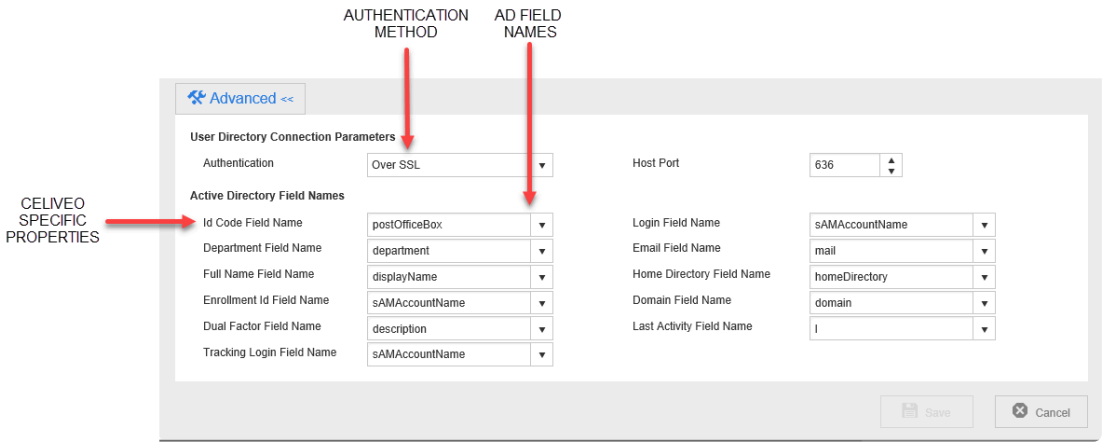
The Advanced settings are important only if you choose to configure the connection method (Simple or Encrypted) and /or store enrollment information on the Authentication Server, instead of the Celiveo Database.

Connection to the Authentication Server can be made in two ways:

- **Simple**: Choose this method to connect to the AD via unsecured port. Simple connection uses port 389 for communication.
- **Over TLS**: Choose this method to enable secured connection to AD. Standard port used for such communication is 636. You can also change the port number.

Since AD does not have fields that correspond to some Celiveo specific properties, you can use the Advanced section to map Celiveo properties to AD field names that are not in use.

For example, when Card Authentication is enabled, Celiveo uses the card number to identify a user. Similarly, when PIN Authentication is enabled, Celiveo uses the PIN code to identify users. Celiveo stores both the card number and PIN code in a Celiveo specific property named Id Code. However, AD does not have a field named Id Code. So, you must store the Id Code in an unused AD field that already exists on the Authentication Server. In the Advanced section, you can map Id Code to the relevant unused AD field.



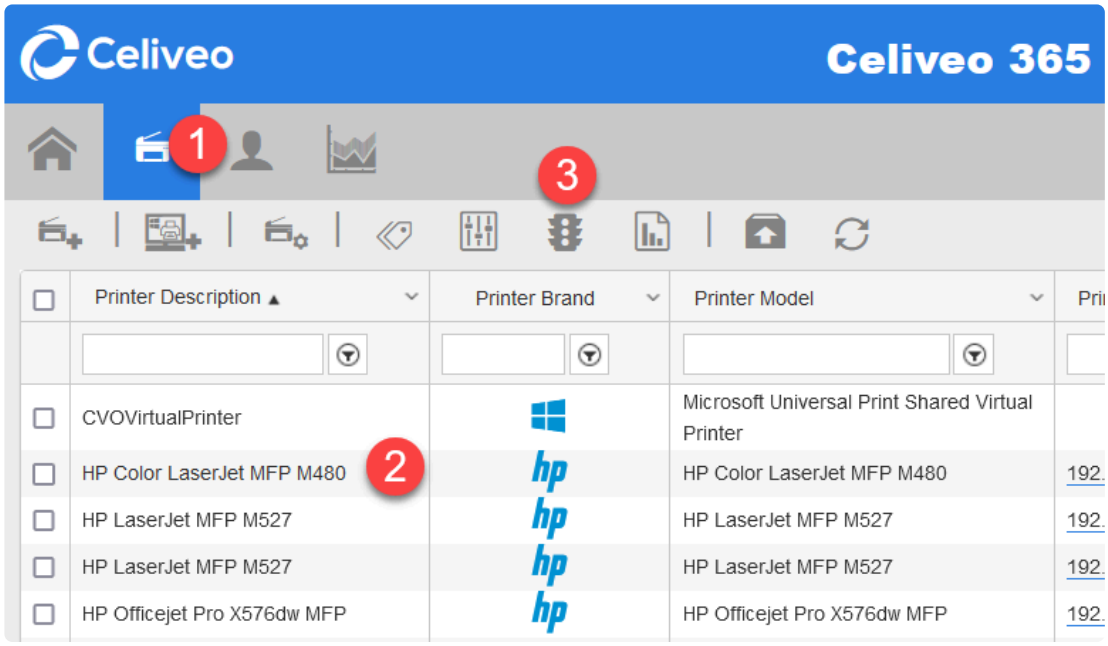
Setting	Description
Id Code Field Name	Default value is [postOfficeBox]. Or, select the Active Directory field which stores the user ID in the Active Directory or User Directory.

Department Field Name	Default value is [department]. Or, select the Active Directory field which stores the user department information.
Full Name Field Name	Default value is [displayName]. Or, select the Active Directory field which stores the user full name information.
Enrollment Id Field Name	Default value is [sAMAccountName]. This field is searched in the Active Directory to match the user login name and get their information during enrollment.
Dual Factor Field Name	Default value is [description]. Or, select the Active Directory field which stores the Dual Factor password.
Tracking Login Field Name	Default value is [sAMAccountName]. Or, select the Active Directory field which stores the user tracking login activity.
Login Field Name	Default value is [sAMAccountName]. Or select the Active Directory field which stores the user login information.
Email Field Name	Default value is [mail]. Or, select the Active Directory field which stores the user email information.
Home Directory Field Name	Default value is [homeDirectory]. Or, select the Active Directory field which stores the user information.
Domain Field Name	Default value is [domain]. Or, select the Active Directory field which stores the user domain.
Last Activity Field Name	Default value is lowercase of letter ‘L’. The time of the most recent authentication by the user. The feature is critical for auto-unenrollment, as the exact time is calculated before the user is automatically un-enrolled. The data of Last Activity Time is stored in the file if the user is enrolled locally. NOTE: Make sure that this field is documented and that it has read/write rights for the indicated AD service account.

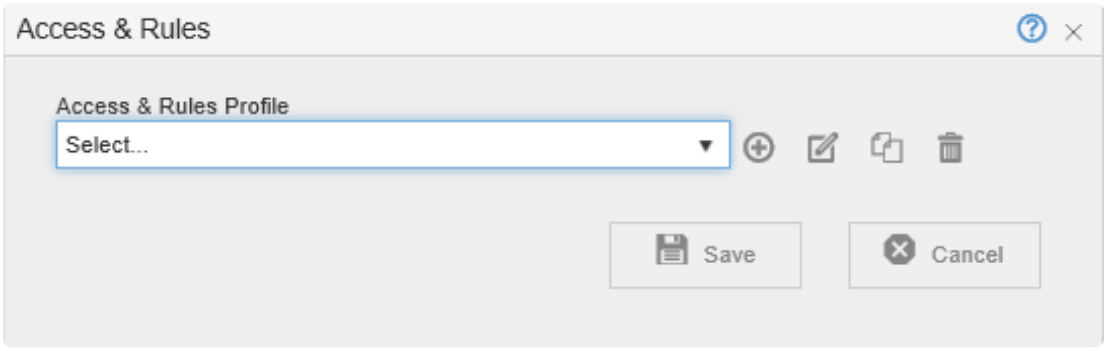
How to…

Create a New Authentication Source Profile

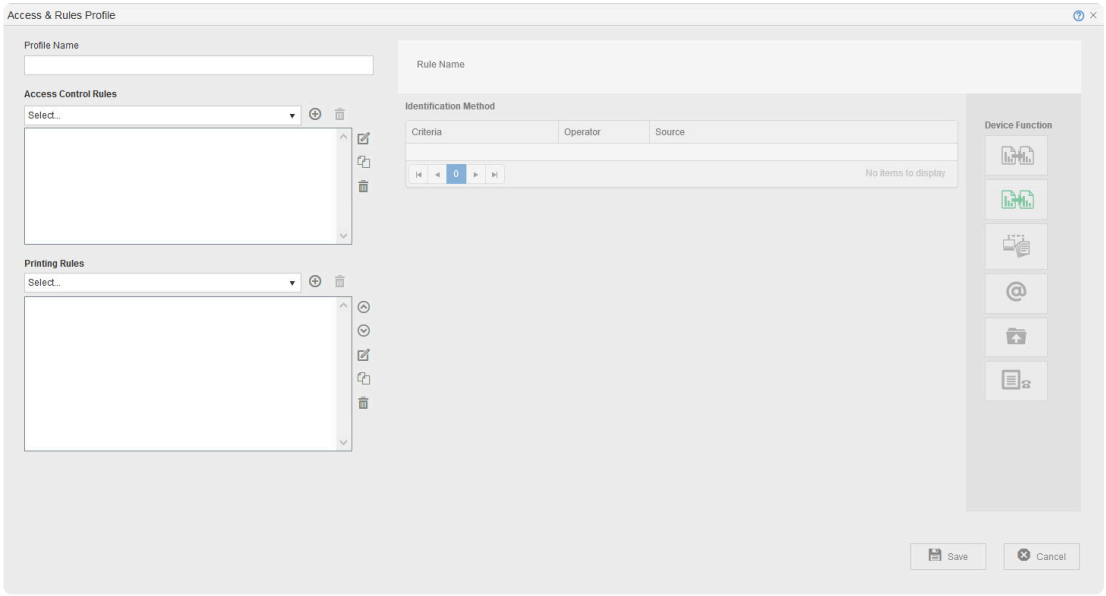
New Authentication Profiles are created while binding Access Control Rules to printers.



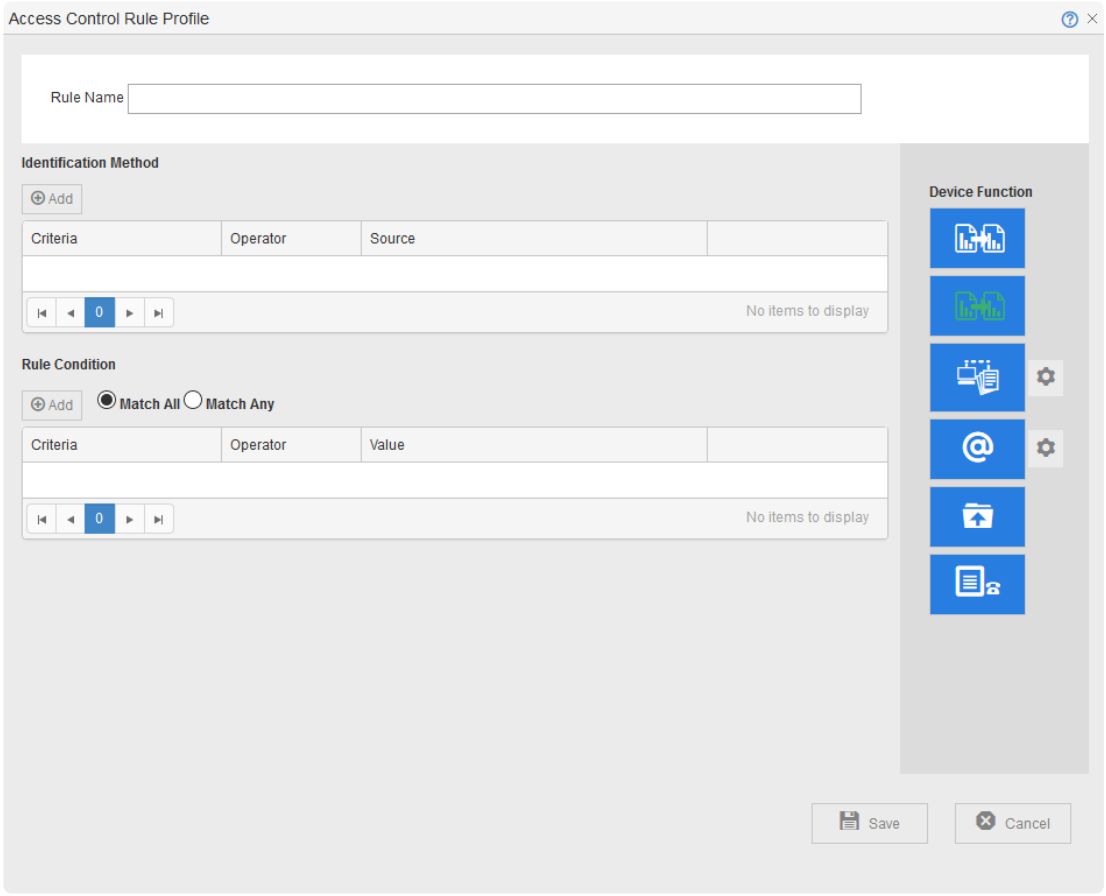
1. On the Celiveo Web Admin, at the main menu, click . The Printer List displays.
2. Select the Printer you want to add the new Access & Rules Profile to.
3. On the printer menu, click . Access and Rules is displayed.



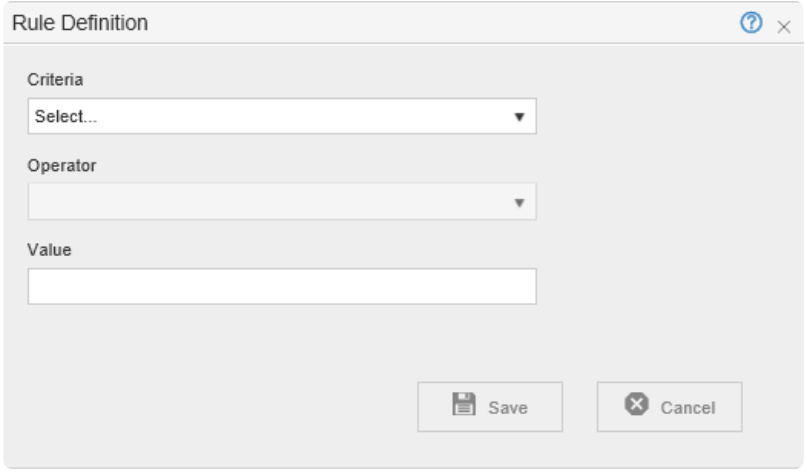
4. Select an Access & Rules Profile from the **[Access & Rules Profile]** drop down and click . The Access & Rules Profile displays.



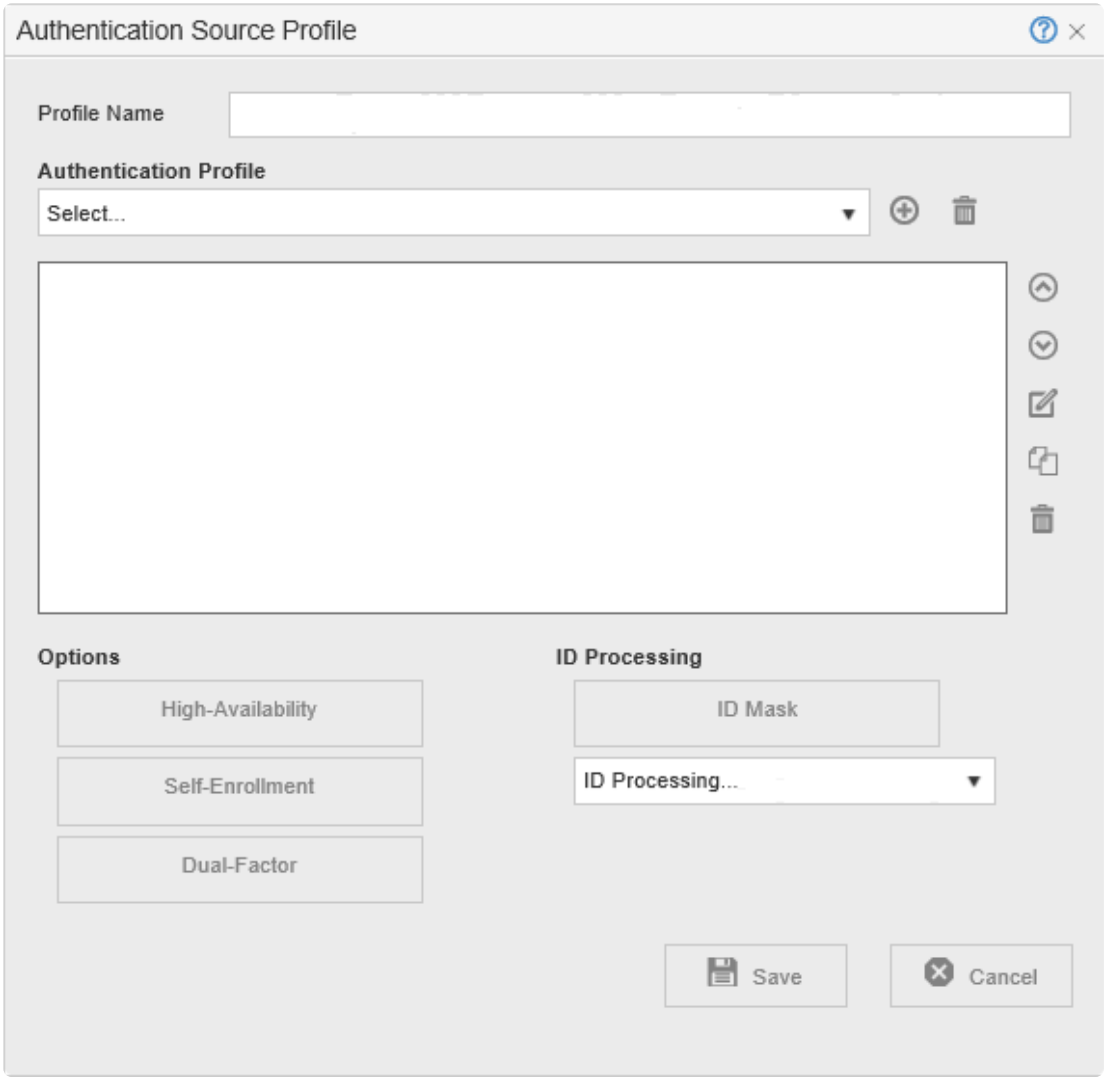
5. In the **[Profile Name]** box, specify a unique name for the Access & Rules Profile.
6. Click adjacent to the **[Access Control Rules]** drop-down. A new rule displays.



7. At **[Rule Name]** specify a name for the rule.
8. In the Access Control Rule Profile, In the **[Identification Method]** section, click ⊕. The Rule Definition is displayed.
9. In the **[Criteria]** drop-down, select **[Card Number]** or **[PIN Code]** for PIN Authentication.



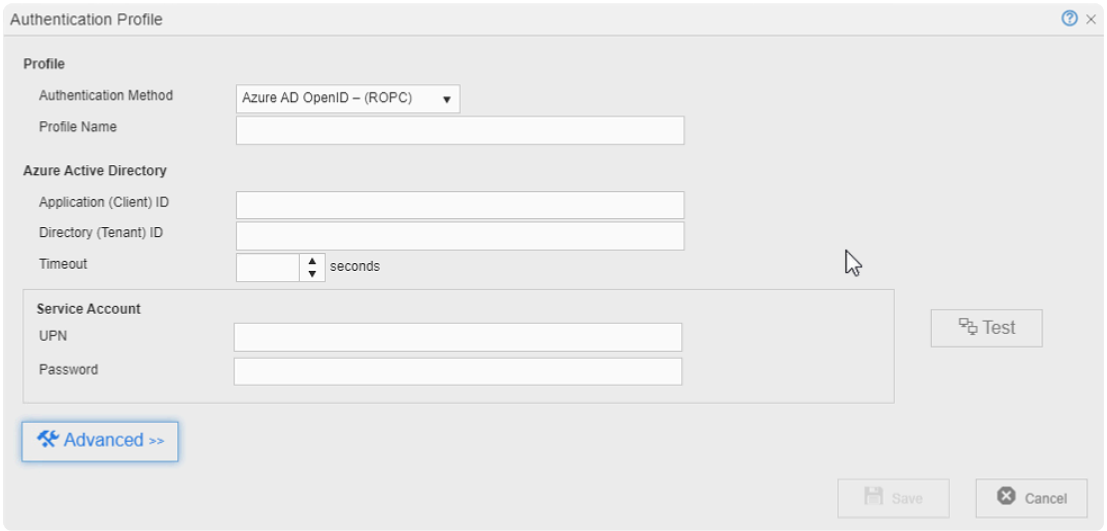
10. Click ⊕, which is located next to the **[Source]** drop-down. A new Authentication Source Profile displays.



11. At **[Profile Name]**, specify a name for the Authentication Source Profile.

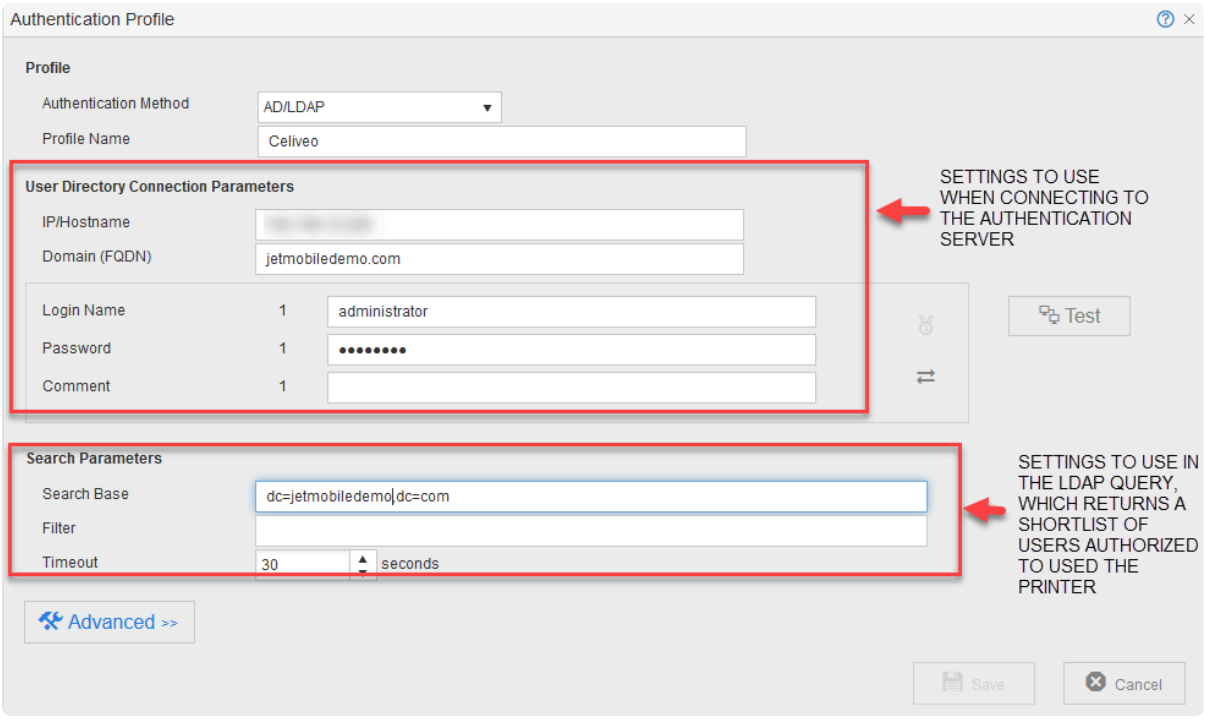
Create and Add an Authentication Profile to an Authentication Source Profile

1. Click ⊕, which is located next to the [Authentication Profile] drop-down. A new Authentication Source Profile displays.



2. To specify authentication against your company authentication server:

a. Ensure that the Authentication Method is set to AD/LDAP.
b. Specify the parameters to query the authentication server.



Configure advanced settings

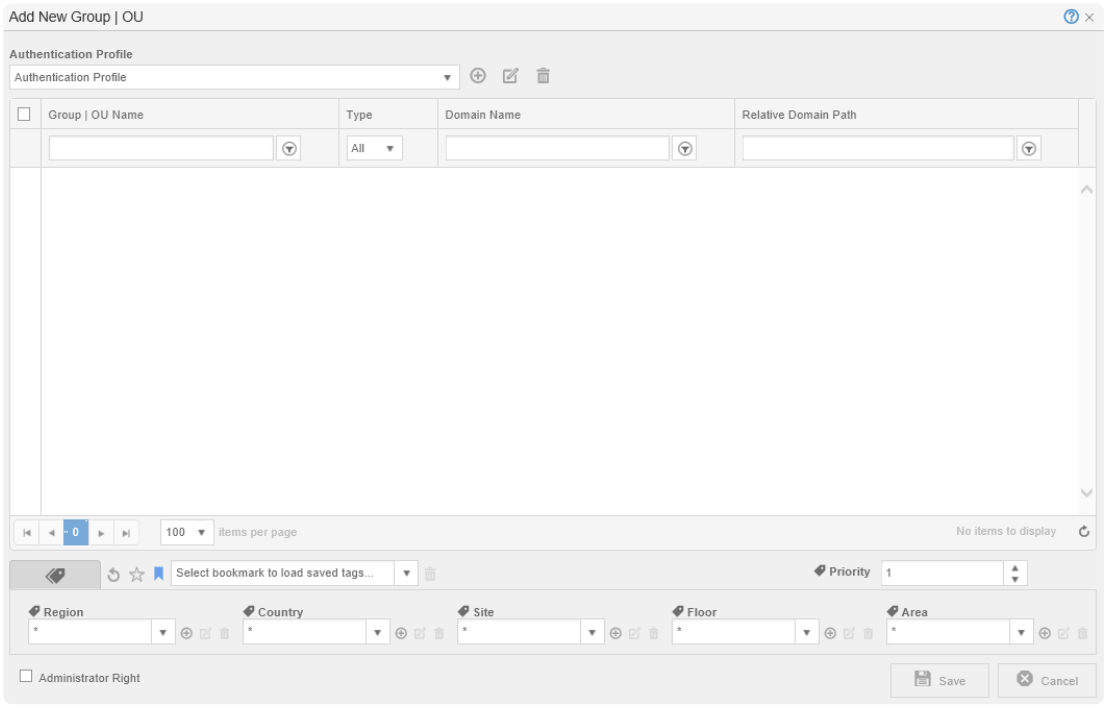
1. Click on **[Advanced]** to access the advance configuration.
2. At **[Authentication]**, select either **[Simple]** or **[Over TLS]**.
3. At **[Host Port]**, depending on the authentication method selected, the port number selected is:
   - 389 for **[Simple]** and
   - 636 for **[Over TLS]**.*

> **IMPORTANT**: *To avoid any dysfunction, especially with HP FutureSmart Printers, make sure your LDAP is properly configured to be used over TLS. To get the step-by-step instructions, please see the Microsoft Blog.

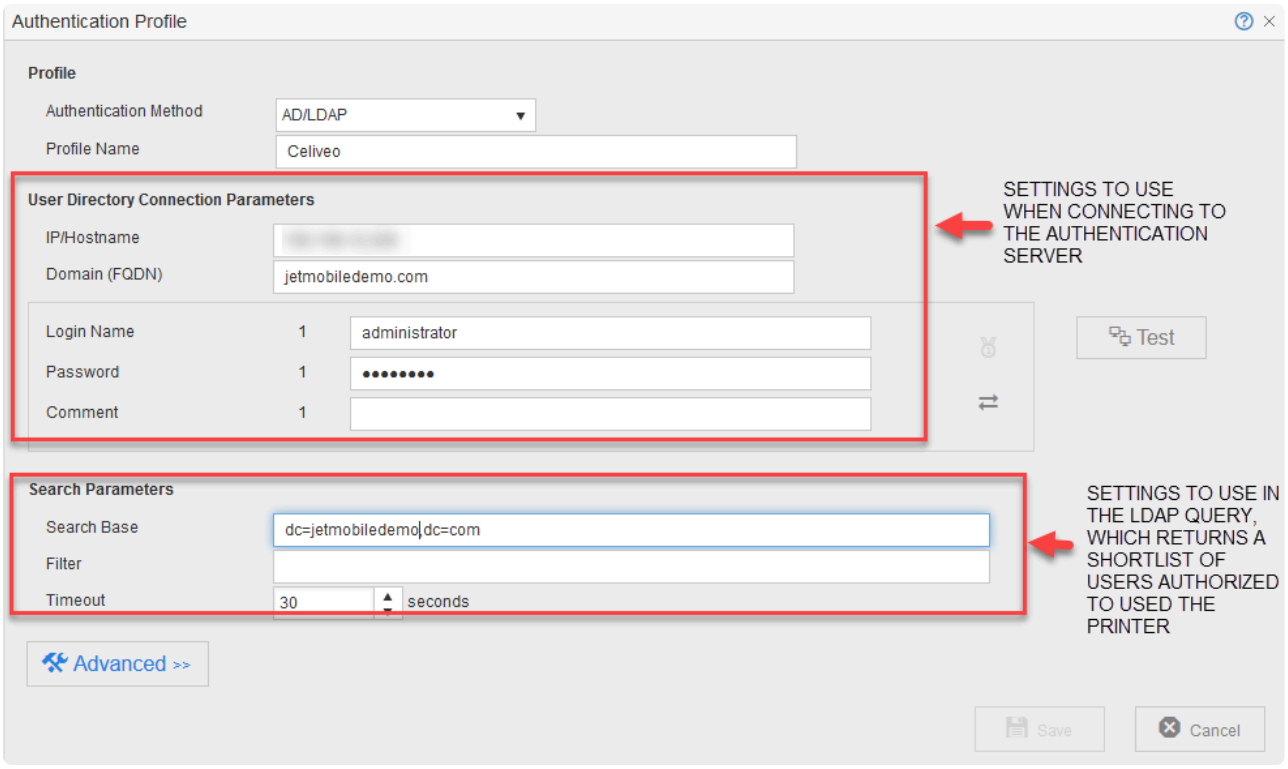
4. Make the required changes to the **[Active Directory Field Names]**.
5. Click **[Save]**. You are returned to the Authentication Source Profile.
6. From the **[Authentication Profile Name]** drop-down, select the Authentication Profile you just created.
7. Click **[Save]**.

Create a New Authentication Profile (Alternate Method)

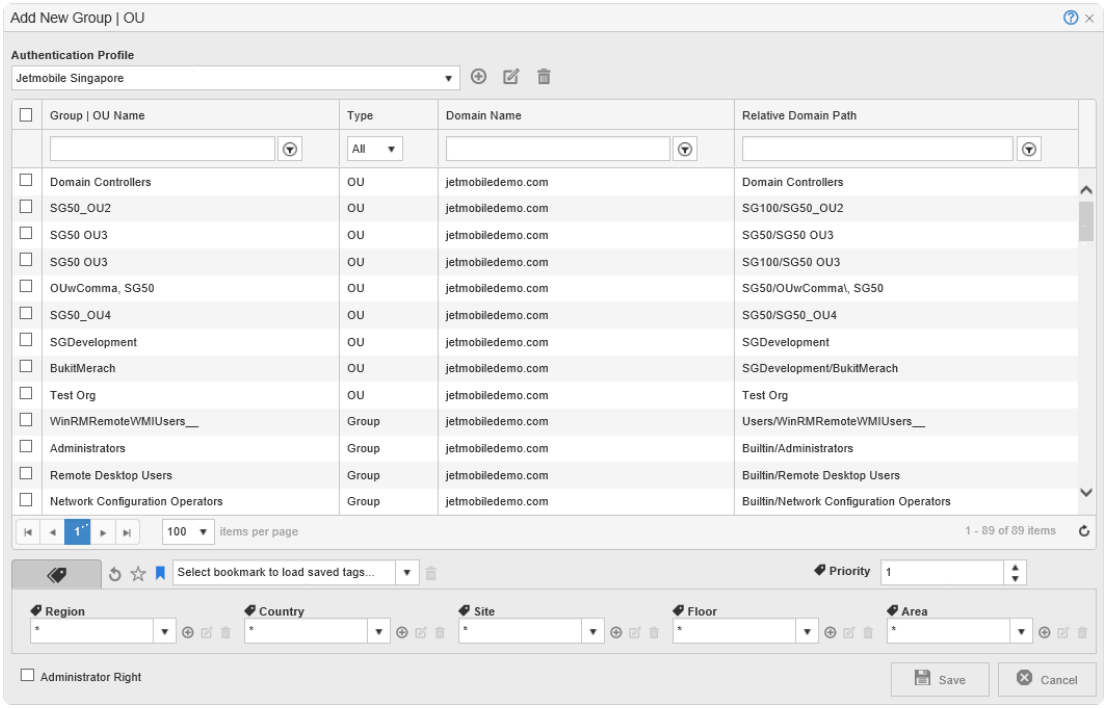
1. From the Celiveo Web Admin Main Menu, click . The User list displays.
2. Click . The User Groups list displays.
3. Click . The Add New Group|OU displays.



4. Click ⊕, which is located next to the **[Authentication Profile]** drop-down. The Authentication Profile dialog displays.
5. At Authentication Profile Name, specify a name to identify the Authentication Profile.
6. Specify the parameters to query the authentication server.



7. Click **[Save]**. The Groups and Organizational units retrieved by the LDAP query you specified is listed in the Add New Group|OU dialog.



8. Inspect the list and verify if the information that the Authentication Profile retrieved is correct.
9. Click **[Cancel]**.

> **Note**: The objective of this exercise was to create the authentication profile and not create a group. Because the authentication profile is already created and verified, we cancel without saving the group.

Last modified: 29 September 2022

11.3. High Availability

Contents

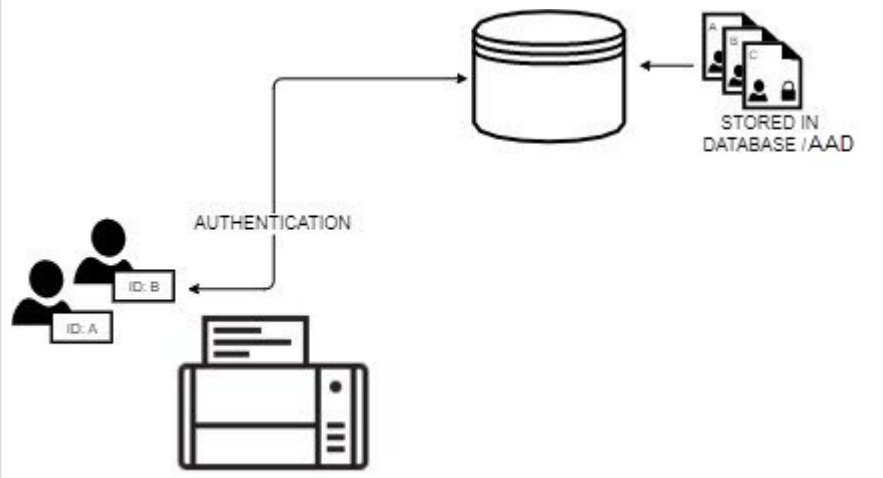
1. About High Availability
   a. What is high availability?
   b. Full Cache Vs Dynamic Cache
   c. Cache First Vs Cache Last
   d. Tracking and High Availability
   e. Limitations

2. How to…
   a. Enable High Availability
   b. Configure High Availability Options

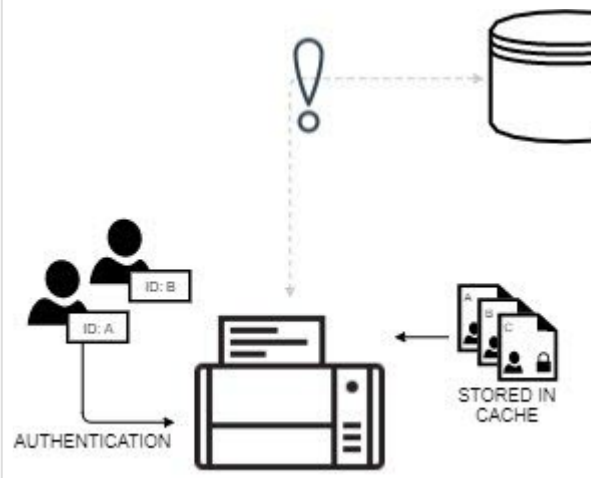
About High Availability

What is High Availability?

High Availability is an optional feature that makes badge authentication and PIN authentication possible, even when the connection with the back end is lost. This feature is implemented via a mechanism that authenticates user details against a cache at the printer, rather than the back end.



Normal authentication



Authentication when link to back

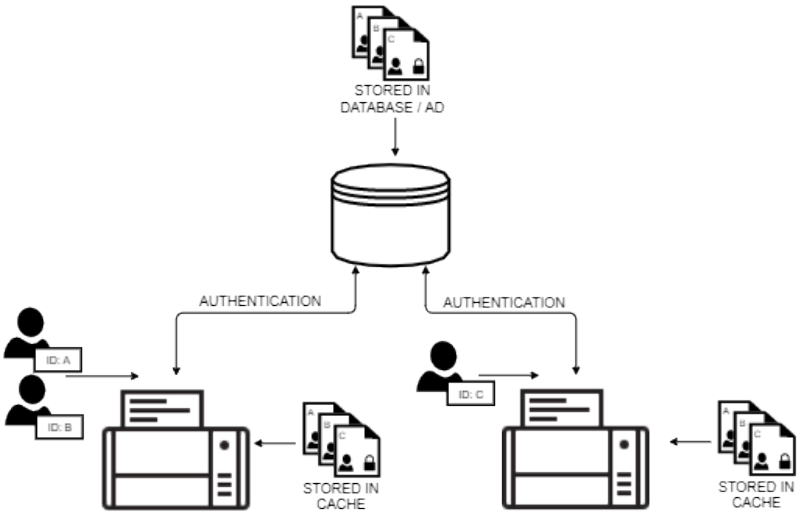
High Availability is offered with any Vertical Connector purchased on top of Celiveo Enterprise.

Full Cache Vs Dynamic Cache

High Availability supports two modes of caching.

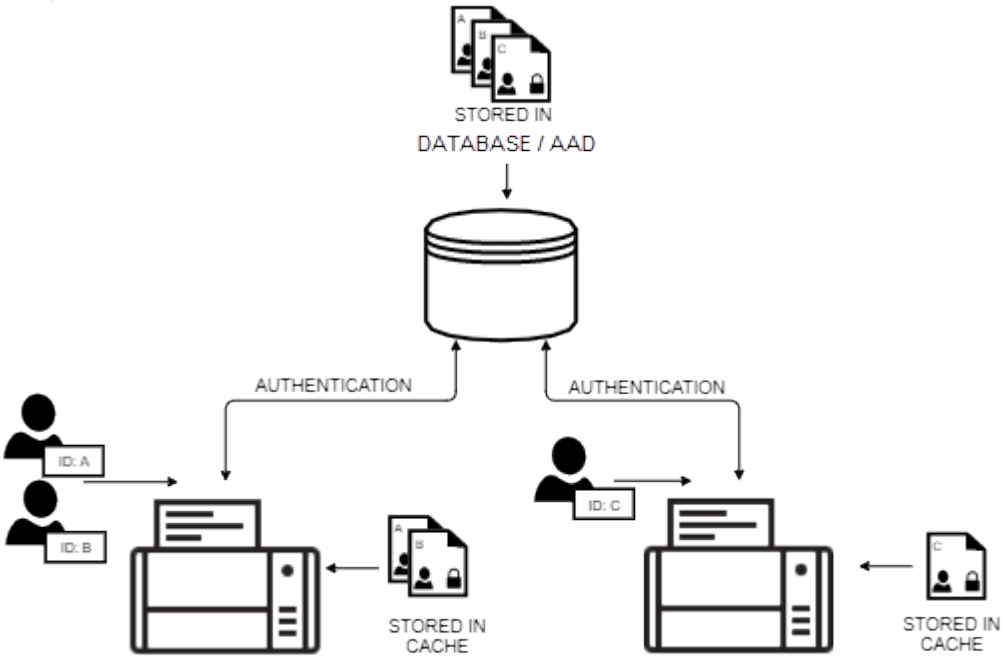
1. Full Cache
   In this mode, the cache downloads the details of all enrolled users from the database/Active Directory (AD). In order to keep the data current, the cache is synced periodically with the back

end. This synchronization happens at every scheduled event on the printer. It is possible to fine tune the list of users that shall be downloaded inside a printer cache using the AD filter string. If different printers need different lists of users, the admin just needs to use different AD profiles for printers.



Full Cache stores details of all users in the cache

2. Dynamic Cache
   In this mode, the cache captures your details whenever you authenticate at the printer. The data is purged from the cache if you do not authenticate at the printer for a specified time.



Dynamic cache stores the details of those who authenticate at that printe r

Because Full Cache contains the details of all enrolled users, any user can authenticate at a printer when the back end is offline. However, keeping the cache in sync with the back end can generate significant network traffic, especially in an environment with a large number of users and printers.

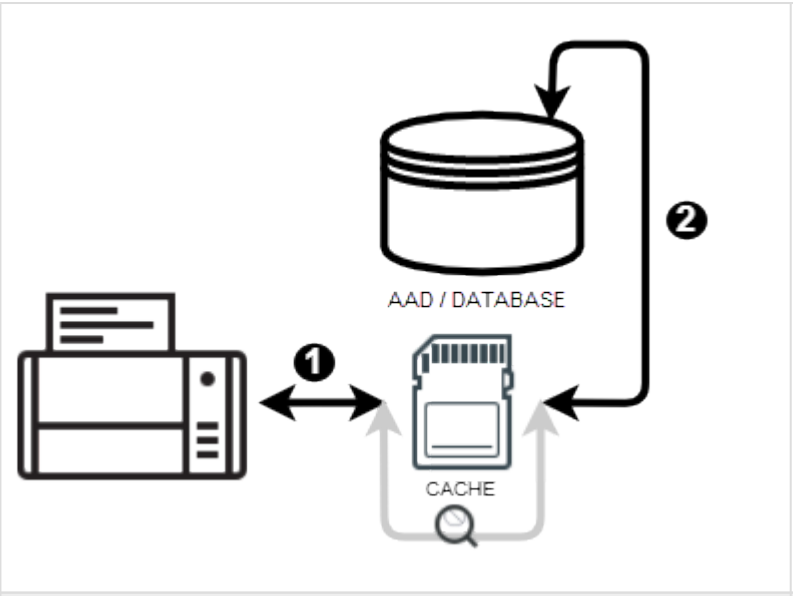
Because Dynamic Cache purges cache data when you do not authenticate at the printer for a while, only recent users of the printer can authenticate when the back end is offline. Typically, the printers that do not contain your details are the ones you are least likely to access. As such, Dynamic Cache allows for

successful authentication most of the time, while keeping network traffic down.

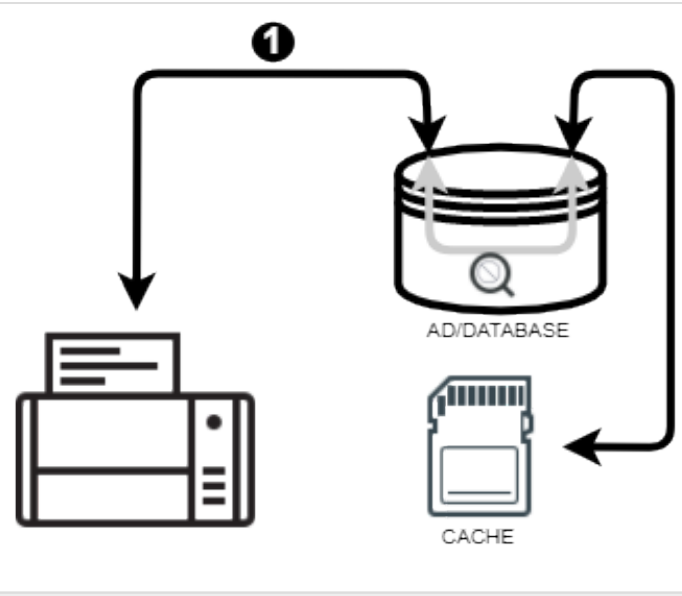
> Note: with Ricoh and Lexmark embedded agents, High Availability only supports Dynamic cache. Full cache is not supported on those two printer brands due to storage constraints.

Cache First Vs Cache Last

You can choose between two authentication methods; authenticate against the cache first or authenticate against the cache last.



Cache first



Cache last

When the Cache First method is enabled, the back end is queried only if your details are not found in the cache. When details are found on the cache, the authentication process becomes much faster, because queries across the network are circumvented, and hence, the impact of network latency is blunted. Consequently, the Cache First method is able to boost performance. The performance gains can be quite significant, especially on corporate networks with geographically distributed branches, where the quality of service (QoS) between branches is not optimal. On the downside, cached details are only as accurate as the most recent sync operation.

For example, If you re-assign the Badge ID of an old user who is currently not existing with the organization, to a new user, and the cached details have not been synced recently, there would be a mismatch as the user details would be already existing in the cache under the old user's name.

When the Cache Last method is enabled, user details are always authenticated against the back end. The cache is checked only if there is no response from the back end. Because details are always checked against the back end, this authentication method is the more secure of the two. In this mode, the cache acts purely as a failover mechanism.

Tracking and High Availability

Tracking data is cached at the printer even if High Availability is not enabled. When the connection with the back end is lost, tracking data is stored in the cache. Whenever the connection is restored, cached tracking data is written back to the back end.

Limitations

When the connection to the back end is lost, upon authentication, High Availability checks the cache for the sources of the most recent print jobs. It then queries the source for pending print jobs matching the user details it just authenticated. Upon finding the print job, it “pulls” the print job and prints it. If the computer you are using to send the print job has not used the printer recently, the High Availability cache of that printer will have no record of the computer. As such, it will not be able to “pull” the job from that computer. Accordingly, you may not be able to print a pull print job, if the computer you are on has not recently used that printer.

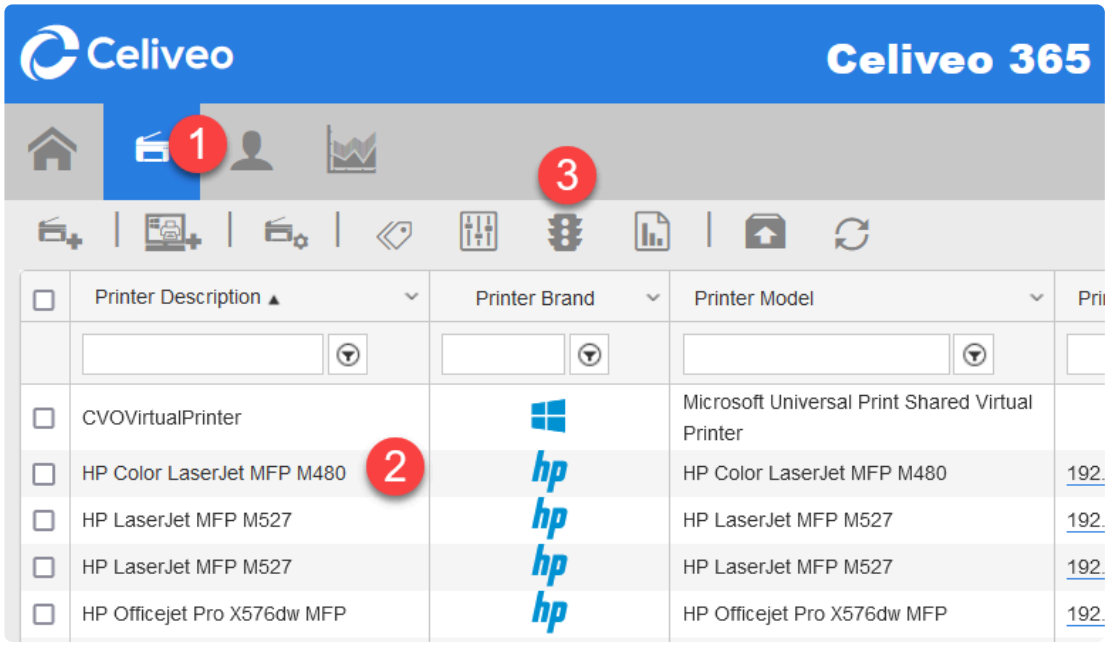
When Dynamic Cache is enabled, you must authenticate at least once to allow for the cache to capture your details. As such, when the back end is offline, you may not be able authenticate at a printer you have not used before.

If you upgrade the Celiveo Smart Appliance Version file name that ends with OSI.fw, the High Availability cache is purged. Thereafter the cache starts rebuilding from scratch, and requires a while to build the cache to effectively implement High Availability.

For security reasons, Smart Card Authentication support High Availability feature in Dynamic Cache mode with Read Cache Last method only. “Read Cache First” method selection, if configured, will be ignored and no cache will be applied.

How to…

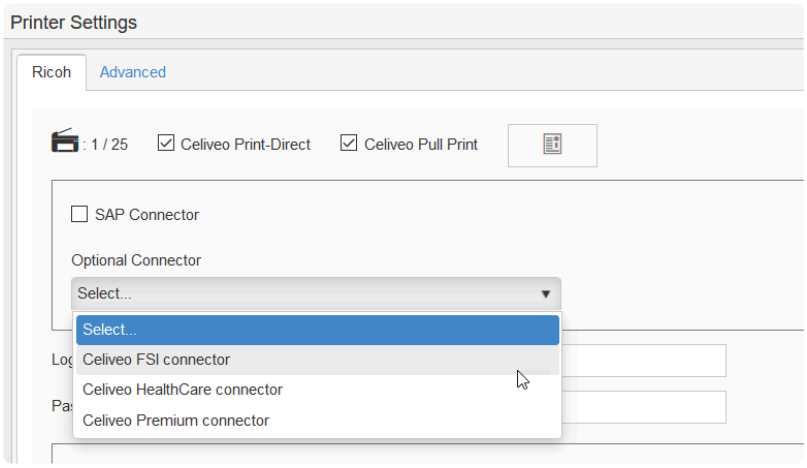
Enable High Availability:



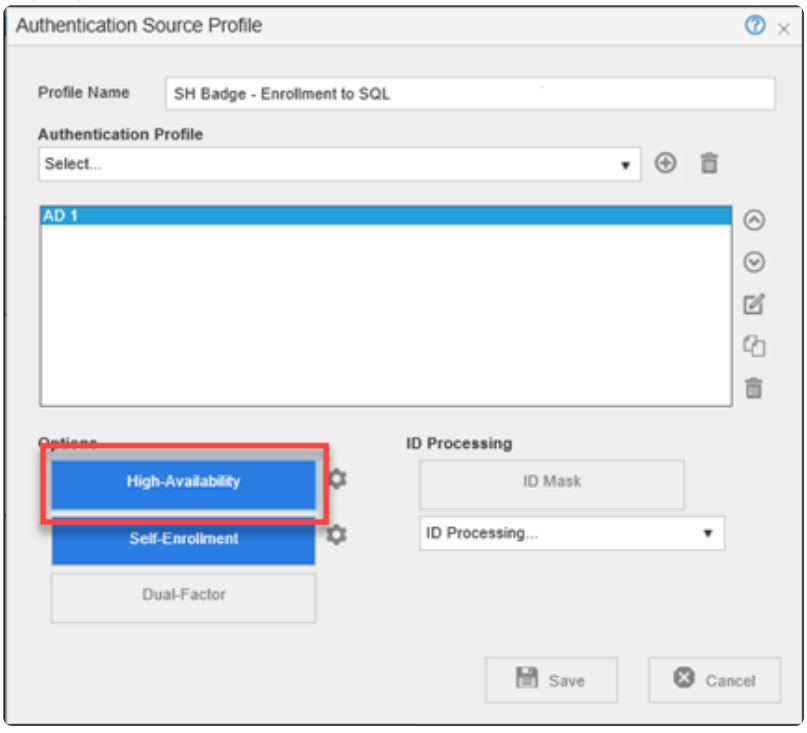
1. On the Celiveo Web Admin, at the main menu, click . The Printer List displays.
2. Select the printer you want to enable High Availability for.

Note: The printer must have has Badge Authentication or PIN Authentication enabled.

3. High availability is supplied by optional connectors for Celiveo Enteprise Edition. In the printer settings, select the desired optional connector.



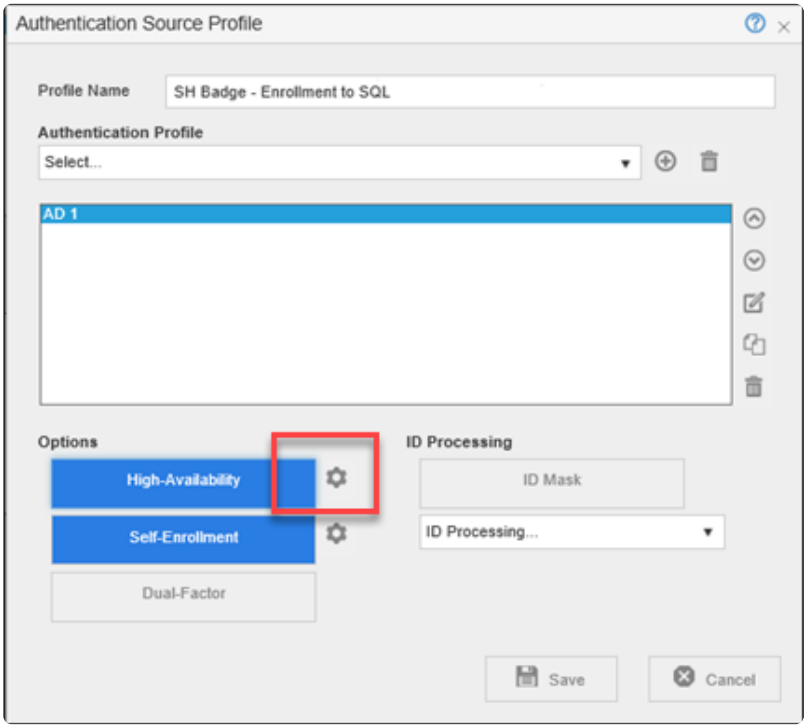
4. On the printer menu, click . Access and Rules is displayed.
5. Click adjacent to Access & Rules Profile. The selected Access & Rules Profile is displayed.
6. Click adjacent Access Control Rules list. The Access Control Rule Profile is displayed.
7. In the row corresponding to the Badge Number or PIN Code, click .
8. Click adjacent to the Source box.
9. To enable, High Availability, click **High-Availability**. When the feature is enabled, the button is highlighted in blue.



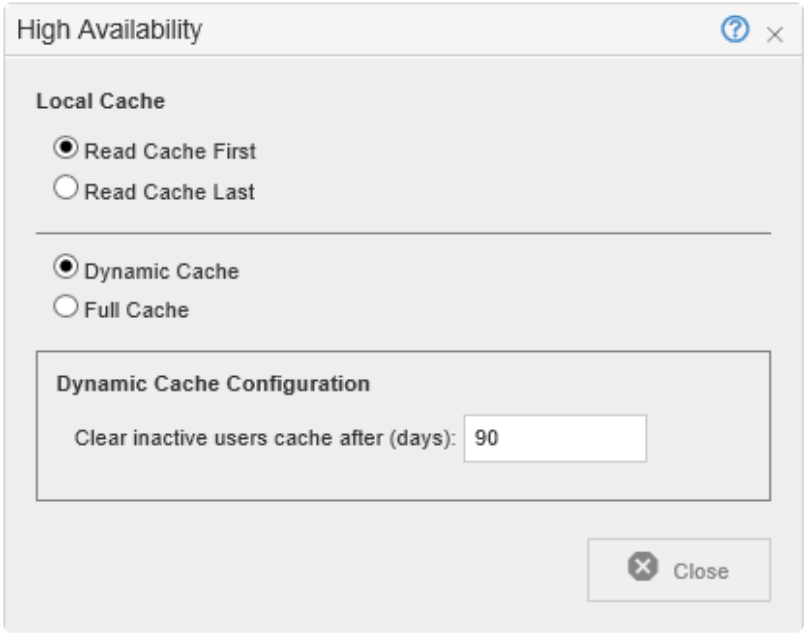
Configure High Availability Options:

1. Open the Authentication Profile containing the High Availability options.
2. Click ⚙ adjacent to the High-Availability button.

Note: This button is visible only if High Availability is enabled.



3. To ensure that details are checked against the cache before the back end is queried, select **[Read Cache First]** (authenticates faster).
   To ensure that details are checked against the back end before the cache is queried, select [Read Cache Last] (more secure).



4. To provide High Availability only for recent users of the printer, but with low network traffic:
   a. Select **[Dynamic Cache]**.
   b. In **[Cache Inactivity Timeout]**, specify how many days to retain user details in the cache.

5. To provide High Availability for all users:
    a. Select **Full Cache**.
    b. Under Full Cache Configuration, specify how often, the cache is synced with the back end. You can choose between monthly, weekly, daily, or a specific date.
    c. Specify a time interval within which sync is performed.

Note: As many printers can attempt to sync at the same time and cause high network traffic, you specify a time interval, rather than a specific time.

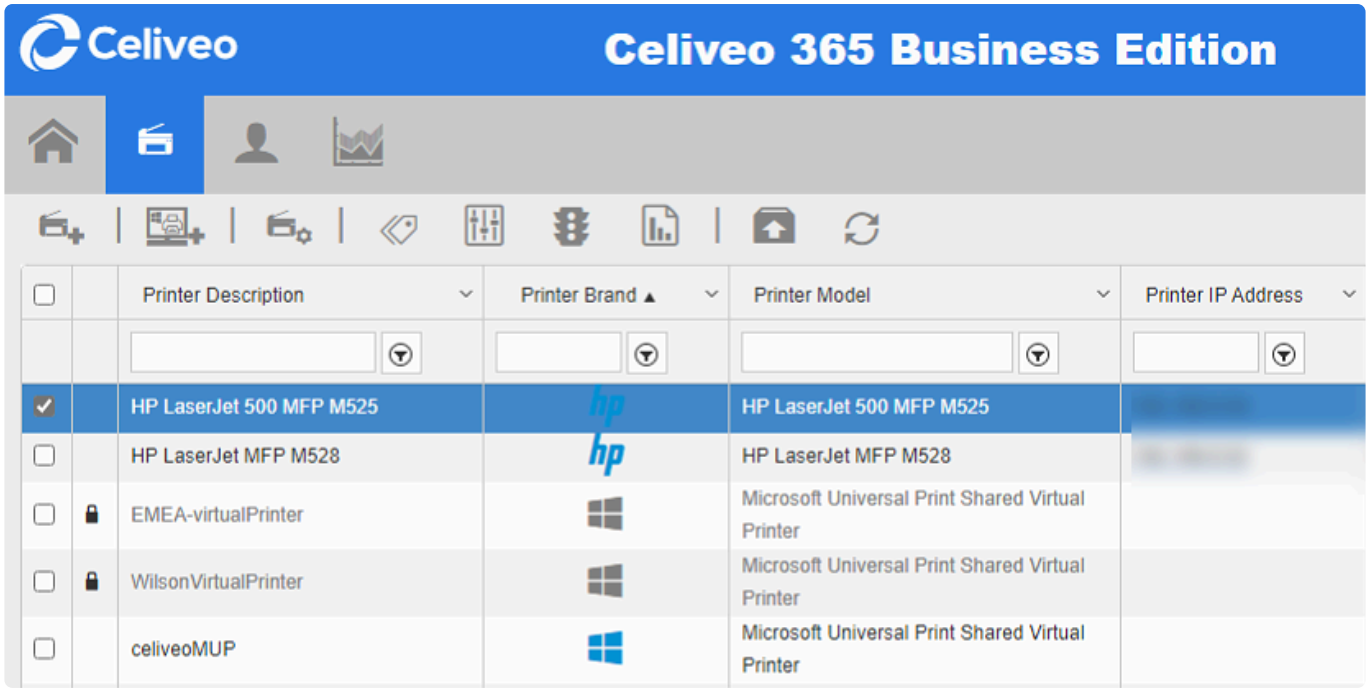
Last modified: 10 October 2022

11.4. Enable ID Code Authentication for Printers

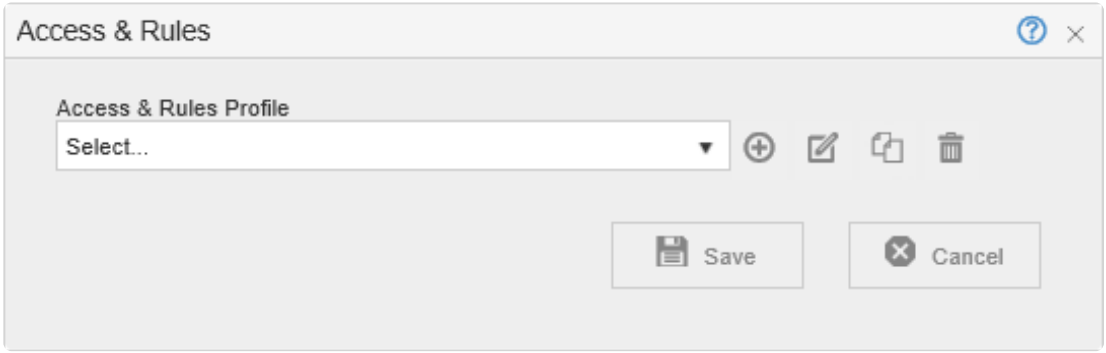
B E

You enable ID Code authentication by creating an Access Control Rule and assigning the rule to a printer. You however cannot assign an Access Control Rule directly to a printer. Instead, you create an Access & Rules Profile for a printer and add the Access Control Rule to the Access & Rules Profile.

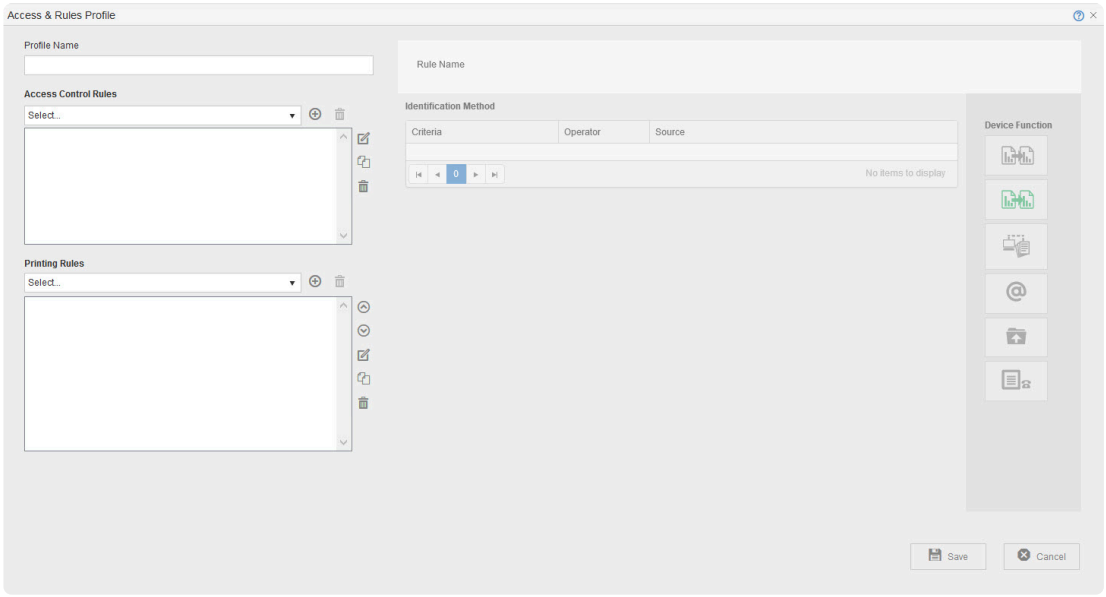
1. Add a New Access & Rules Profile to a Printer



1. Select the printer to add the Access and Rules Profile to.
2. Click . The Access & Rules dialog is displayed.



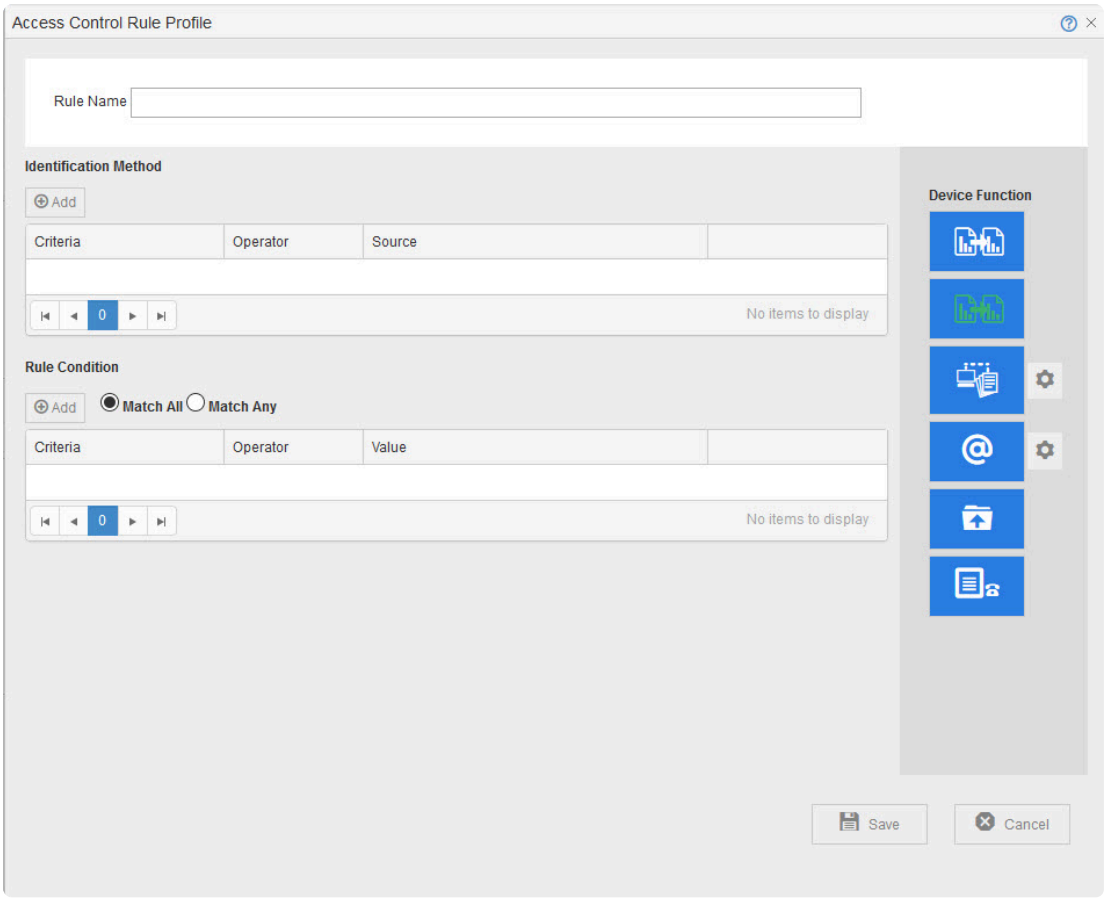
3. Click . The Access and Rules profile is displayed.



4. At **[Profile Name]**, specify a unique name for the Access & Rules Profile.

2. Add a New Access Control Rule to the Access and Rules Profile

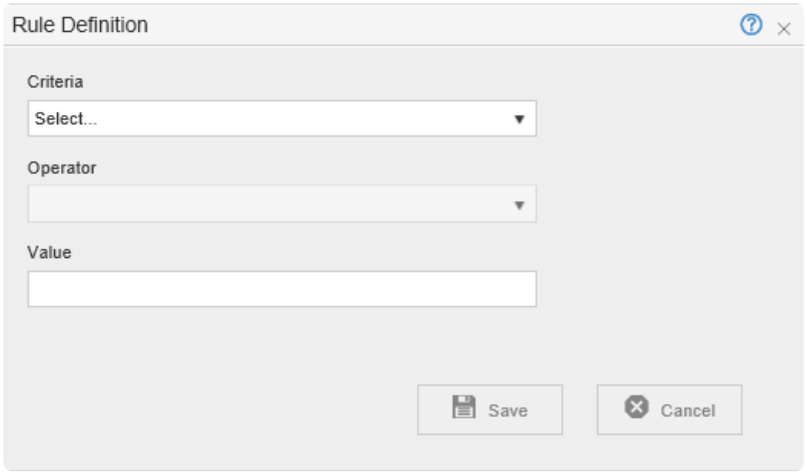
1. Click ⊕ , located in the same row as the **[Access Control Rules]** drop-down. The Access & Rules Profile displays



2. At **[Rule Name]**, specify a unique name for the Access Control Rule.

3. Add ID Code Authentication as the Identification Method

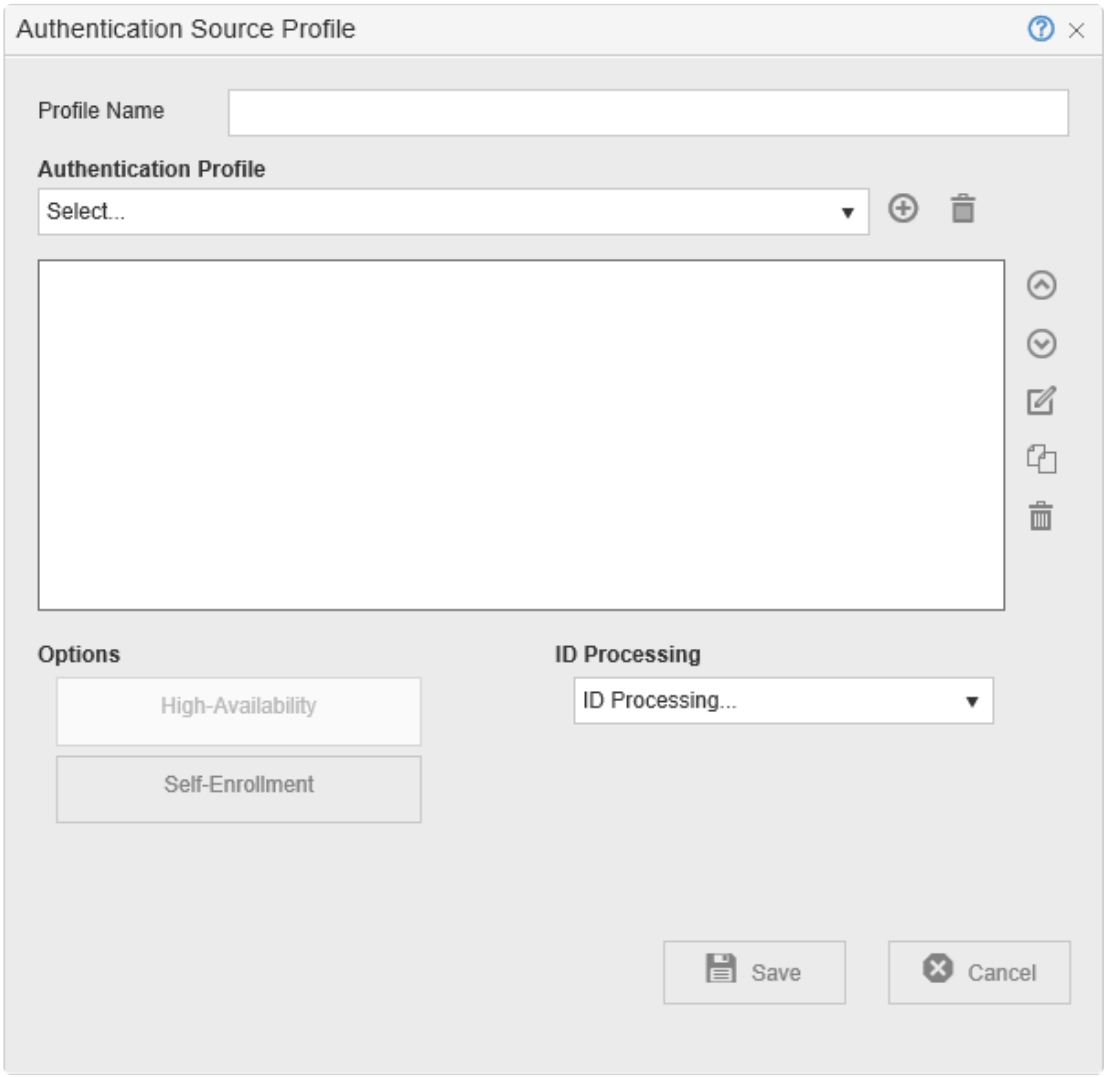
1. Click **[Add]**, located below **[Identification Method]**. The Rule Definition displays.



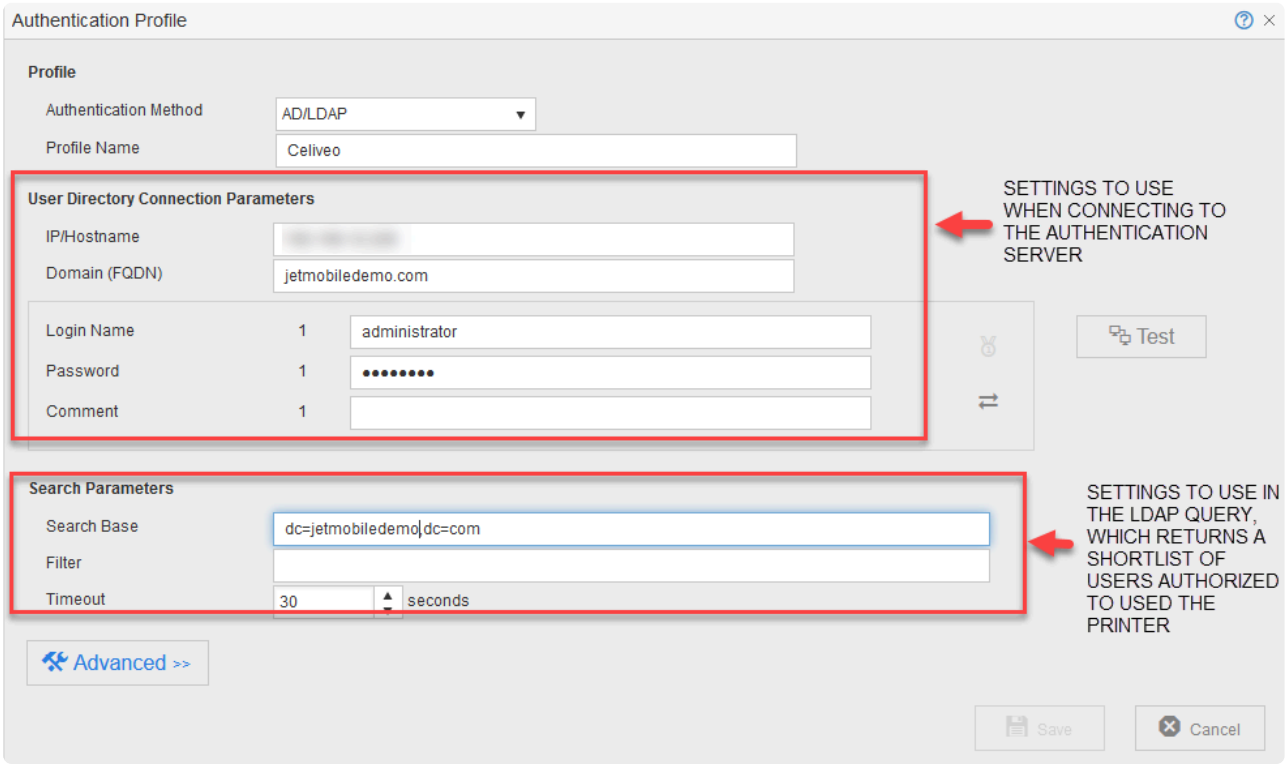
2. From the **[Criteria]** drop-down, select **[IDCode]**.
3. From the **[Operator]** drop-down, select **[Is In]**.

4. Build the Authentication Profile to Validate the PIN

1. Click ⊕, located next to the **[Source]** drop-down. The Authentication Profile displays.



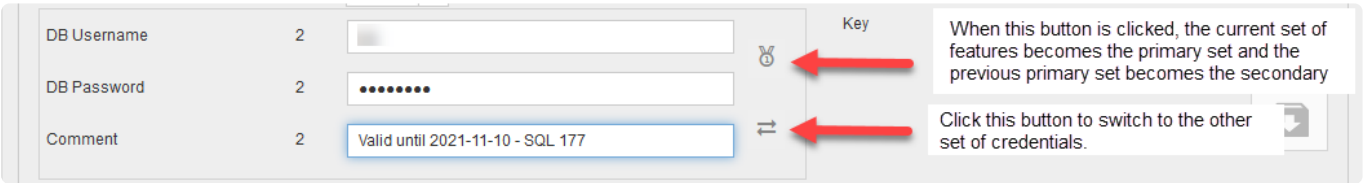
2. In the **[Profile Name]** box, specify a unique name to identify the profile.
3. Click ⊕, located in the same row as the **[Authentication Profile]** drop-down. The Authentication Profile is displayed.
4. Specify the AD/LDAP query (similar to that of the screen capture shown below) that returns the list of users who are authorized to use the printer.



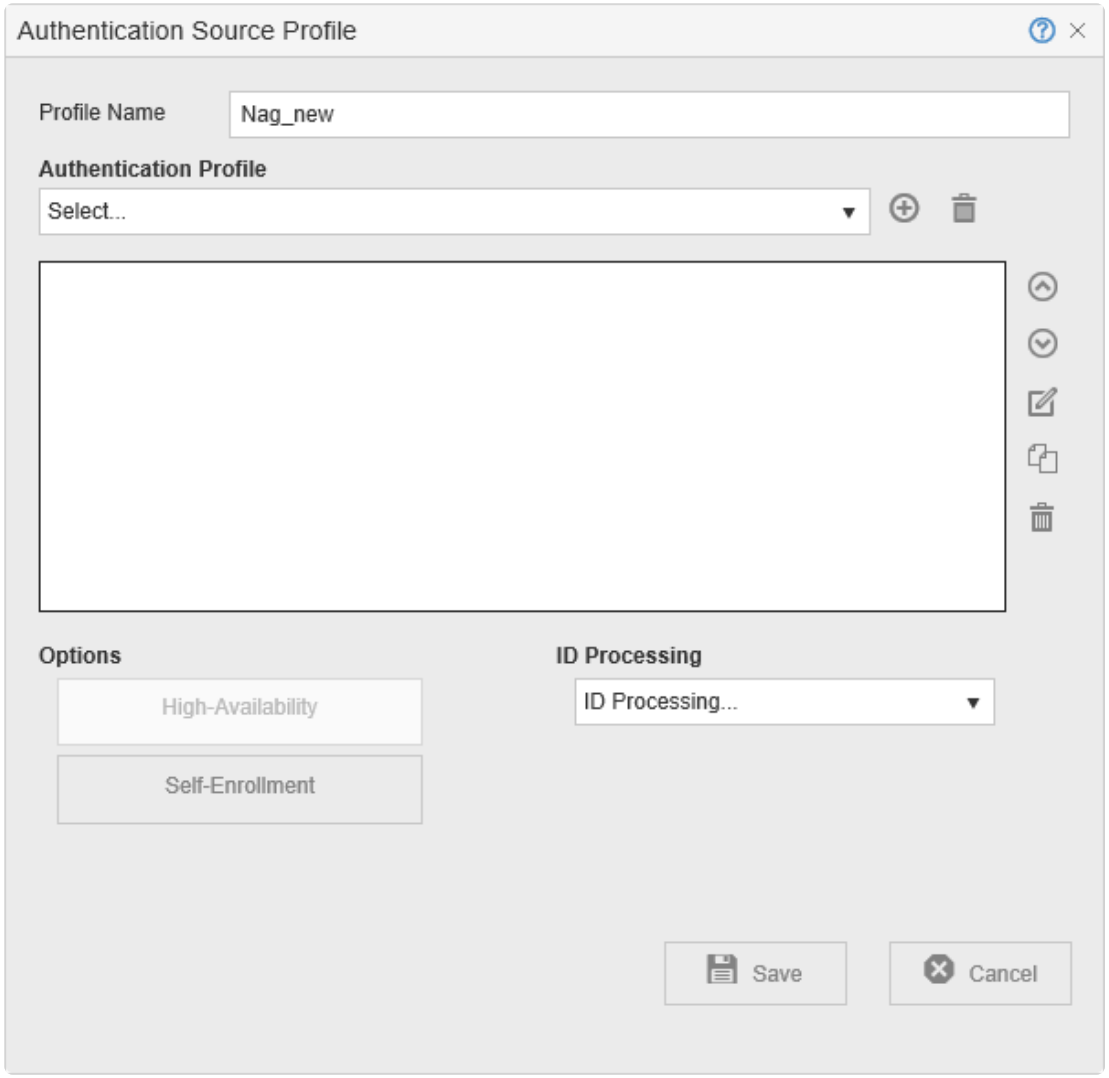
5. Click **[Test]**.
   If login to the Authentication Server is successful, a message is displayed below the [Test] button.
6. Click **[Save]**. You are returned to the Authentication Source Profile.

Dual Service Account System

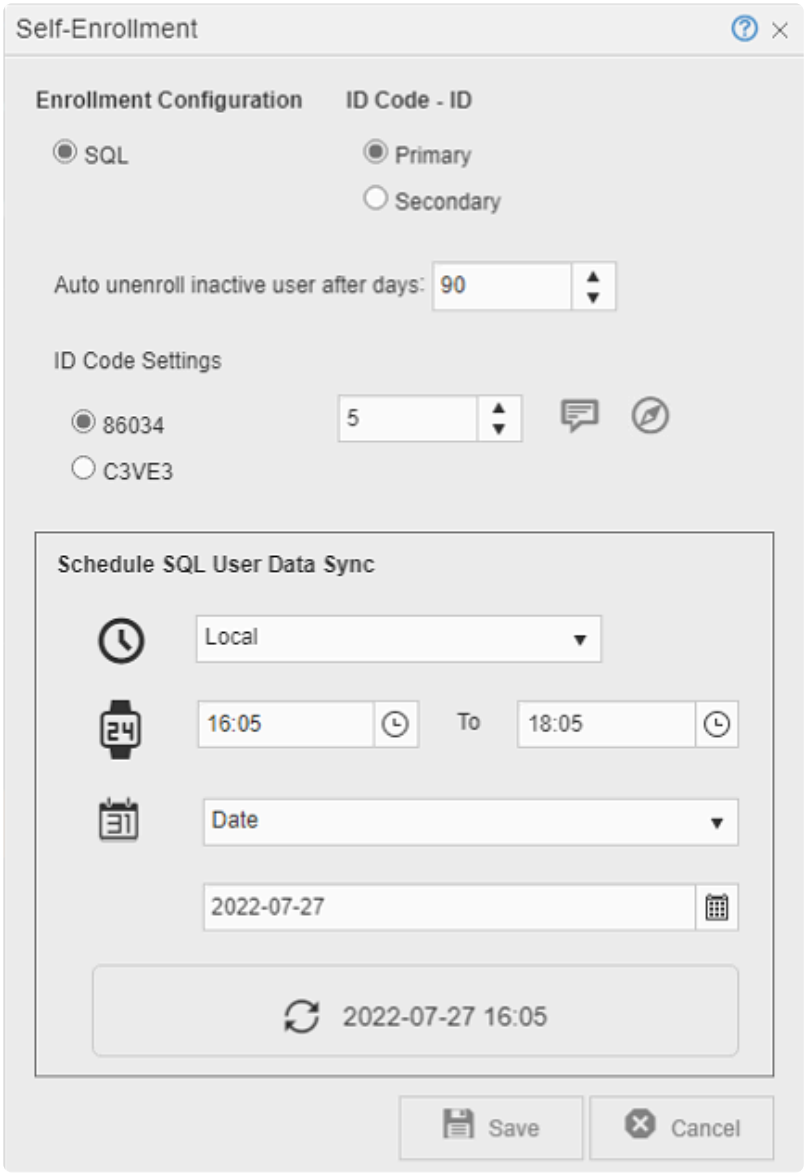
To avoid any connection error after refreshing/changing the login/password on service accounts used by Celiveo, the administrator can define a secondary set of credentials so that if the default (primary) set is declined by the solution, then the secondary set takes over and prevents the access from being denied.



5. Specify How to Enable Self Enrollment



1. Click **[Self-Enrollment]**.
2. Click ⚙ next to the [Self Enrollment].



3. At **[Auto unenroll inactive user after days]**, enter the number of days.
   An enrolled user who has not used the Celiveo system after the specified number of days is automatically removed.

> **Note**: In order to function, this features requires that Time and Date are properly configured on the printer.

4. To enable authentication with a Smartphone using BLE (Bluetooth Low Energy), tick the **Use Celiveo Mobile ID** checkbox.
5. At **[ID Code Settings]** specify if you want a numeric (made of digits) or alphanumeric (made of digits and letters) PIN. You can also choose the length of your code.
   a. Numeric ID codes shall not:
      - Start with 0
      - Be made of consecutive digits, for example, 123456 or 2345
      - Be made of repeated digits, for example, 11111
      - Have the same digits except one, for example, 51111
      - Be made of repeated patterns, for example, 123123

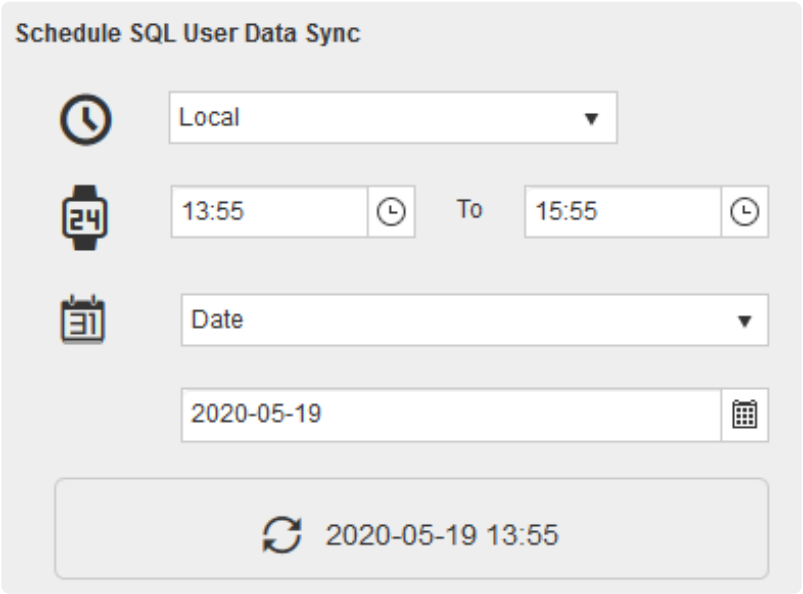
b. Alphanumeric ID codes shall:
   - Be uppercased, for example, 45ER9
   - Always be uppercased when entered on MFP screen, for example, at5p => AT5P
   - Have a random mix of digits and letters
   - Supported letters can be A to Z except for o and i that can be mixed up with 0 and 1.
   - Supported digits can be 1 to 9, no zero

c. Alphanumeric ID codes shall not:
   - Be lowercased
   - Be made of the same characters, for example, AAAA
   - Be made of repeated patterns, for example, ABAB or TOTO

If you have more than 1000 users, do not use less than 5 digits for the PIN.

6. At **[Schedule Time Zone]**, select one option:

Local	Apply the time settings of the local machine.
UTC	Apply the preferred Coordinated Universal Time (UTC) time zone.



7. Set the range of time for the data sync to occur.
   To avoid a sudden increase in network traffic, the update is scheduled to happen anytime during the specified period.
8. Set the frequency of the data sync.

Date	The data sync occurs on a specific date. Set the date to start the data sync.
Daily	The data sync occurs every day during the specified time frame.
Weekly	The data sync occurs every week on a specific day of the week. From the drop menu, select the day of the week.
Monthly	The data sync occurs every week on a specific day of the month. From the drop menu, select the day of the month.

Note: PIN Settings is a global configuration. The PIN length and enrollment configuration (SQL or AD/LDAP) once defined, cannot vary across Access Profiles.

9. Click . The Notification Message displays.
10. Specify the text for the notification and click **[Close]**. This template is used to inform users of their ID code when they enroll.

11. Click . You are taken to the ID Code generating portal.
    a. Log in using your Windows credentials.
    b. Note down the URL of the portal. You need to send the link to users to enable them to generate their own ID Codes and enroll themselves.
12. Close all dialogs by clicking **[Save]** to save all settings.

If you are using Internet Explorer, please refer to this article to enable the **Generate** button on the generating Portal.

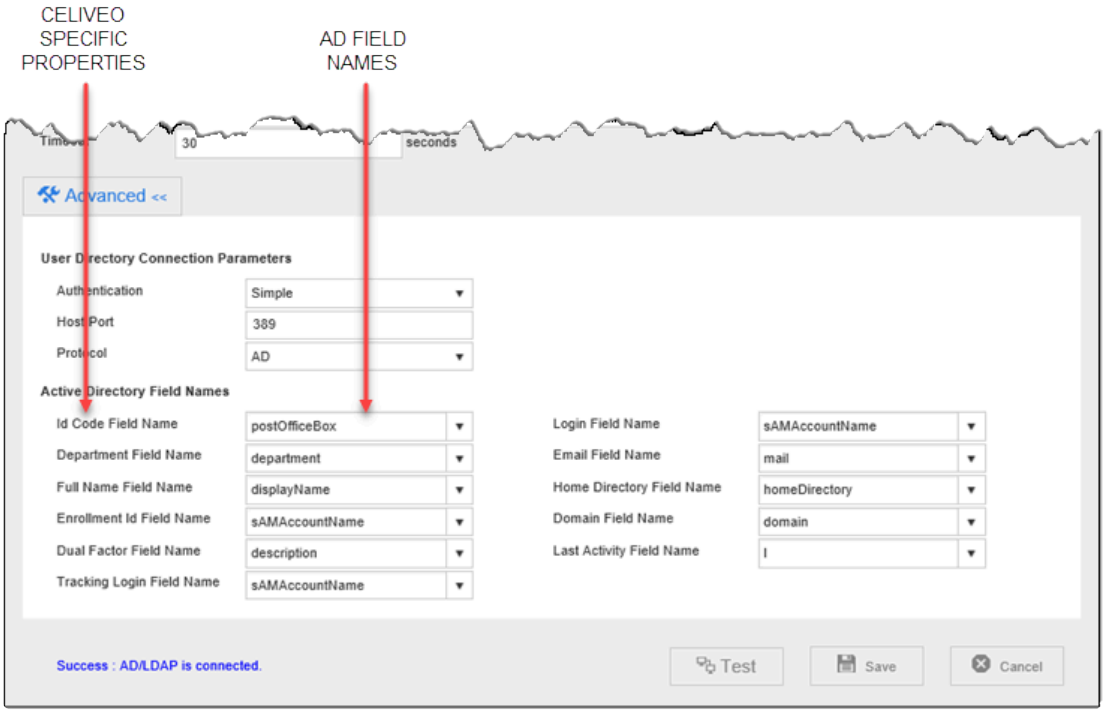
Last modified: 29 September 2022

11.5. Save Card Number and ID code on Active Directory

1. Introduction
2. How to…
   a. Specify the AD Field to Store the Card Number/ID Code
   b. Make Celiveo Save the Card Number/ID Code in AD

Introduction

In the article on Enabling Card Authentication, and Enabling ID Code Authentication, the Card Number and PIN were stored in the Celiveo Database (CeliveoDB). If required, you can store this information directly on the Active Directory (AD). However, the AD does not have field that corresponds to the Celiveo specific Id Code field, which is where the ID Code and Card Number is stored. As such, the Celiveo specific Id Code must be mapped to an unused field on AD.

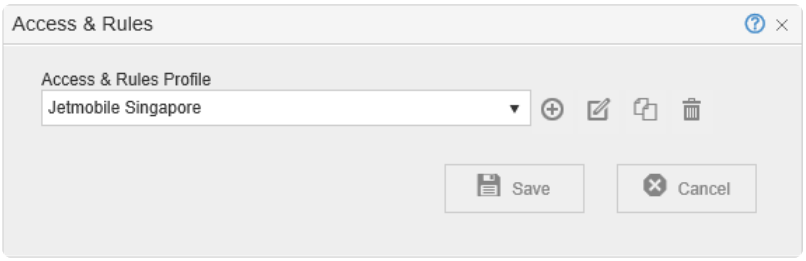


How to…

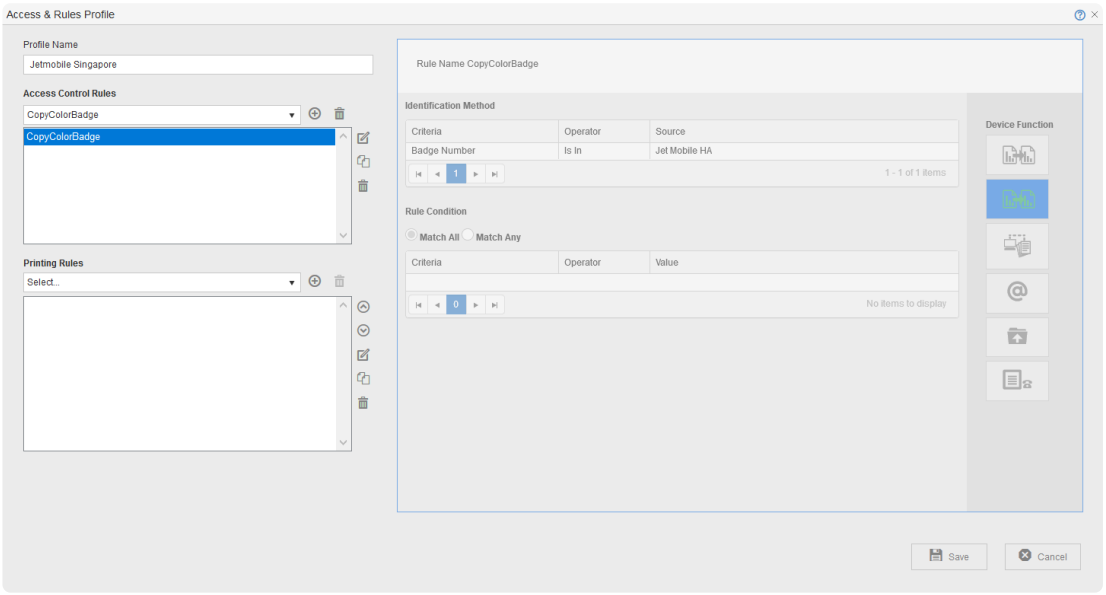
Specify the AD Field to Store the Card Number/PIN Code

1. Display an Authentication Profile that uses ID Code authentication or Card authentication.

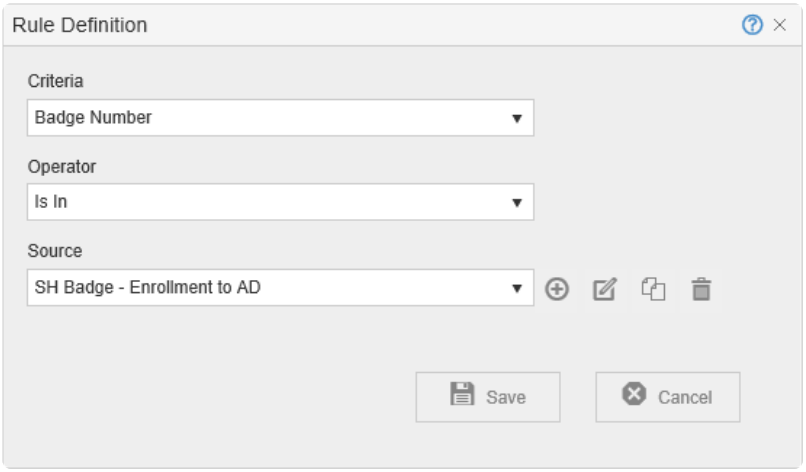
a. On the Celiveo Web Admin, at the main menu, click . The Printer List displays.
b. Select a Printer that uses Card authentication or ID Code authentication.
c. On the printer menu, click . Access and Rules is displayed.



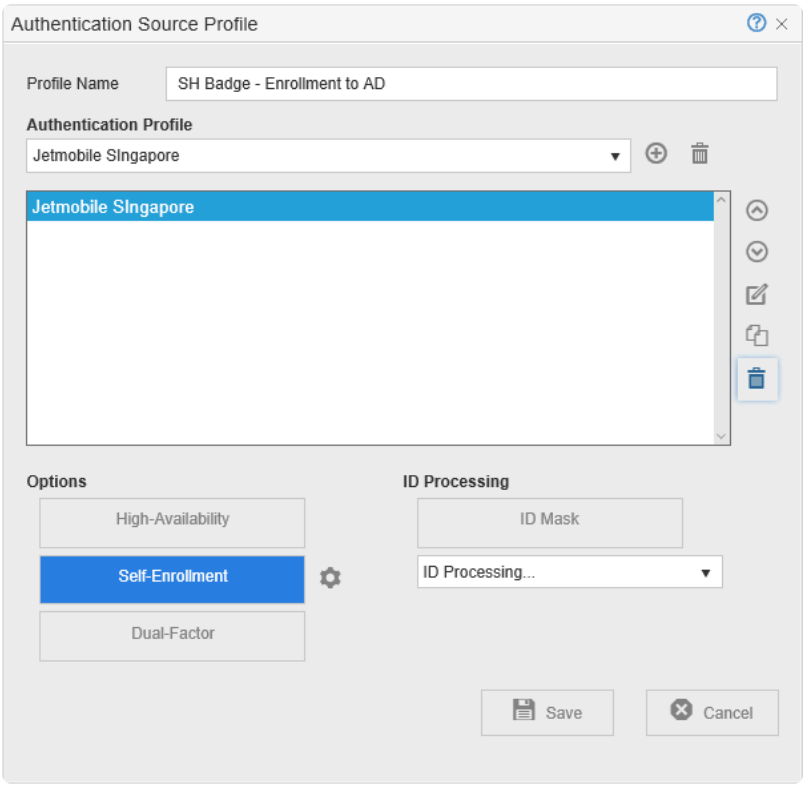
d. Click . The Access & Rules Profile displays.



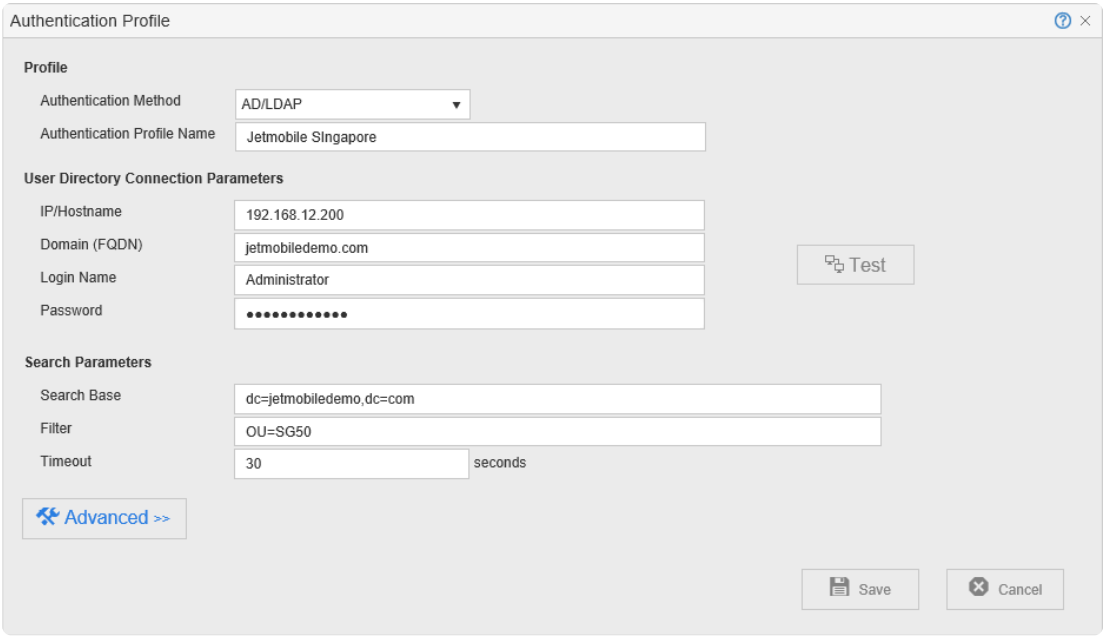
e. In the Access Control Rules section, select the Access Control Rule and click . The Rule Definition



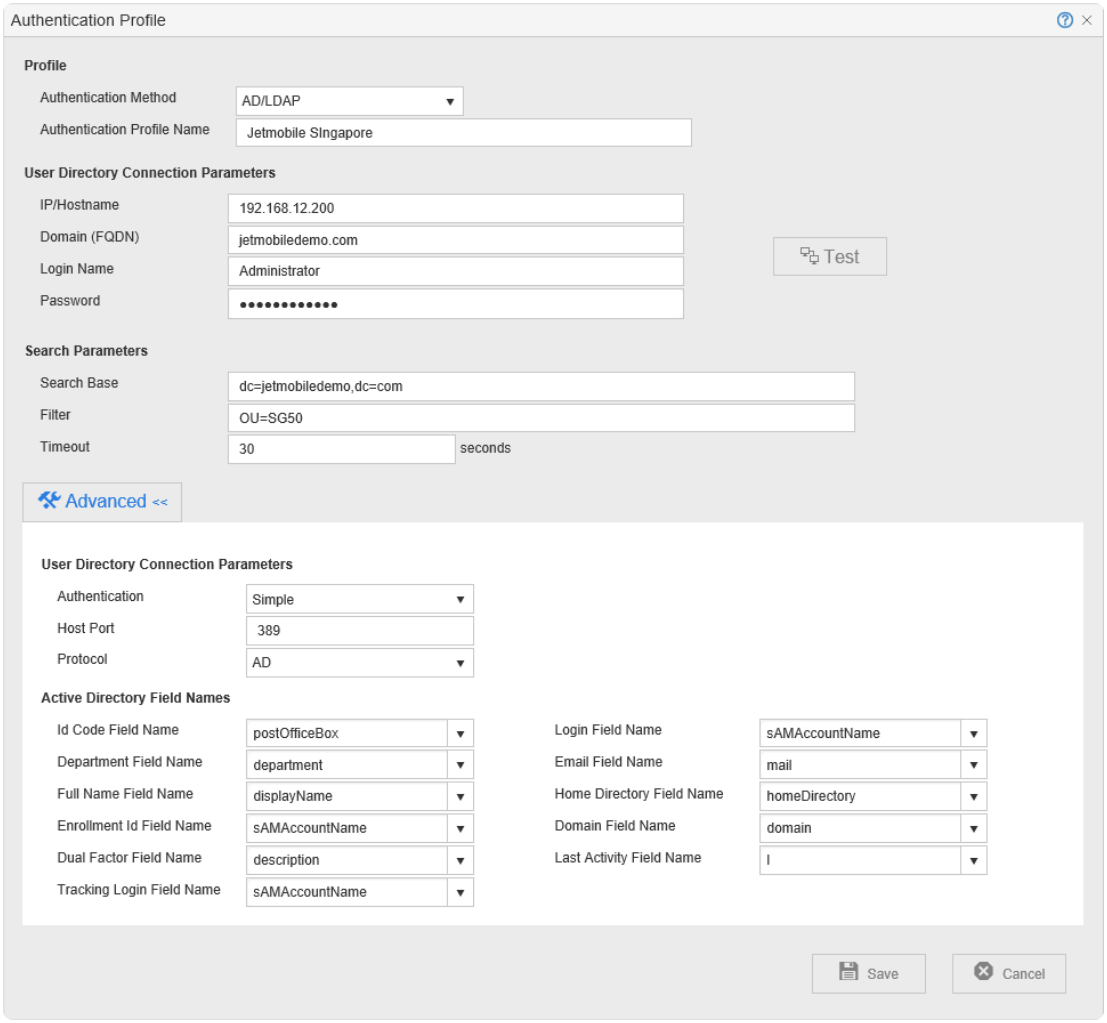
f. Click located next to the **[Source]** drop-down.



g. Select the Authentication Profile and click . The Authentication Profile displays.



2. Click **[Advanced]**. The screen expands to show the advanced properties.



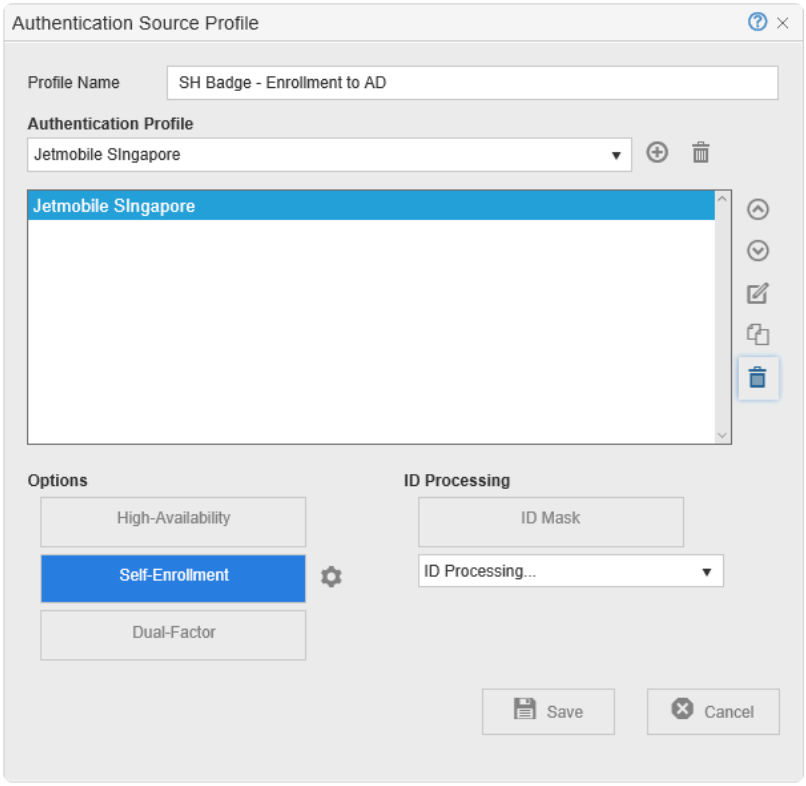
3. In the **[Id Code Field Name]** drop-down select the AD field to store the PIN Code or Card Number.
4. Click **[Save]**.

> **Note**: When using AD enrollment with SHA256 ID conversion, the field where the ID is stored needs to have a minimum length of 64.

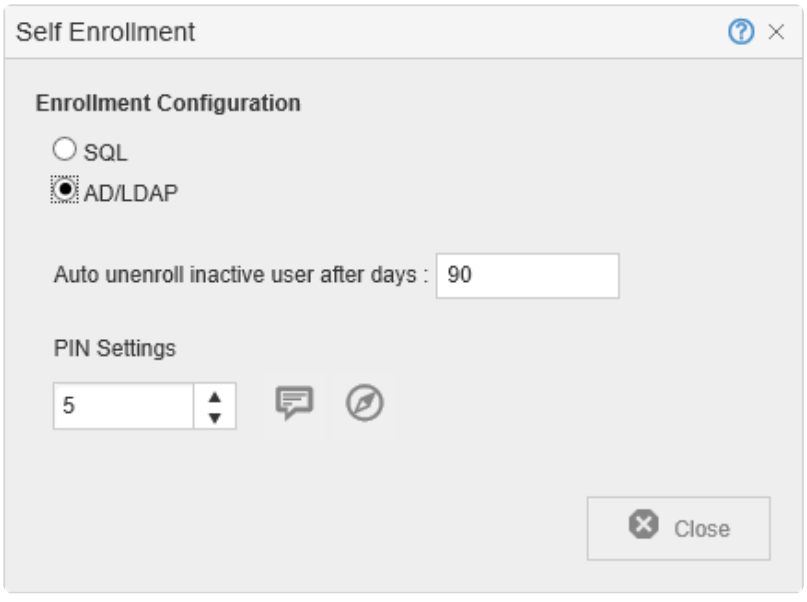
> **IMPORTANT**: It is recommended to index the AD attribute(s) where the user IDs are stored (card number, PIN code) so that live user authentication against AD is faster. By default the primary user ID attribute is stored in **postOfficeBox**.

Make Celiveo Save the Card Number/PIN Code in AD

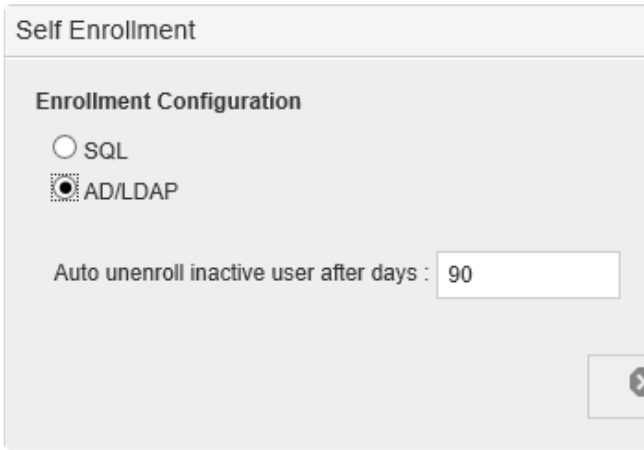
1. Display the Authentication Source profile of a printer (See steps 1 – 6) in previous procedure.



2. Click ⚙ located next to **[Self-Enrollment]**.
   Note: The settings button (⚙) is visible only when [Self-Enrollment] is turned on.
3. Select **[AD/LDAP]**.



Self Enrollment (PIN Authentication)



Self Enrollment (Card Authentication)

4. Click **[Close]**.

Last modified: 29 September 2022

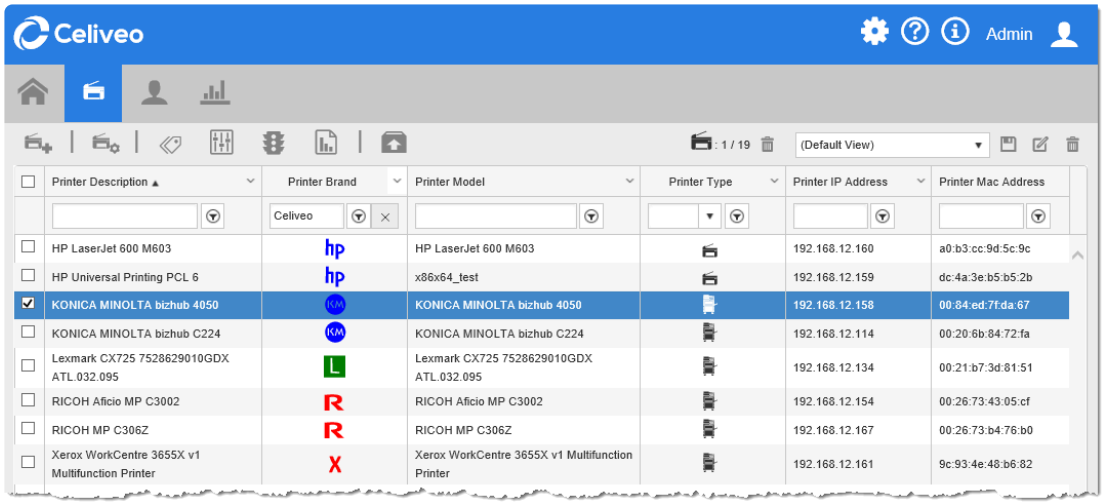
11.6. Enable Smart card authentication for printers

Enable Smart card Authentication for Printers

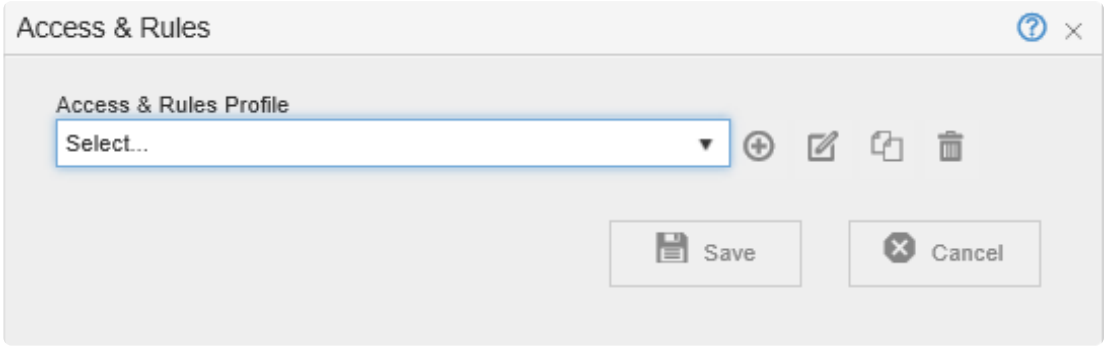
You enable Smart card authentication by creating an Access Control Rule and assigning the rule to a printer. You however cannot assign an Access Control Rule directly to a printer. Instead, you create an Access & Rules Profile for a printer and add the Access Control Rule to the Access & Rules Profile.

Workflow

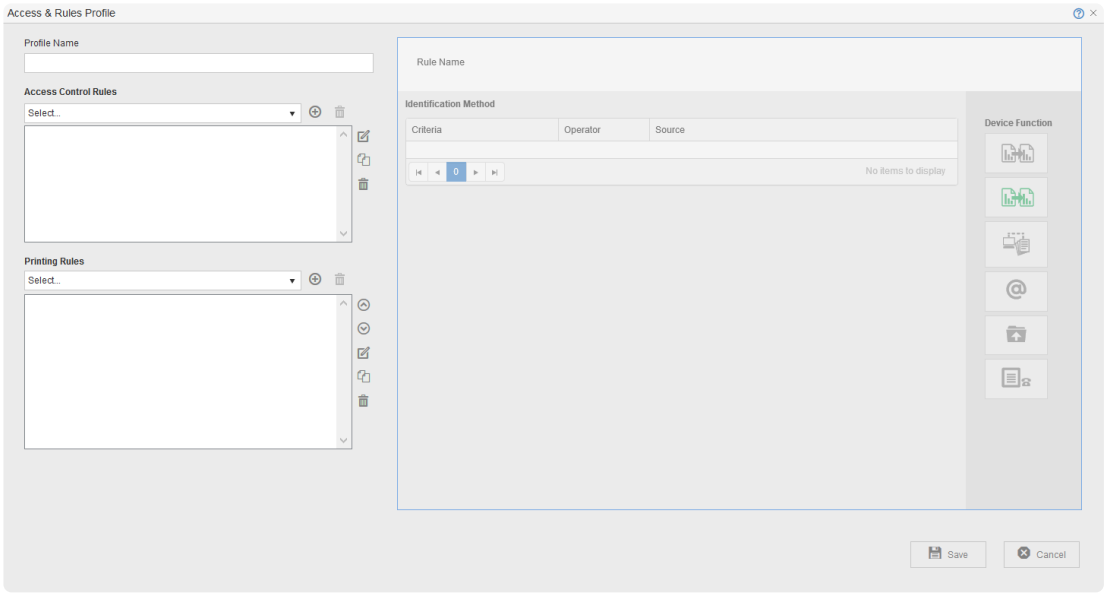
1. Add a New Access & Rules Profile to a Printer



1. Select the printer to add the Access and Rules Profile to.
2. Click . The Access & Rules dialog is displayed.



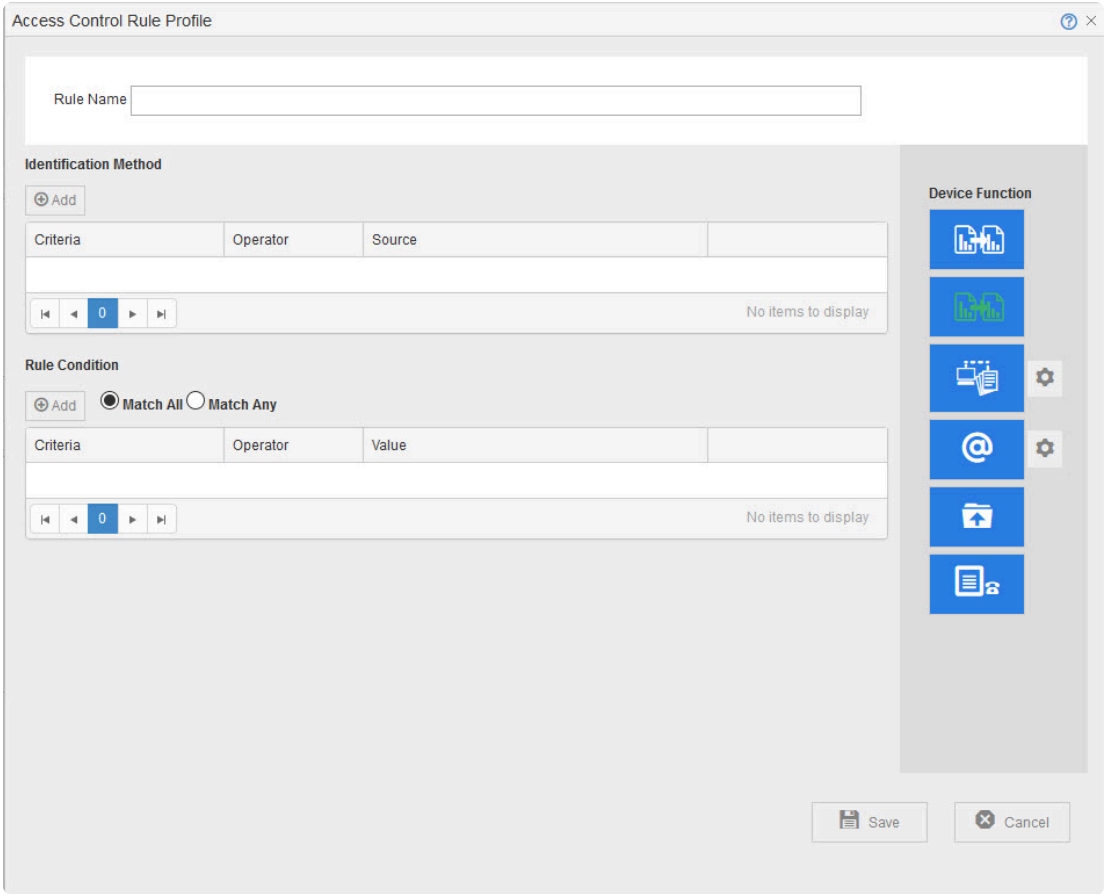
3. Click . The Access and Rules profile is displayed.



4. At **[Profile Name]**, specify a unique name for the Access & Rules Profile.

2. Add a New Access Control Rule to the Access and Rules Profile

1. Click ⊕, located in the same row as the [Access Control Rules] drop-down. The Access & Rules Profile displays.

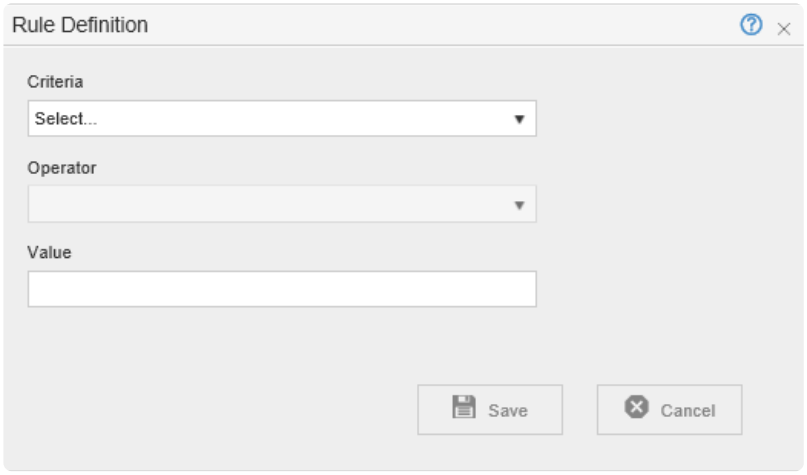


2. At **[Rule Name]**, specify a unique name for the Access Control Rule.

3. Add Smart card Authentication as the Identification

Method

1. Click **[Add]**, located below **[Identification Method]**. The Rule Definition displays.



2. From the **[Criteria]** drop-down, select **[UPN in Smartcard Cert]**.
3. From the **[Operator]** drop-down, select **[Is In]**.

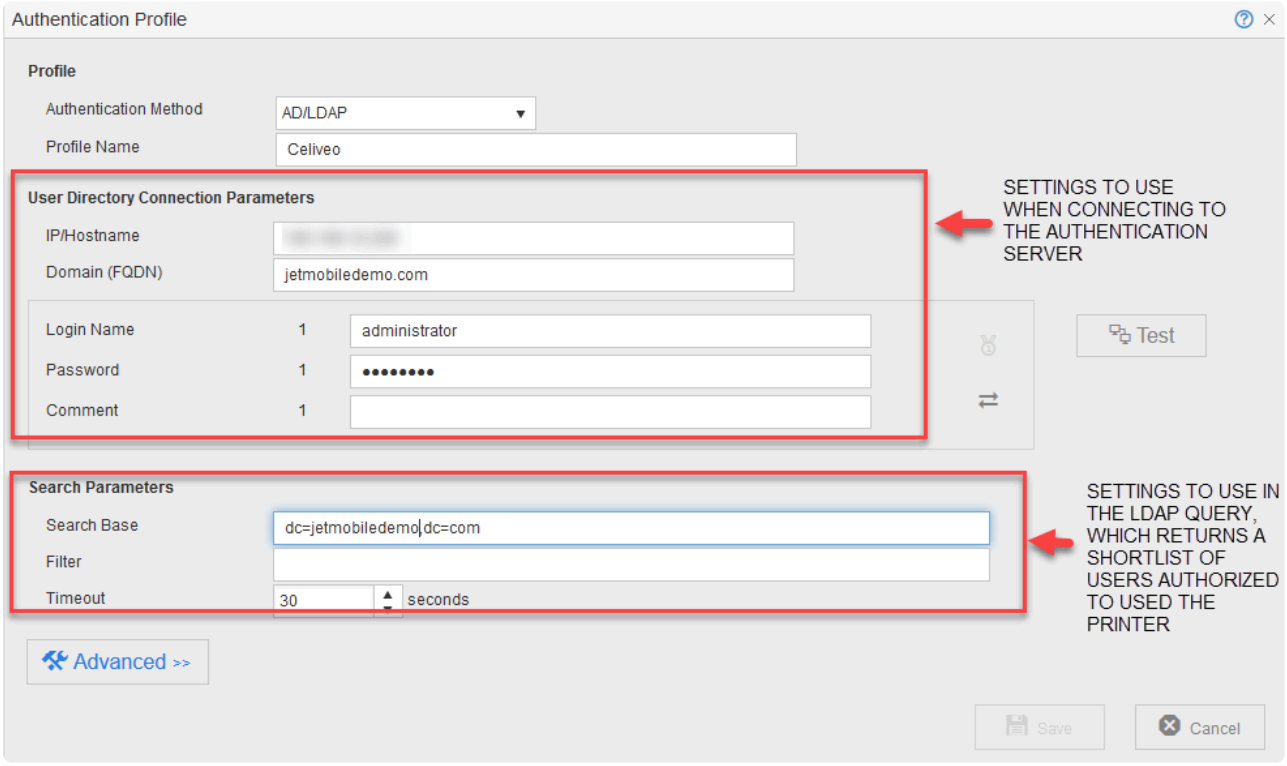
NOTE:

- A Smartcard license feature connector is required to use **[UPN In Smartcard Certification]**
- **[UPN In Smartcard Certification]** identification method can be combined with **[Username and Password]**
- **[UPN In Smartcard Certification]** identification method cannot be used with the **[Celiveo Authentication Gateway]** authentication method.

4. Build the Authentication Profile to Validate the Smart card

1. Click ⊕, located next to the [Source] drop-down. The Authentication Source Profile displays.

2. In the **[Profile Name]** box, specify a unique name to identify the profile.
3. Click ⊕, located in the same row as the **[Authentication Profile]** drop-down. The Authentication Profile is displayed.
4. Specify the AD/LDAP query (similar to that of the screen capture shown below) that returns the list of users who are authorized to use the printer.



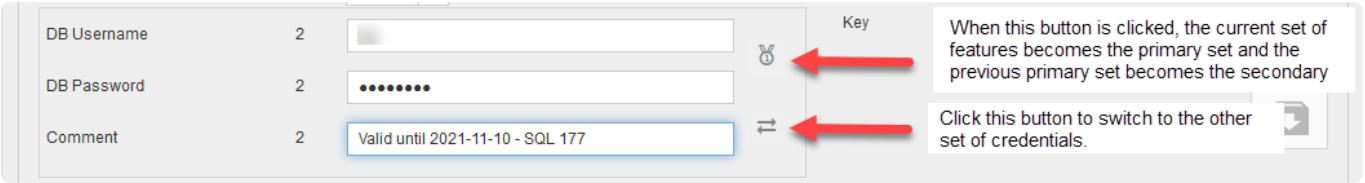
5. Click **[Test]**.
   If login to the Authentication Server is successful, a message is displayed below the **[Test]** button.

> Note: A Write error to the Enrollment Primary field will not prevent the SmartCard authentication profile from being successfully created.

6. Click **[Save]**. You are returned to the Authentication Source Profile.

Dual Service Account System

To avoid any connection error after refreshing/changing the login/password on service accounts used by Celiveo, the administrator can define a secondary set of credentials so that if the default (primary) set is declined by the solution, then the secondary set takes over and prevents the access from being denied.



p(banner tip). **Note**: The Login User (Login Name) used in Celiveo Authentication Profile requires AD/LDAP Read and Write rights to user's attributes.

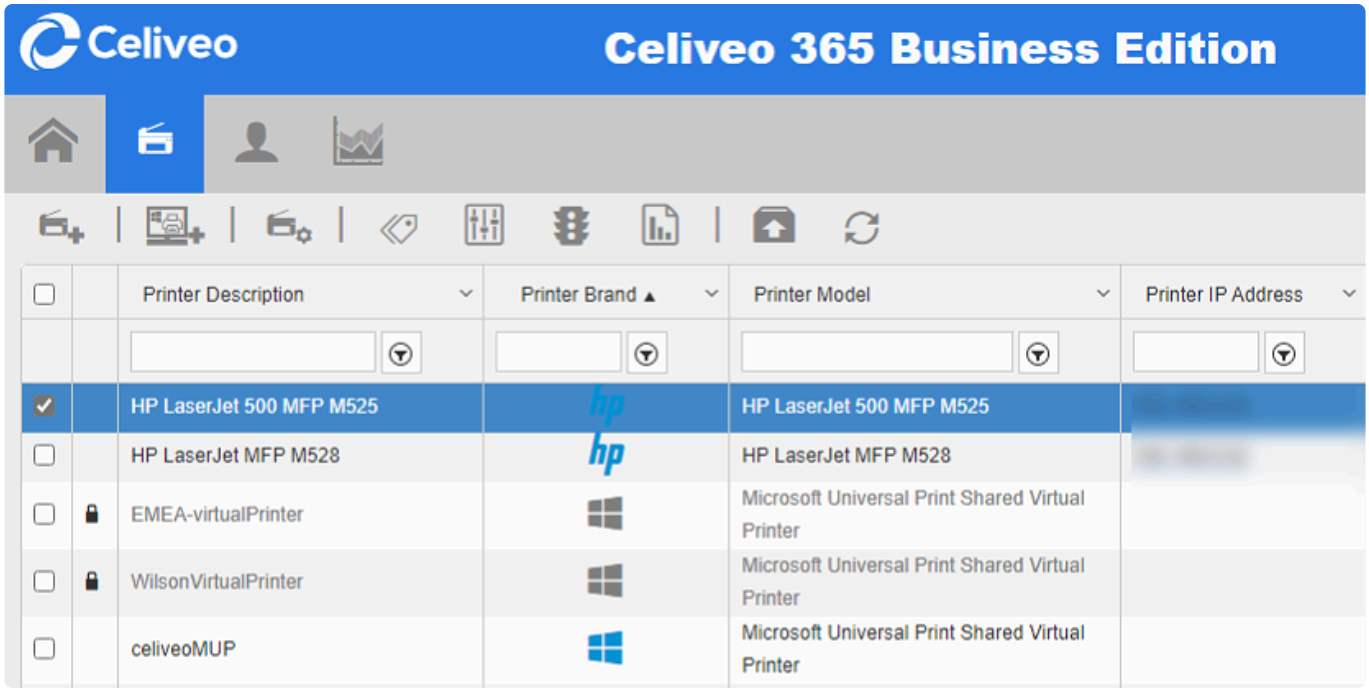
5. Specify How to Process Smart card

1. Under **[Smart card]** section, click **[Upload Smart card configuration File]** to upload a SCAS file.
2. Click **[Card Validation]**.
3. Click the settings icon next to **[Card Validation]** to configure the Card Validation settings.
   You can select any of the validation methods:
   - **Pin Code**: You will be prompted to enter a pin code after inserting the Smart card into the reader.
   - **Certificate Expiration Date**: The Smart card is verified using the Certificate expiration date.
   - **Certificate KeyPair Validation**: The Smart card is verified using the Certificate Keypair.
   - **Certificate Authority**: The Smart card is verified using the Certificate Authority file. You can add multiple certificate authority files for card validation. Select a file in the drop-down list or click the + icon next to the drop menu to add a new certificate authority file.
   - **CRL**: The Smart card is verified using the Certificate Revocation List (CRL). You can only use one CRL file for card validation. Select a file in the drop-down list or click the + icon next to the drop menu to add a new CRL file.
4. Select **[High Availability]** option, to configure the settings that determine how to manage authentication when the printer cannot connect to the organization network.

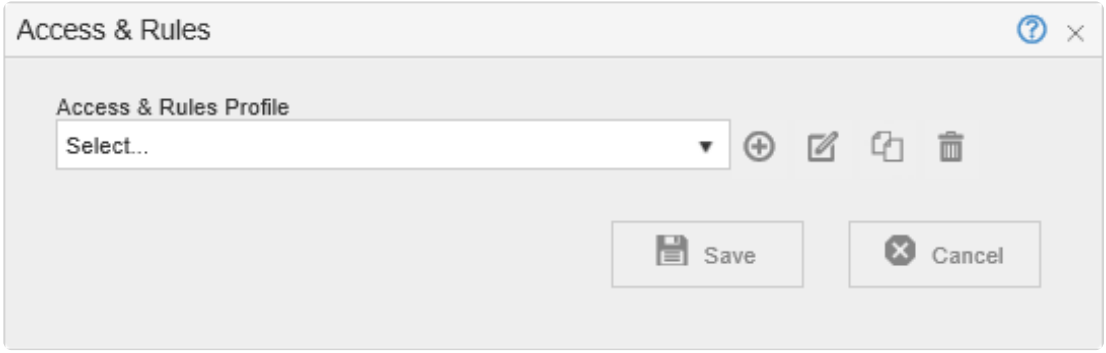
> **IMPORTANT NOTE**: For security reasons, Smart Card Authentication support High Availability feature in **Dynamic Cache** mode with **Read Cache Last** method only. **Read Cache First** method selection, if configured, will be ignored and no cache will be applied.

5. Click **[Save]** until all dialogs close.

6. Enable Smart card Authentication for Remaining Printers



1. In the Printers List, select the printers you want to apply the Access and Rules Profile to.
2. Click . The Access & Rules dialog is displayed.



3. From the **[Access & Rules Profile]** drop-down, select the Access and Rules profile for the Printer.

Last modified: 10 October 2022

11.7. Configure BLE RF IDEAS Readers for Smartphone Authentication with Orange Pack-ID Application

Celiveo engages with Orange Pack ID for mobile authentication at the printer (reader). Users can store their Card (Badge) ID credentials in their smartphones via this mobile app and can authenticate using their Smartphone at the Reader to successfully login at the printer.

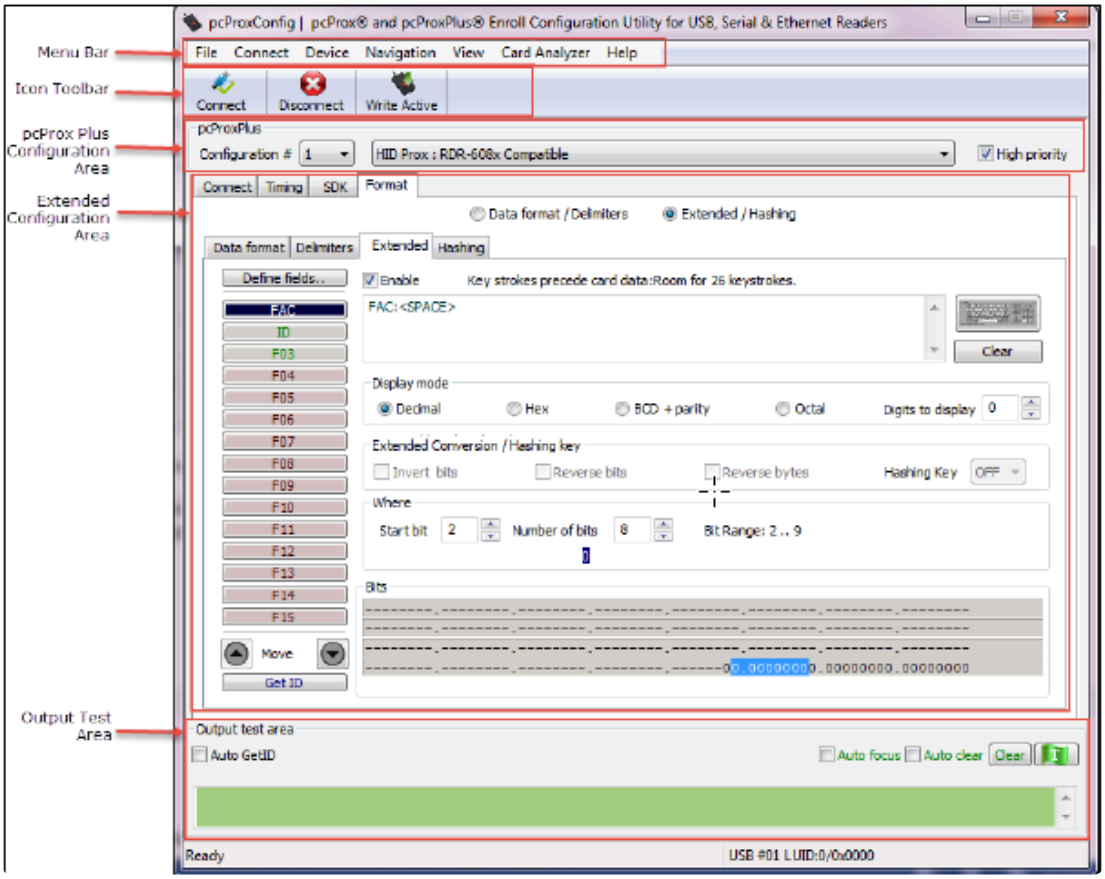
Using the pcProx Configuration utility tool, the BLE pcProx Reader can be configured to read user credentials from Orange Pack ID.

Configuring BLE RF IDEAS Readers for Smartphone Authentication

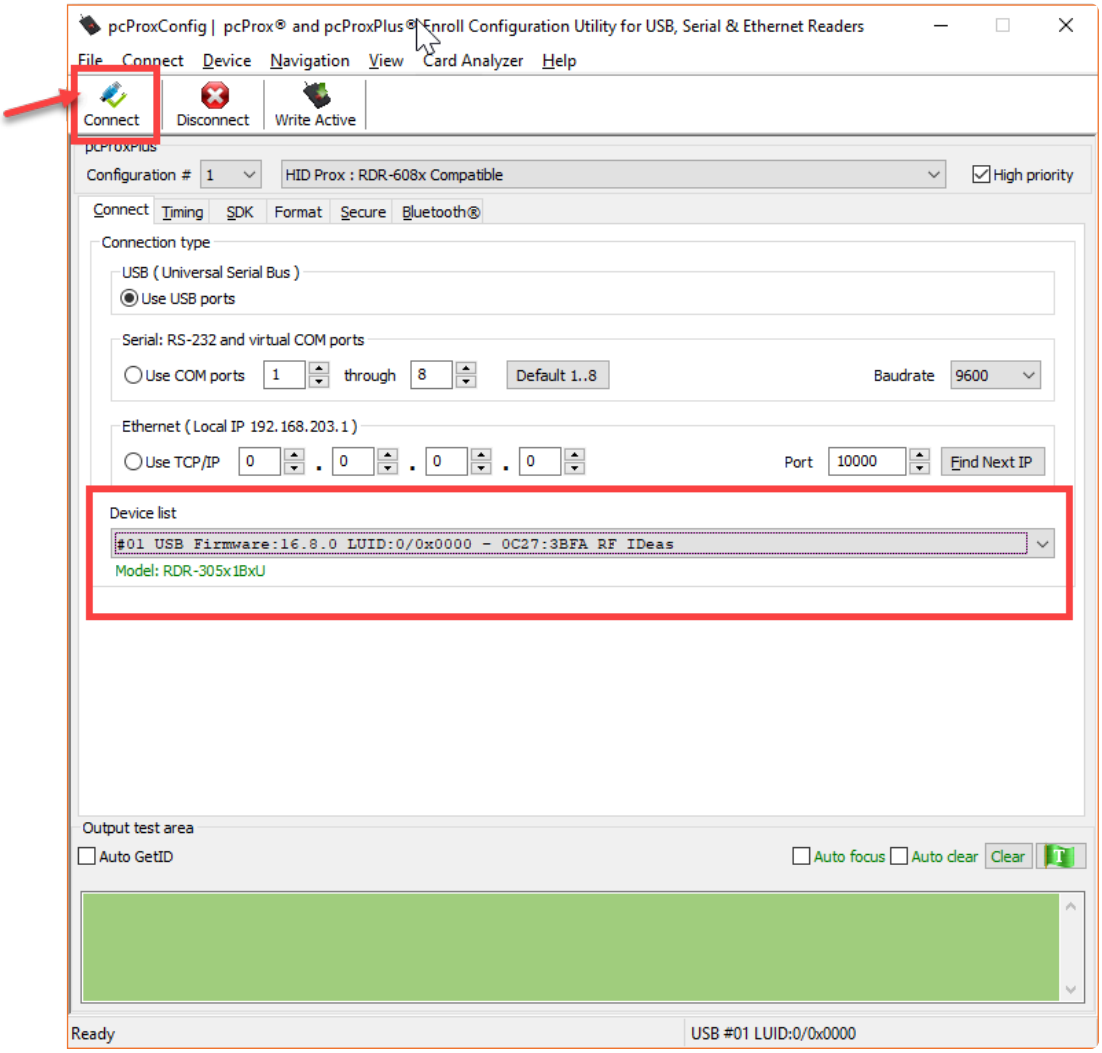
You will need to install the **pcProxConfig** tool to allow configuring the reader for Orange Pack ID, obtainable at https://www.rfideas.com/support/downloads

1. Unzip the file pcProxConfig-5.2.39.zip and install the executable on a Windows **PC**. After installation the pcProxConfig icon will appear on your desktop. When you start the utility, the screen should look as below. (The USB cable of the RF IDeas reader should be plugged into the USB port of the PC).

> **Important**:
> The reader P/N as displayed on the label must be RDR-30581BKU-SFT or RDR-30582BKU-SFT
> You **MUST** use version 5.2.39 of pcProxConfig.exe or newer. Older versions will not work.



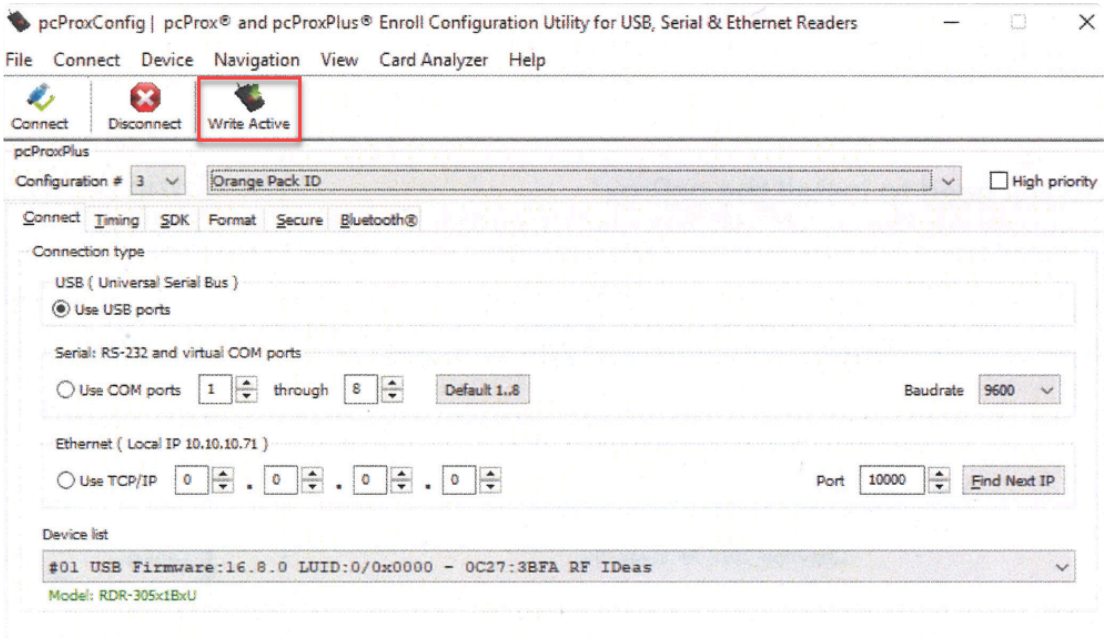
2. Connect the pcProx® Plus BLE Reader to the system via USB port.
3. Click **Connect** on the Icon toolbar menu.
4. The model number and VID/PID of the Reader will be displayed on the Device list.



The Model number RDR-305×1BxU must be displayed in green font as shown, indicating that the reader is connected.

Note: If Orange Pack ID does not show up, you may be using the wrong version of pcProxConfig, or you may have the wrong reader.

5. Configure the settings to 3 and choose Orange Pack ID in the options.
6. Click **Write Active**. This allows to write the configurations selected to the device.



The reader is now configured to read the Pack ID mobile credentials.

Note: If “758x Equivalent” configuration is left turned on, iPhone users will experience Apple Pay automatically opening when the phone is tapped to the reader. To prevent this, Configuration #2 can be set to OFF.

Last modified: 29 September 2022

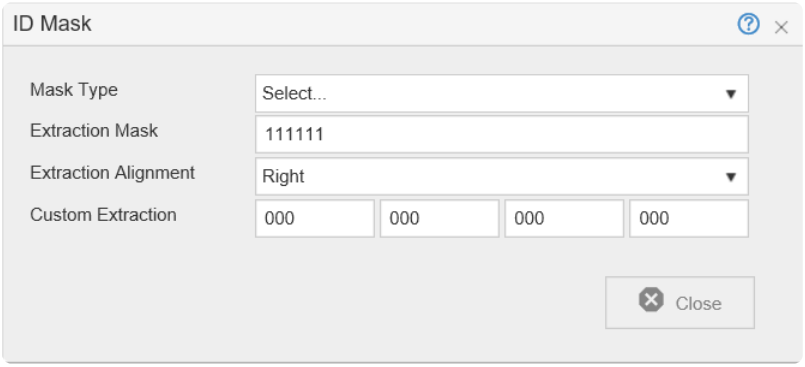
11.8. Configure ID Mask

Masks are used to extract values from specific positions of a badge ID. When you select a standard reader type from the [Mask type] drop-down, the corresponding ID mask is automatically applied when the badge ID is read.

Celiveo uses HID Type B (OMNIKEY 5×27 CK) card reader.

To configure ID mask under Authentication Source Profile in Web Admin:

Select a reader card type to apply an appropriate ID mask or configure a custom mask.



Select reader type

At **[Mask type]**, select a reader type and click **[Save]**. The relevant mask will be applied.

Mask type	Card Type
Magnetic Card Track 1	Swipe card reader
Magnetic Card Track 2	Swipe card reader
Magnetic Card Track 3	Swipe card reader
HID 26bits Corp	Proximity reader
HID 34bits Corp	Proximity reader
HID 35bits Corp	Proximity reader
HID 37bits Corp	Proximity reader
HID 37bits Cn Corp	Proximity reader
EM-Marin	Proximity reader
HITAG	Proximity reader
LEGIC	Proximity reader
MIFARE	Proximity reader

Configure custom ID mask

1. At **[Mask type]**, select **[Custom Mask]**.
2. At **[Extraction Mask]**, Enter the extraction mask to apply to the badge number string.
    - The mask allows the extraction of a smaller value from a badge value. It can consist of values ‘1’ and ‘X’. ‘1’ retains the digit, ‘X’ removes the digit.
3. Select the alignment of the extracted mask.
4. Set the values of **[Custom Extraction]**.
    - (for HID Prox badges only) Enter the first and last bit numbers for the site code followed by the first and last bit numbers of the badge number. This allows for the extraction of a range of bits from a badge. The mask is a ‘D’ followed by a 12-digit string D’aaabbbcccddd’ where:
        - ‘aaa’ is the first bit number for the badge site code
        - ‘bbb’ is the last bit number for the badge site code
        - ‘ccc’ is the first bit number for the badge number
        - ‘ddd’ is the last bit number for the badge number

Once settings are complete, click **[Save]**.

HID Card Data Formats

Knowledge of the card format allows to properly decode the data. The 26-bit Wiegand standard format is the industry standard used globally. You can also learn more about HID Card Data formats in the article here.

Last modified: 29 September 2022

11.9. Custom Access Control for HP FutureSmart Printers

What is Custom Access Control?

Celiveo administrators are able to force a customized OXPd Authorization Agent Configuration – also called Authorization Proxy – on HP FutureSmart printers.

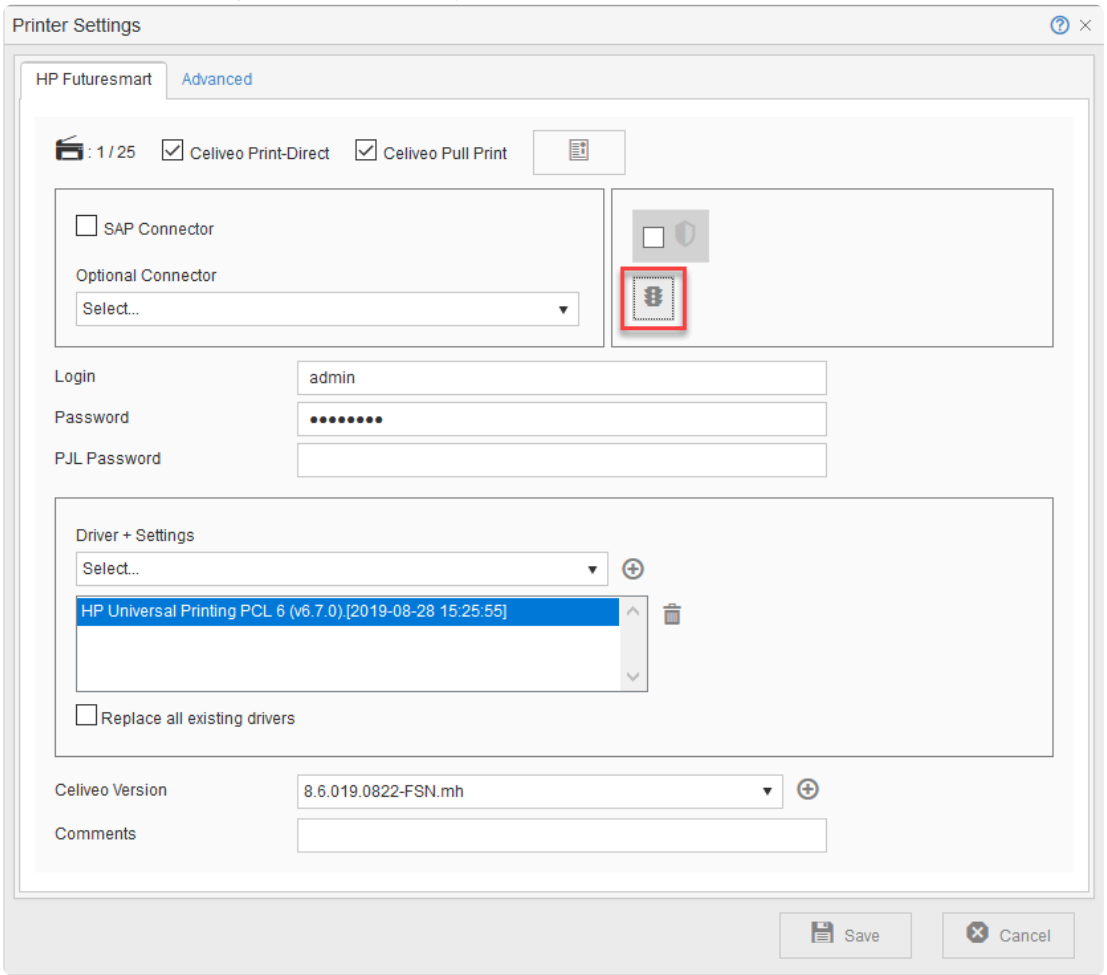
This allows to define which Printer functions are controlled by Celiveo.

How to apply Custom Access Control?

Celiveo has a default Authorization proxy configured on the printer by the solution. The Web Admin allows the download of the default XML configuration file for an admin to customize it and upload it back to the Celiveo Web Admin in order to be deployed on printers.

To do so:

1. In the Web Admin, select your HP FutureSmart printer and click the **Printer Settings** icon.
2. The Printer Settings window displays.



3. To enable Custom Access Control, click the icon.

4. The options display:

Download icon – This allows the download of the current Celiveo OXPd Authorization Agent configuration. If the Celiveo OXPd Authorization Agent is disabled, a sample file will be downloaded as a reference. This file can be edited with custom configuration and then uploaded to the Web Admin.

Note: The sample file will not reflect any setting applied on the Printer EWS or via any third party software such as HP WebJetAdmin.

Upload icon – This allows to upload the modified Access Control file. This requires the printer to be synchronized again for the new settings to be applied.

Reset icon – This will remove the Celiveo OXPd Authorization Agent. This also requires a new printer synchronization.

Note: If the Reset option is used, the Celiveo Access Rules will not be applied on this printer. The user can then configure Access Control on the Printer EWS or using any third-party software such as WebJetAdmin.

How to customize the configuration file?

Understanding the Configuration file

The XML file begins with a section which gives you an identifying code (GUID) for each Printer function, called “Permission” and each Sign-in Method available on the printer.

The section starts with the **< OxpdConfigurationReferenceObjects >** element and contains 2 sub-elements:

- **< PermissionList >** which provides the GUID for each permission.

- **< SignInMethodList >** which provides the GUID for each Sign-in method.

You will need the GUIDs to customize the configuration file.

As an example, this is the GUID for the “Print from USB Drive” permission:

```
··<Permission>CRLF
····<id>12642a24-5e74-41a2-a154-20d20436abee</id>
····<name>Print·from·USB·Drive</name>CRLF
··</Permission>CRLF
```

Customizing the Configuration file

The actual rights given are in the section which begins with the **< OxpdAuthzProxy >** element and are divided into three sets:

- **< guestPermissionId >** All printer functions (Copy, Fax, Scan, etc.) that you need to be accessible without authentication (Guest Access) need to be identified in this section. Put each Permission GUID under the **guestPermissionSet** element and inside the **guestPermissionId** tag.

In this case:

```
··<guestPermissionSet>CRLF
····<guestPermissionId>12642a24-5e74-41a2-a154-20d20436abee</guestPermissionId>
```

Users can Print from USB Drive without Authentication.

```
··<Permission>CRLF
····<id>12642a24-5e74-41a2-a154-20d20436abee</id>
····<name>Print from USB Drive</name>CRLF
··</Permission>CRLF
```

- **< PermissionToSignInMethod >** In this section, you will define which specific Authentication Agent will be used for Authentication on each printer function.

Under the **< PermissionToSignInMethod >** section, put the Permission (function) GUID inside the **permissionId** tag and the corresponding sign-in method GUID inside the **signInMethodId** tag.

In this case:

```
··<PermissionToSignInMethod>CRLF
····<permissionId>cedab422-33b3-4638-b6a1-604e54525215</permissionId>CRLF
····<signInMethodId>60c23e33-38f5-4584-884a-c7d4999e63d0</signInMethodId>CRLF
··</PermissionToSignInMethod>CRLF
```

The “Copy” function requires the user to be authentified by Celiveo.

```
<Permission>CRLF
··<id>cedab422-33b3-4638-b6a1-604e54525215</id>CRLF
··<name>Copy</name>CRLF
</Permission>CRLF
```

```
····<SignInMethod>CRLF
····· <id>60c23e33-38f5-4584-884a-c7d4999e63d0</id>CRLF
····· <name>CvoAuthSC</name>CRLF
····</SignInMethod>CRLF
```

- **< defaultSignInMethod >** Put the desired sign-in method GUID inside the defaultSignInMethod tag.

Put the desired sign-in method GUID inside the **defaultSignInMethod** tag.

Here, the default sign-in method is the Celiveo Authentication Agent.

```
··<defaultSignInMethod>60c23e33-38f5-4584-884a-c7d4999e63d0</defaultSignInMethod>
```

```
····<SignInMethod>CRLF
·····<id>60c23e33-38f5-4584-884a-c7d4999e63d0</id>CRLF
·····<name>CvoAuthSC</name>CRLF
····</SignInMethod>CRLF
```

- **< allowAlternateSignInMethods >** This element value should be set to “False” in order to restrict the access to the activities with another Authentication Agent. By default, it is set to “True”.
- **< addNewPermissionToGuest >** This element , when set to “True” will grant the Guest Access to newly installed applications (when Celiveo is already installed). Otherwise, the New Applications (Permissions) will be locked by the Default Sign In Method. By default, it is et to “False”.

Sign-in Methods GUIDs

Description	GUID (Permission ID)
Celiveo Authentication for Celiveo Badge, PIN and Username and Password profiles	60c23e33-38f5-4584-884a-c7d4999e63c9
Celiveo Authentication for Celiveo Smart Card profiles and Celiveo Smart card profiles with Login and Password as secondary profile	60c23e33-38f5-4584-884a-c7d4999e63d0
Celiveo Dual Factor Authentication for Celiveo Badge with Dual Factor Enabled profiles	60c23e33-38f5-4584-884a-c7d4999e63d1
Celiveo Enrolment with the Celiveo “Enroll Me” Permission	d4840600-9f9b-434f-b4b1-56e6c78b971f
HP Pin Authentication Agent	41accec0-a865-4dc5-9e1f-25ab790ebec0
HP LDAP Agent	8a3a1a8c-773f-8b17-1dc6-1780745631a2
HP Windows Agent	5470b2ae-29cf-415b-a22d-349b50c9cb13

Control Panel Features GUIDs

Description	GUID (Permission ID)
Settings	3dfe6950-5cf9-41c2-a3b2-6154868ab45d
Copy/Print	3c06acc4-f0e9-4248-8933-4aa500cee7b8
Manage Stored Jobs	fbd10c44-f550-498a-bfa0-b7e634afa551
Manage Trays	d41cc382-c023-46dc-b722-4178a599901a
Enable Print from USB Drive	7b8e9297-1c88-4316-b1c8-ed7a5b8eb4c7
Default Print Options	07799ea1-52ea-4cc8-8dbf-1458dc2f39d1
Print Quality	dceabb35-81d0-4c5f-a2f8-4c9c318b043b
PCL and PostScript Settings	7389ff49-20e5-41ff-9b96-5c1df60d7e67
Scan/Digital Send	2565f335-e4ad-4cde-966d-30d9f3f1999f

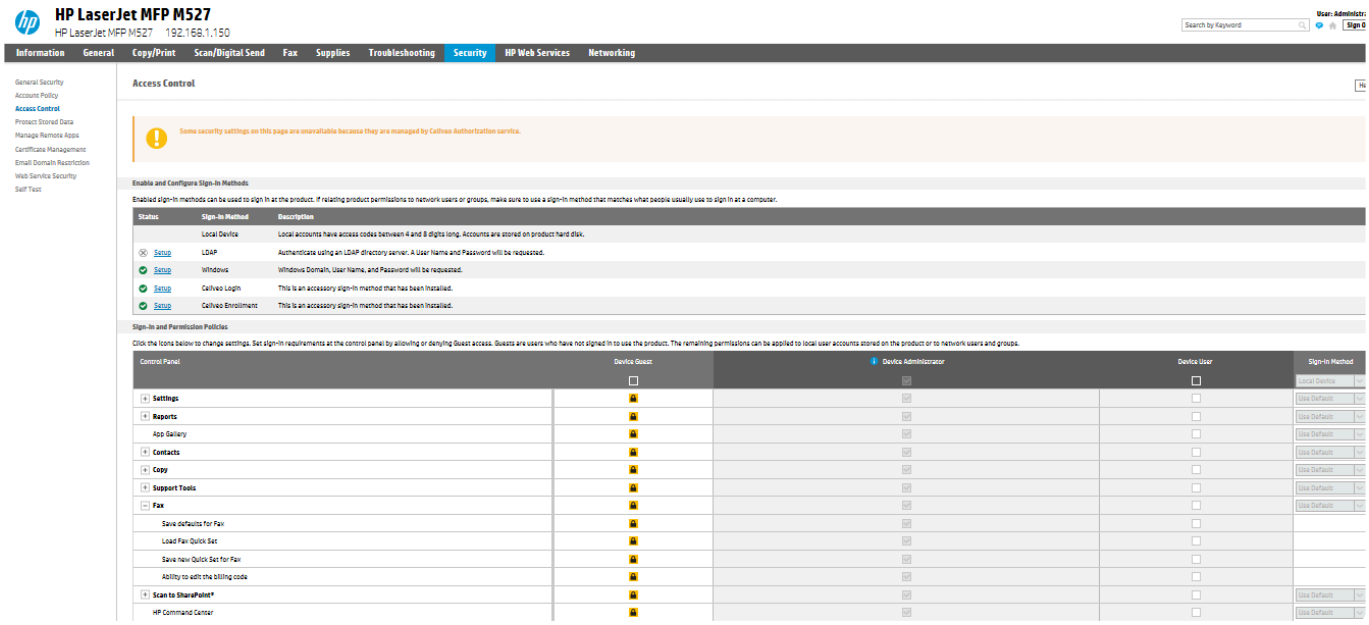
Email Settings	a639160a-7b18-4c02-b4a4-00b9026f00d6
Email Setup	52099d81-6fd5-481f-84ef-588c8ce39a3c
Scan to USB Drive Settings	4d1dc259-0d38-4bfd-b121-b11c22bc67bc
Network Folder Settings	74d83bcd-0cd0-4f89-aca5-39df93cb0b0d
Digital Sending Software (DSS) Setup	c980a35a-3e93-4971-b8c6-f76cbfbeedcf
Fax	965dabb4-8d1a-42df-943a-74c368a4c144
Fax Send Settings	eca4c819-4f03-458c-9aff-62f4be730e0b
General	a062b6d9-8475-4663-8bbf-c9ed15e8d460
Date/Time	defd075a-d6a7-498e-9efb-4b9465a8c091
Display Settings	cdd8157e-c605-473d-939b-98994607a436
Energy Settings	fdc59fb8-3a54-426d-9f5a-2d9087233bb0
Restore Factory Settings	b532012c-4017-472a-97d7-625f628bf75b
Enable Device USB	74425807-8557-49ae-820c-ce203f15e96b
Manage Supplies	1a2d31a0-b6c8-4497-a708-707792bd2609
Networking	4fdcd8b2-6e7e-44da-924a-85981a727c1b
Network Protocols	4692a241-8998-4aa8-9d31-1f8ccb43ea14
Reports	34876b06-05be-4044-b61c-40cca9dfe4cb
Configuration/Status Pages	7bb1b399-d731-4f3e-a013-82ce9ea9434f
Supplies Status Page	978af7de-4501-4709-b4e6-ecc056d41917
Usage Page	7e162dc5-a9af-4af2-b3a3-48c2d6e6bb7b
Configuration Page	c4fc5dcf-d03f-46e0-8e42-085ec5c3c108
File Directory	a12676bb-aa09-44bf-9608-a8d14cde50d7
Fax Reports	f22bab25-0bde-4983-9e28-24e536f13981
Blocked Fax List	5d1f0b3f-131e-4901-9807-a17d21ed11ba
Fax Activity Log	8591cb93-584c-43db-af22-eb9a817add9c
Billing Codes Report	84fc50f6-338d-4f5c-baba-e3a90418f364
Last Fax Call Report	d13fe446-6403-40c4-8f95-c734978d3dd3
Other Pages	81fbf819-ac36-481d-8736-c66a20a3ce75
App Gallery	4443c06a-0b8a-4442-aad7-ac773c9B9cee
Contacts	900a0d59-533a-497e-8e89-2b5bc898d5cc
Ability to edit a Speed Dial	ed979c88-86e4-422a-9842-6da6d53b431b

Ability to manage contacts in a Personal address book	1047e094-c564-4bcc-8a14-370bfddfb796
Ability to manage contacts in shared address books	6d777dcb-f62b-4cec-b536-c39078e14fc5
Copy	cedab422-33b3-4638-b6a1-604e54525215
Save defaults for Copy and Scan to Job Storage	57325ed2-49cd-4253-86f4-dc9af7103bda
Load Copy Quick Set	1fc3f42a-f887-461c-a27a-66a73156308a
Save new Quick Set for Copy	6b27ea0c-5311-4ce7-b0a8-aa4d21afe76b
1-sided copy output	7deecd46-5c05-4ce7-9c23-0c6fa1d5fc01
Support Tools	1d370ecf-fb74-44ae-8934-39740a6911ed
Troubleshooting menu	a9e3da1b-8173-419f-bd6a-2cc325567c4c
Retrieve Diagnostic Data	e4835c1f-7f0e-446b-9fc2-f18ef145698f
Fax	44aa632b-cfa3-4c10-8cab-697a9bef610b
Save defaults for Fax	016d46c6-5a3a-4646-910d-0ede122b949e
Load Fax Quick Set	8b99a8ad-9432-48a1-baca-22b0df6c65e4
Save new Quick Set for Fax	c33fdc04-682f-43ab-9f70-fdedfdc1d74b
Ability to edit the billing code	922cd28d-77a8-47a8-85c4-f117f5f69c82
Scan to SharePoint®	a3d696df-b7ff-4d3d-9969-5cd7f18c0c92
Ability to edit the SharePoint® path	19363c7c-235e-4c78-8be3-fb4673d59b25
HP Command Center	A935C131-CBE6-4d09-9AC2-624C12A9033B
Job Log and Active Jobs	56ce9217-377d-4d5c-a950-a2ad37c07882
Details or Cancel any user’s job	3c40cf32-1d3d-4051-9ba2-0a7b839b0288
Ability to Promote any user’s job	4068badd-7fa0-4c8f-b875-bf7e04dec26e
Ability to view other specific users’ jobs in the Job Log	ef4dbcd9-34d5-46e2-af53-1bacda9e2a34
Print from Job Storage	87550e5e-f927-11df-950b-00306e48bff7
Stored Faxes	d544b0ba-a3fb-4911-a82b-bf4f891b3308
Delete protected jobs without entering the password or PIN	a4dfaedc-7724-48ea-948a-5cd7b11407f0
Ability to view other specific users’ jobs and folders	535ea693-db6d-4beb-b548-f1693460eab3
Scan to Job Storage	d6c8dbb4-0cea-4147-b8a7-0cffd9c3ca90
Print from USB Drive	12642a24-5e74-41a2-a154-20d20436abee
Remote Scan Request	573619b2-7527-48b7-9ef7-ea0dcca519b5
My Print Jobs (Celiveo)	b629740c-1667-11da-a344-0010837a5f07

Enroll Me (Celiveo)	b629740c-1667-11da-a344-0010837a5f08
Email	b8460c9e-43c8-4290-a0f8-8ce450867f09
Ability to edit the BCC field for email	1502c3b6-db02-4010-ab27-a9a11f353ff0
Ability to edit the CC field for email	eb70fc52-81a7-4261-9978-f31c09ed87dc
Ability to edit the From field for email	5a707440-966b-4598-9c9b-29b08838d9a7
Ability to edit the body of an email	1d073e3c-7bd1-4269-b029-4e26c17c65b8
Ability to edit the Subject field for email	e56b78b2-5081-4473-9761-f90c79cca974
Ability to edit the To field for email	b35a7519-0680-46cd-834c-3096ab8a8692
Save defaults for Scan to Email	d5e988c7-c39c-4e77-b53f-51c6fdea210a
Load Email Quick Set	d8a96619-9aba-4249-afac-b2db90d0ca8b
Save new Quick Set for Email	5af2a754-d27c-40a4-a56d-2e7191def383
Scan to Network Folder	65acca51-619d-4e29-b1d0-6414e52f908b
Save defaults for Scan to Network Folder	f69557b5-82f6-4269-894c-1b4046a0a92a
Ability to edit the network folder path	ee19ffb2-d93c-42ab-a23b-b868a63304a3
Load Scan to Network Folder Quick Set	3ecf76a7-4ebe-4265-8cdf-22f4f359daf9
Save new Quick Set for Scan to Network Folder	f753d9a7-c4fc-47c8-abd3-49d901528f29
Scan to USB Drive	09866970-7133-404f-bb20-440b9148e8e2
Save defaults for Scan to USB Drive	00aed7aa-fc3b-4d18-81dd-e46365576f6a
Load Scan to USB Drive Quick Set	1bd63e89-82c9-4360-82c6-1fe9b4241247
Save new Quick Set for Scan to USB Drive	4044fe20-84a3-4314-a708-35626144609b
Supplies	a5e59604-d216-4977-a901-4774fcacbcb4
Trays	
Ability to modify tray size and type settings	e402dfff-566a-45c9-a0d3-18350436666e

On the Printer Panel

Once the configuration file has been customized and uploaded to the Web Admin and once the printer has been synchronized, the Custom Access Control configuration is applied and the Security Settings are locked on the printer panel. If the Celiveo Authentication Agent is removed, the settings become available again.



Last modified: 29 September 2022

11.10. Using Microsoft AD LDS software

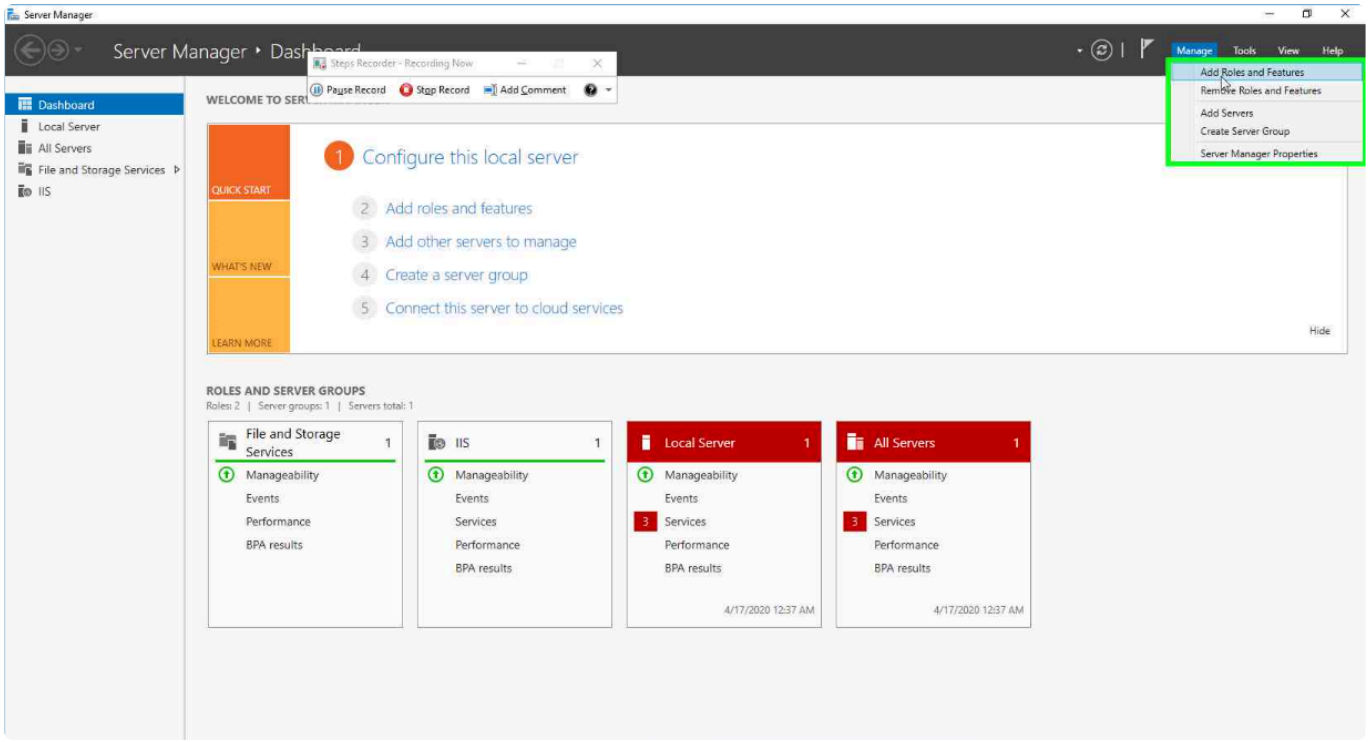
No Active Directory? AD LDS allows to manage easily and professionally users

Some clients do not have Active Directory but need Print Management and a users list is necessary to provide authentication service on printers.
A solution is to use free Microsoft AD LDS software (Active Directory Leightweight Directory Services) to manage users and groups and make them accessible from Celiveo Web Admin and printers.
AD LDS is a scaled-down version of Active Directory, much smaller and simpler to install and use than the full blown version. It runs on PC workstations and Servers OS, can be used standalone and it is even possible to have multiple instances of AD LDS running independently on the same PC or server, they will not interfere with each other. Celiveo supports natively AD LDS users directory in authentication profiles thanks to its AD/LDAP interface.
With AD LDS you benefit from:

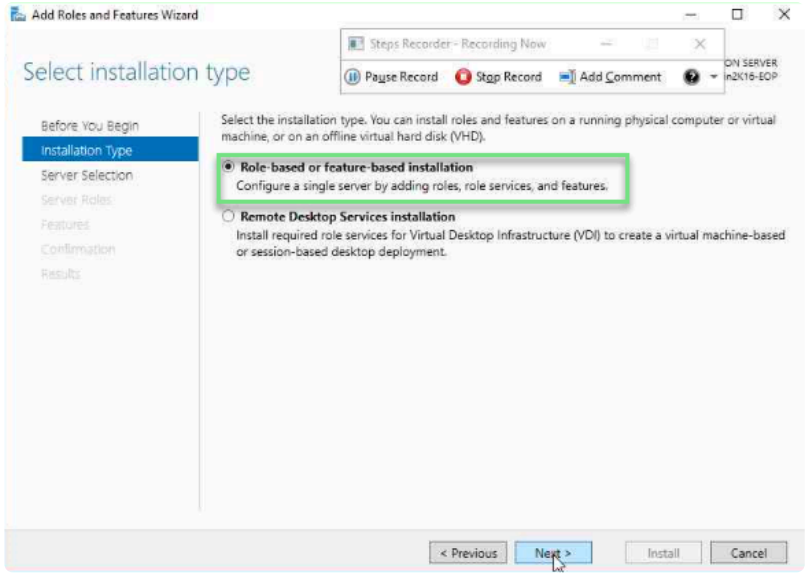
- A Microsoft graphical UI to manage users and groups (ADSI Edit tool present within AD LDS)
- Management through Powershell cmdlets
- The ability put users in groups, used to grant rights on printers/rules
- The ability to import users lists from CSV list into AD LDS. This can be useful if users are coming from a third party system, ie a door management system with card numbers, or a PIN code generation system.
- A fast track to Active Directory and Azure AD the day you want to migrate
  Note that PC login against AD LDS is possible but we don't recommend it, it is best to then use a full blown Active Directory software.
  If you are already familiar with Active Directory, AD LDS has some limitations, detailed in the AD LDS Microsoft page:
  https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732019
  AD LDS can be downloaded from that link:
  https://www.microsoft.com/en-us/download/details.aspx?id=1451
  A lot has already been written on AD LDS, you will find here an excellent article detailing how to install and setup AD LDS on Servers and PCs:
  http://www.rebeladmin.com/2018/02/step-step-guide-setup-active-directory-lightweight-directory-services-ad-lds/

Installing AD LDS

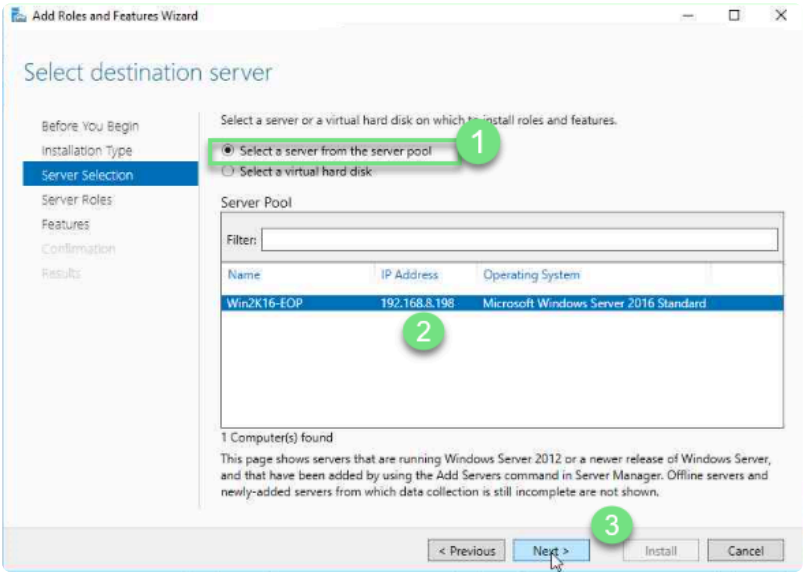
Open Windows Server Manager and click **Manage > Add Roles and Features**.



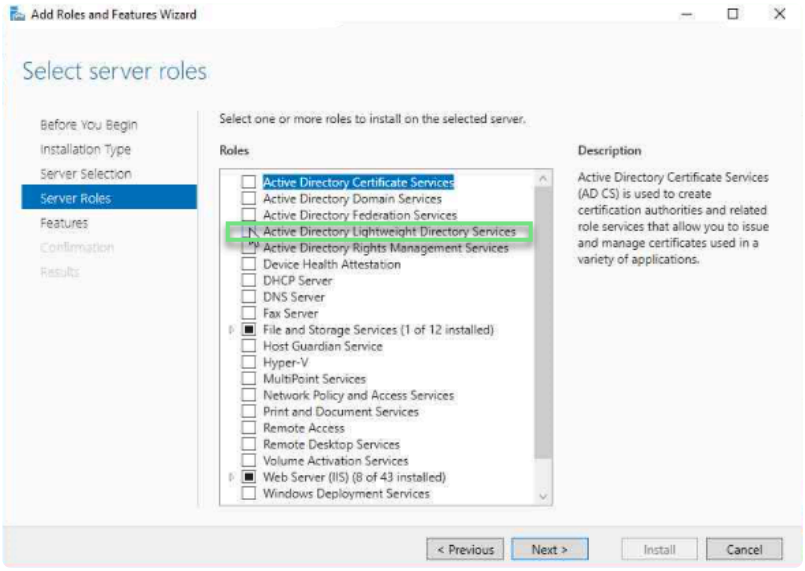
In the **Installation type** section, select **Role-based or feature-based installation** and click **Next**.



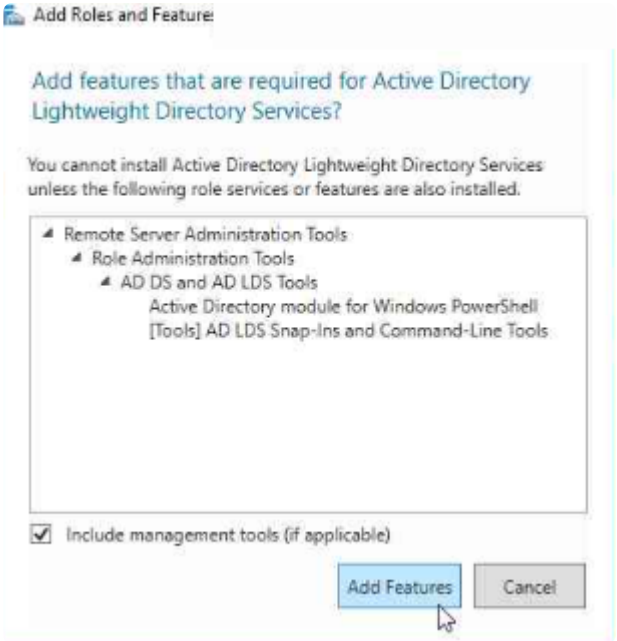
In the **Server Selection** section, click **Select a server from the server pool**, select a server and click **Next**.



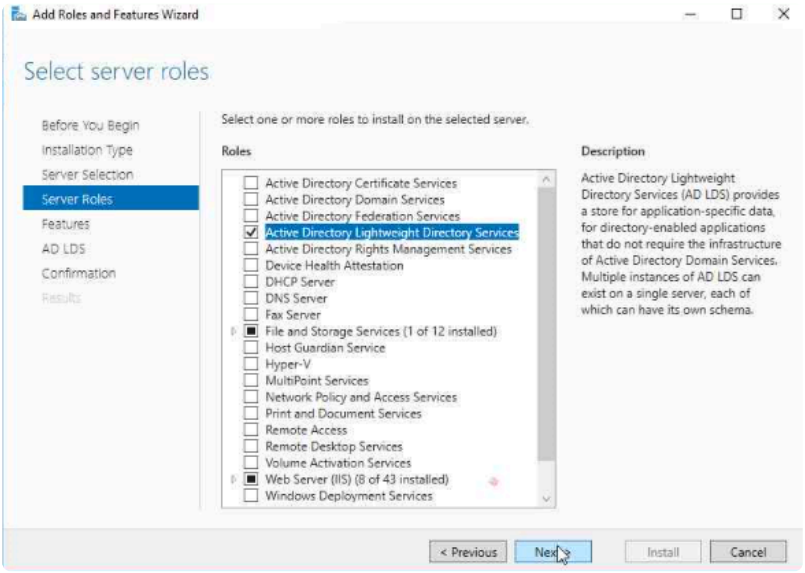
In the **Server Roles** section, select **Active Directory Lightweight Directory Services** from the **Roles** list.



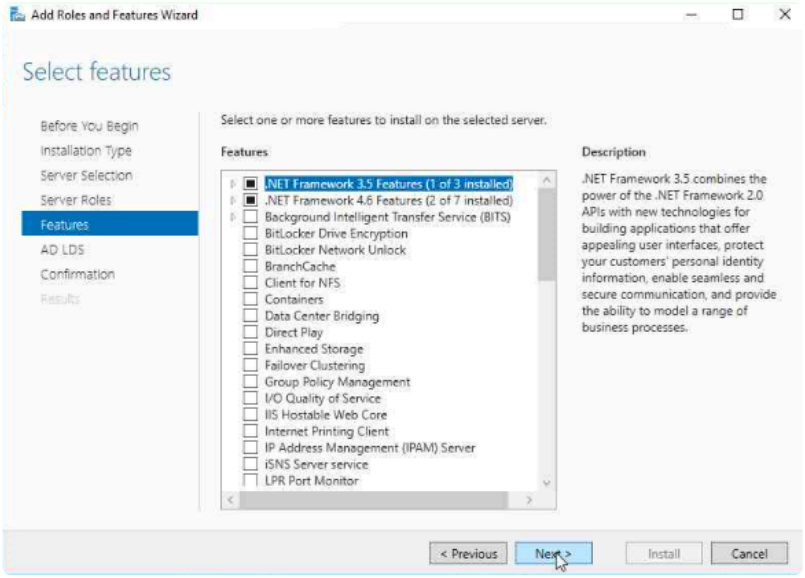
In the **Add Roles and Features** pop-up window, click **Add Features**.



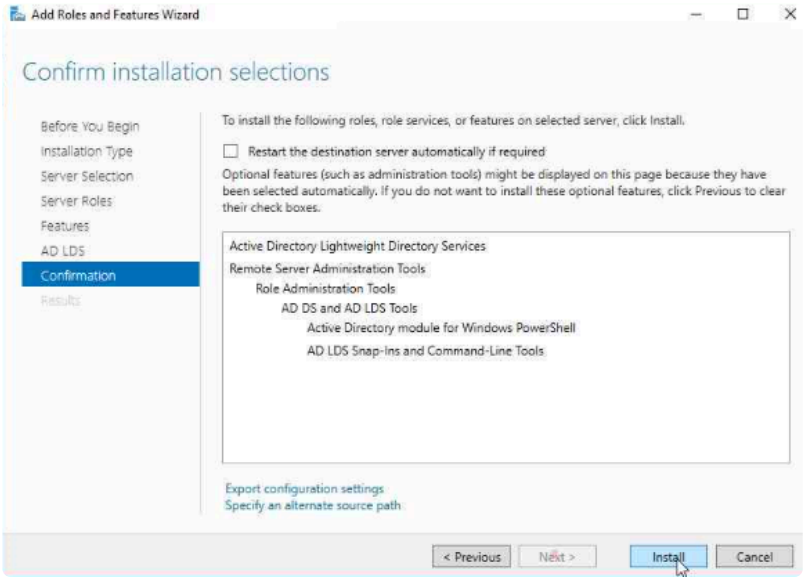
Back to the **Server Roles** section, click **Next**.



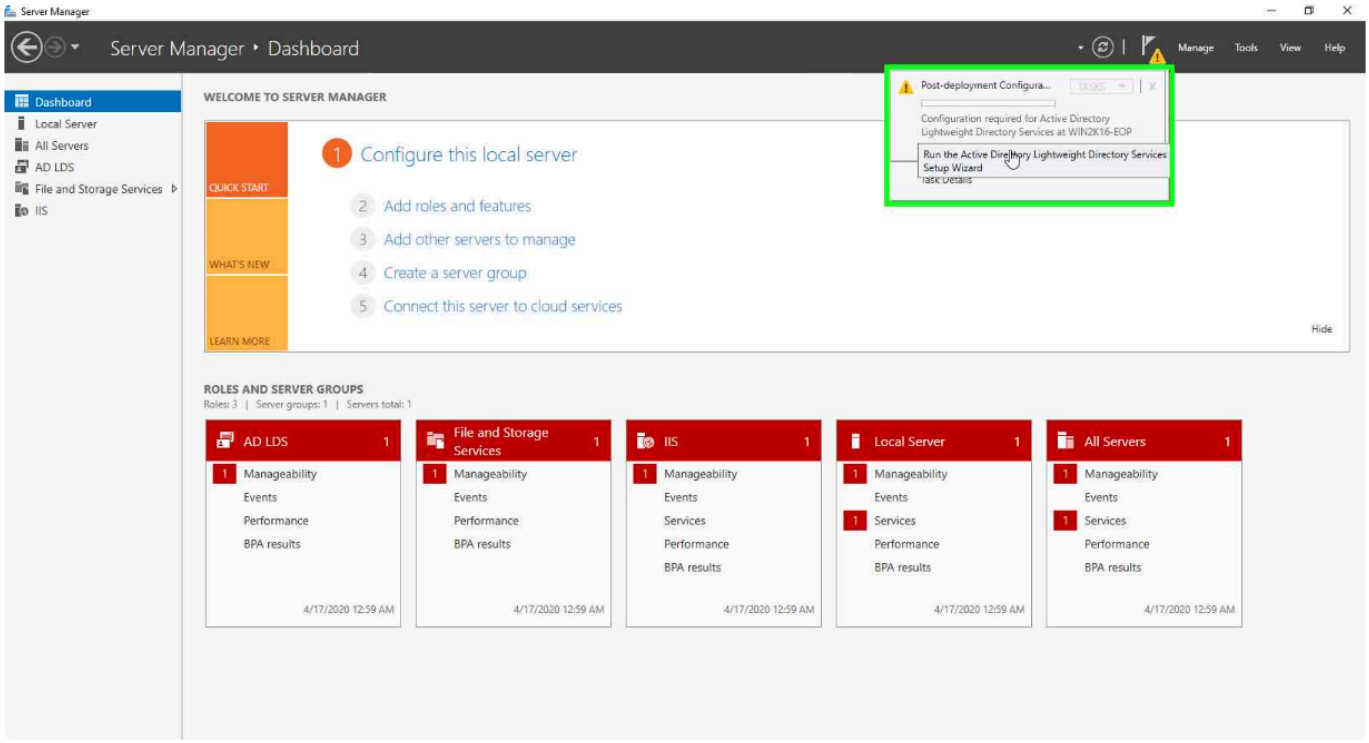
In the **Features** section, select **.NET Framework 3.5 Features** and **.NET Framework 4.6 Features** then click **Next**.



In the **Confirmation** section, click **Install**.

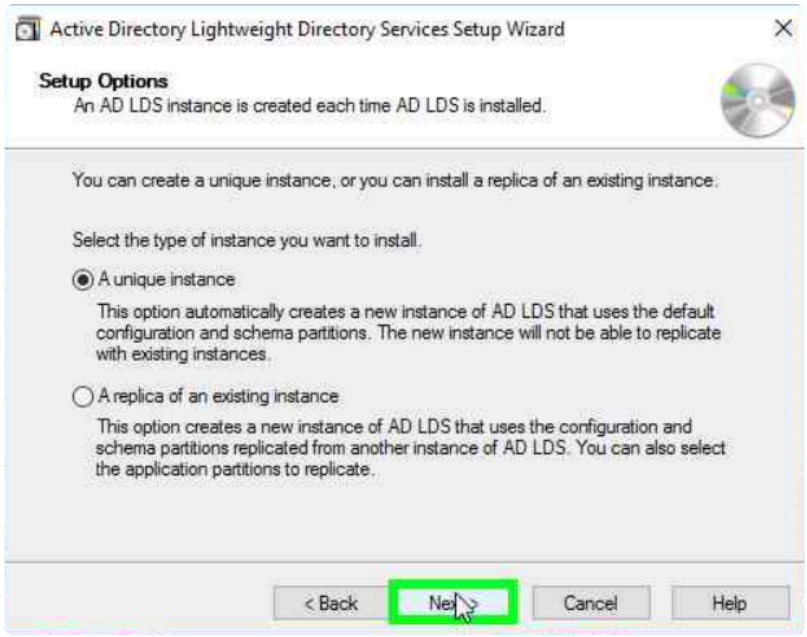


In Windows Server Manager, click the yellow exclamation mark to enter the setup wizard.

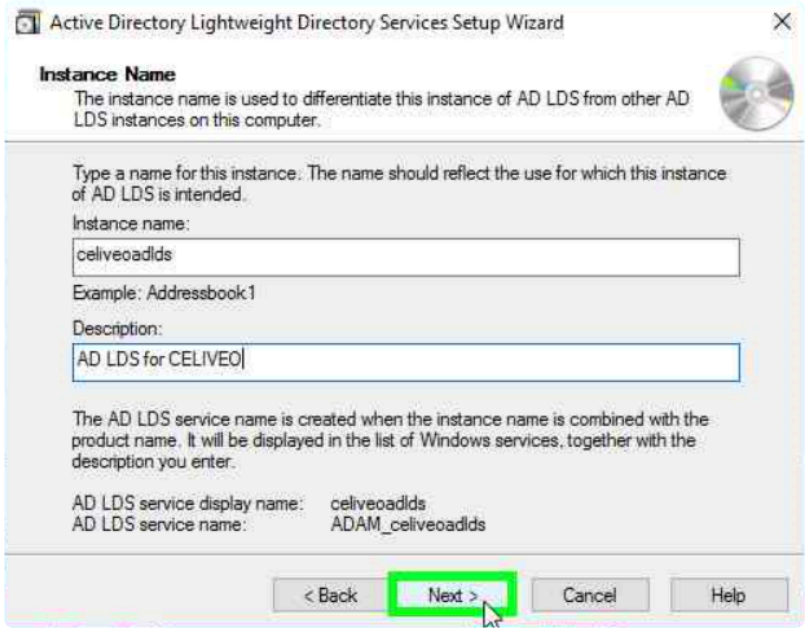


Click **Next**.

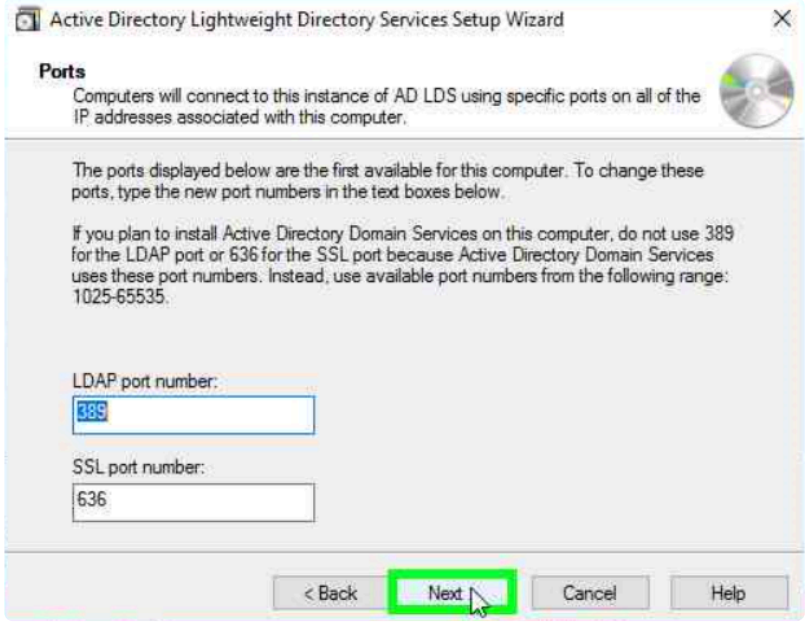
In the **Setup Options**, select **A unique instance**.



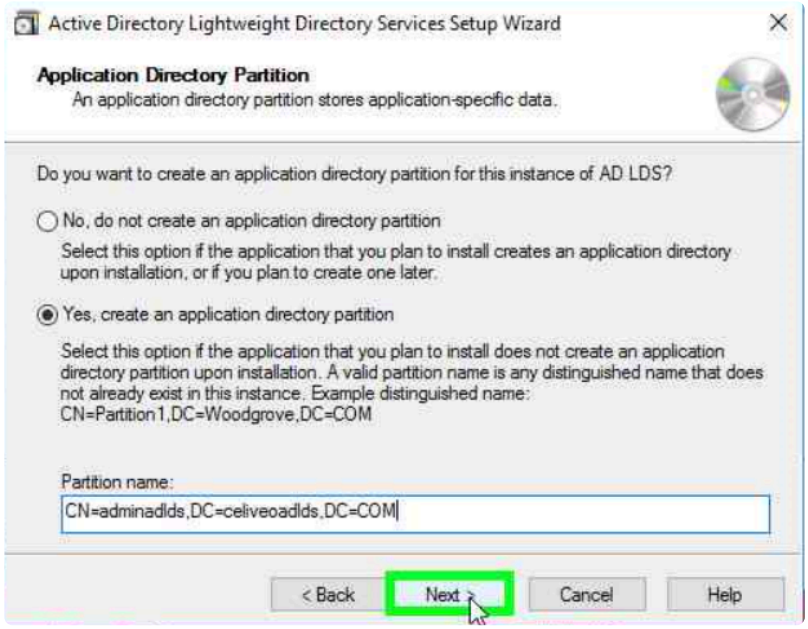
Enter an Instance name and description and click **Next**.



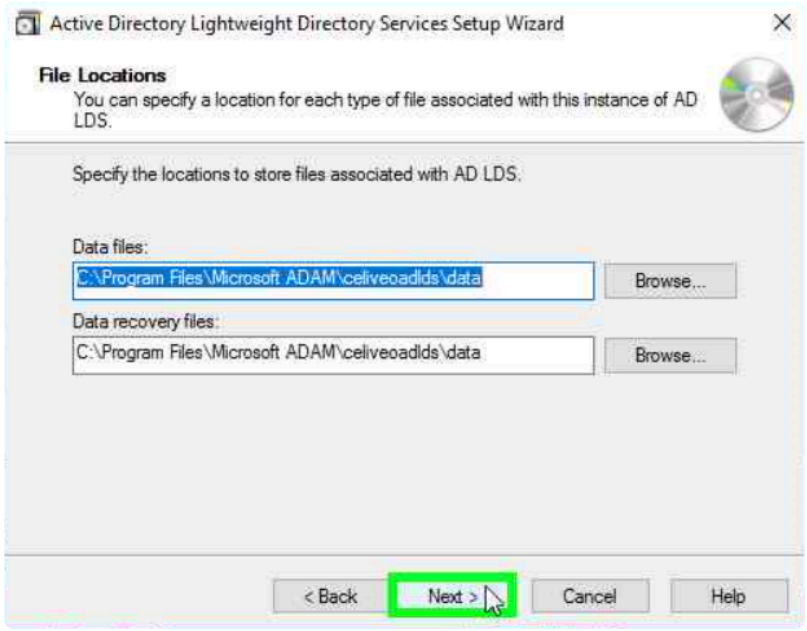
Enter the LDAP and SSL port numbers and click **Next**.



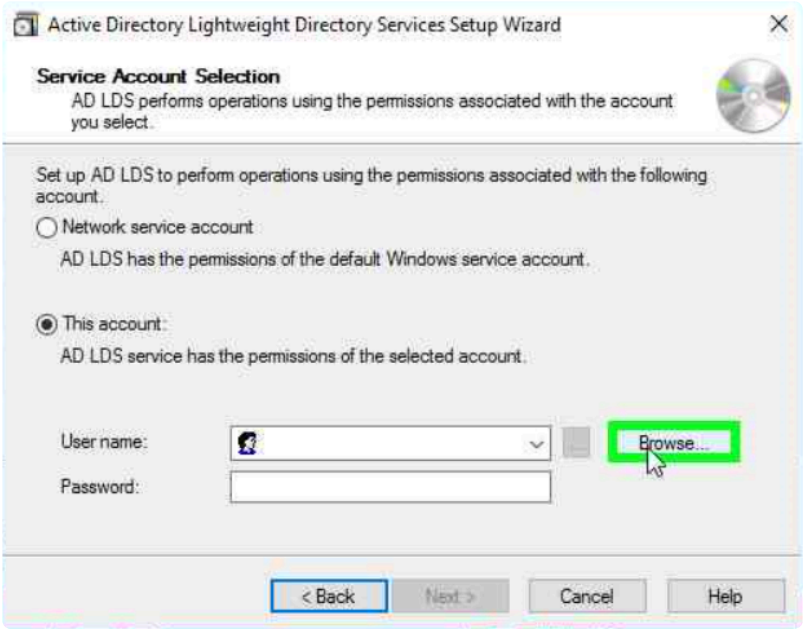
Select **Yes, create an application directory partition**, enter a partition name and click **Next**.



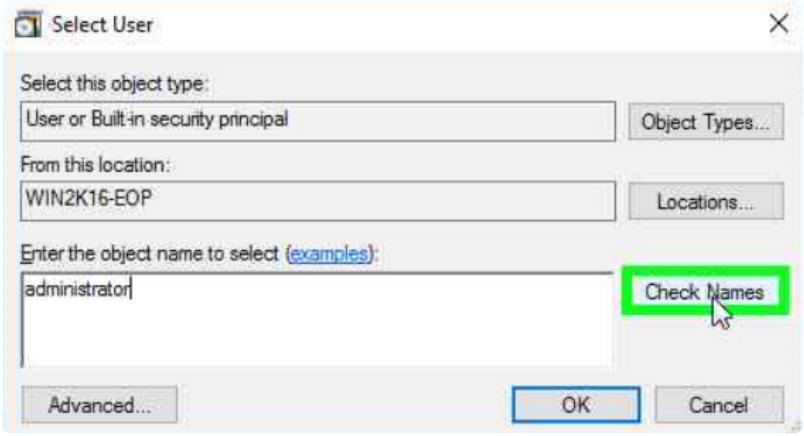
Select the locations to store the files associated with your instance of AD LDS and click **Next**.



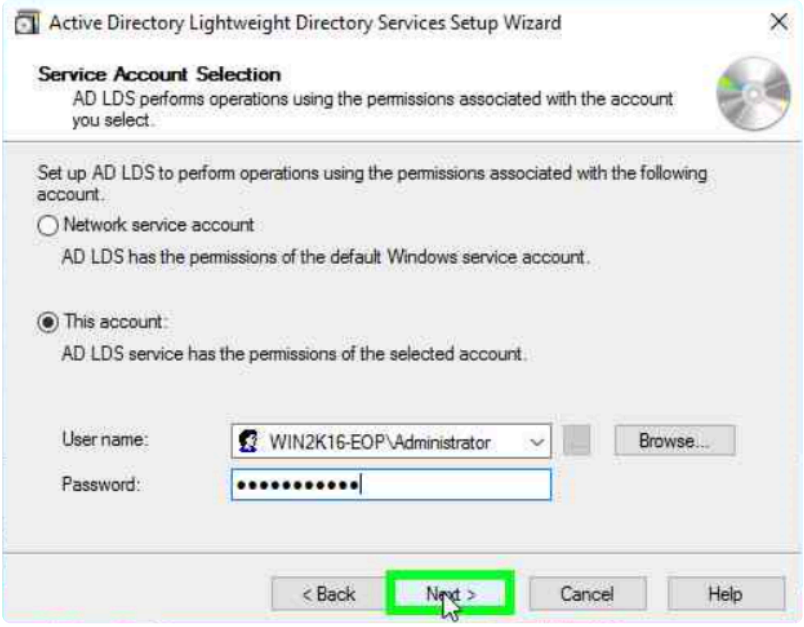
In the **Service Account Selection** window, select **This account**.
Click the **Browse** button to select a user.



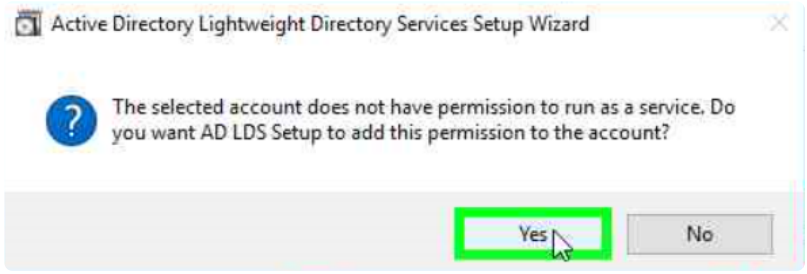
Type a user name in the dedicated field and click **Check Names**. Then click **OK**.



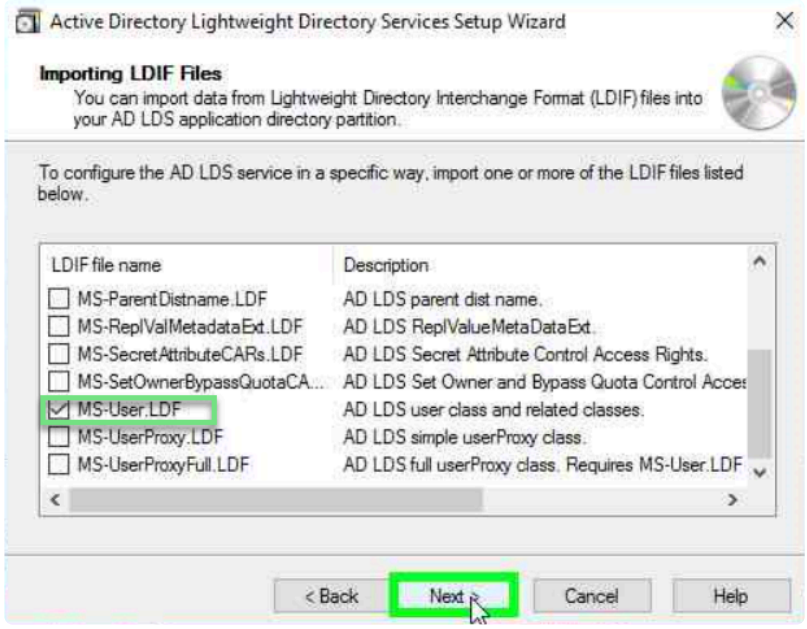
Enter the selected user's password and click **Next**.



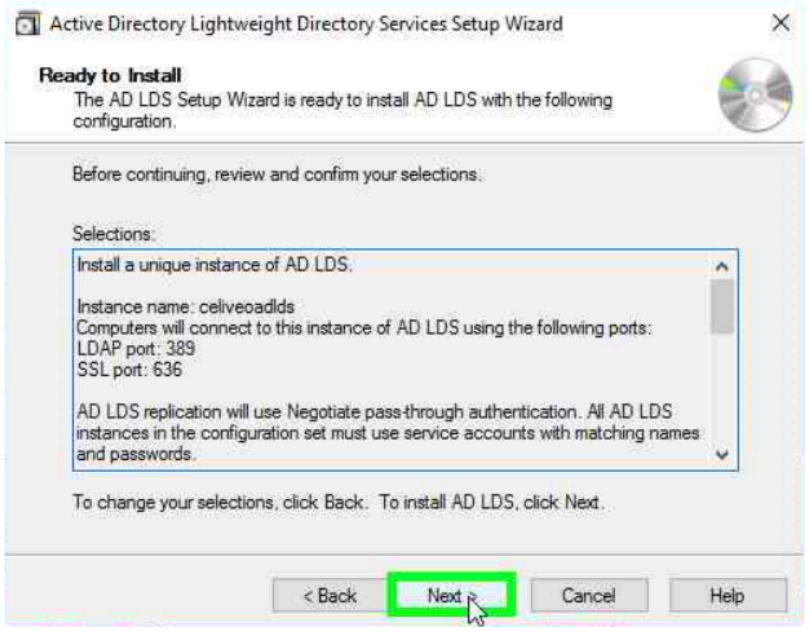
When prompted to add the permission to run as a service to the account, select **Yes**. Then click **Next**.



Select the **MS-User.LDF** file in the LFIF files to import list and click **Next**.



In the **Ready to Install** window, click **Next** to start the installation.



When prompted, click **Finish** to complete the installation.

AD LDS and User Authentication for printers

No sAMAccountName attribute:

sAMAccountName is a legacy AD attribute (logon name that supports old versions of Windows) progressively replaced by the user UPN (userPrincipalName). The Windows Print Spooler still uses the sAMAccountName but you won't find it in AD LDS or in Azure AD. That won't be an issue as with a mouse click you can instruct Celiveo Authentication profile to use the UPN attribute instead of sAMAccountName. Note that the UPN attribute shall then contain the user PC login name, not the real UPN (which contains the domain name), otherwise there will be no match to the user name used by the Windows print spooler when supplying print jobs to Celiveo pull print service.

Indexing the user ID attribute:

When there are a large number of users the lookup for a PIN code or card number is much faster if the attribute (field) that contains it is indexed.
By default Celiveo uses the postOfficeBox attribute to store the user ID (card or PIN) and it is indexed, but any other attribute can be selected.
If you need to index an attribute in Active Directory that article explains how to proceed:
https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995762

Importing/exporting users list with PIN/card ID in/from AD LDS using CSV file

Microsoft provides the free csvde utility to import/export users into AD LDS. That can't import/export password, which are not be necessary when using AD LDS to store a pre-defined list of users and card ID/PIN codes. The documentation for
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc732101

Updating frequently the list of users

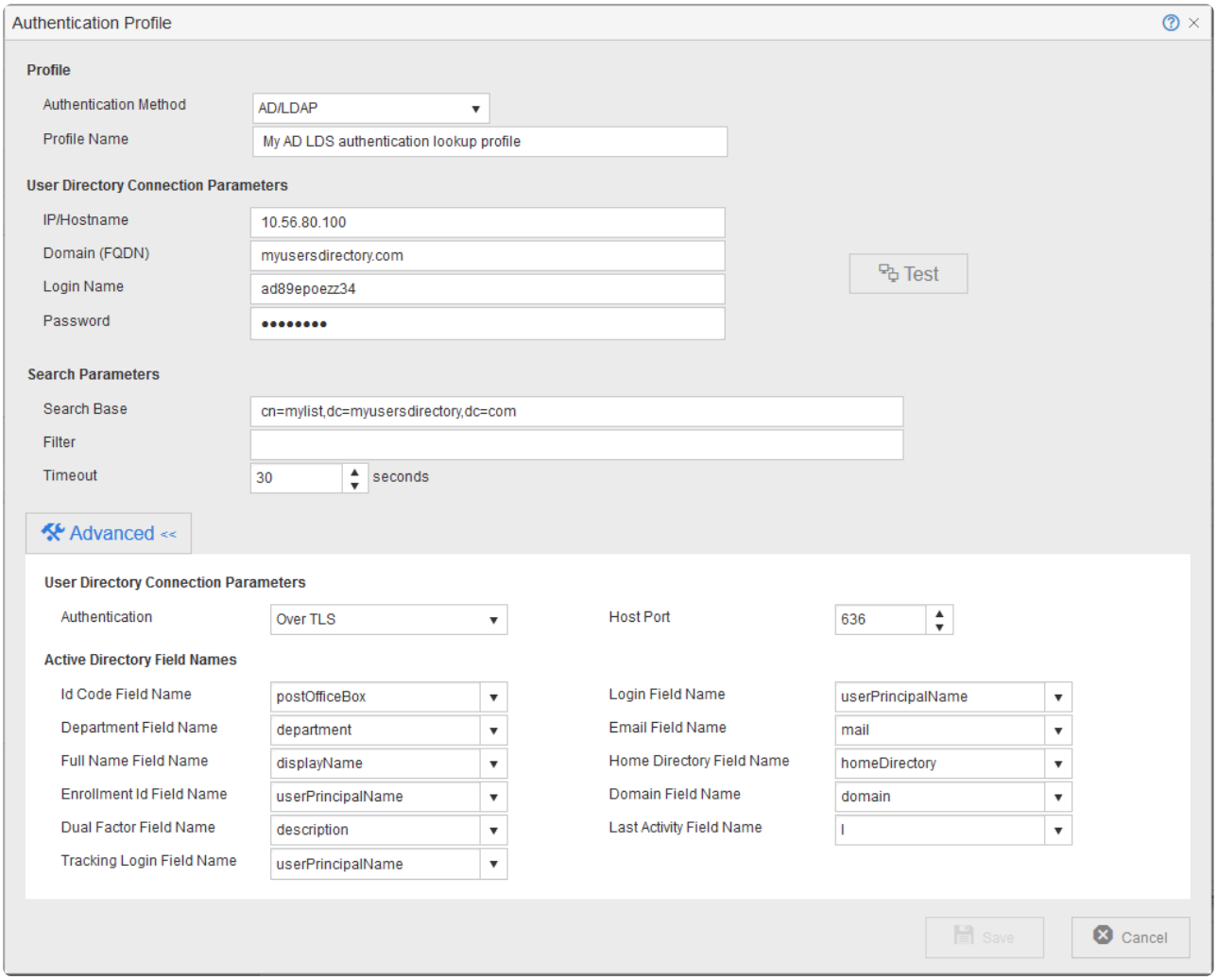
Microsoft warns that “By design AD LDS keeps track on all deleted records though. This lead to the scenario where the database file grew more and more, as all deleted records were not permanently deleted by only flagged as “to be deleted””. The file adamntds.dit grows significantly when a script is run very frequently and performs significant updates. The link below describes the issue and the solution.
https://docs.microsoft.com/en-us/archive/blogs/isablog/the-case-of-the-big-ad-lds-database

Configuring AD LDS for Celiveo Users list

- Create admin accounts to manage the AD LDS system. We recommend you define a complex and long password and use a non-explicit login name.
- Create a service account with read/write access rights, that will be used in the Celiveo Access Control profile to query AD LDS for user IDs and users information. We recommend you define a complex and long password and use a non-explicit login name.

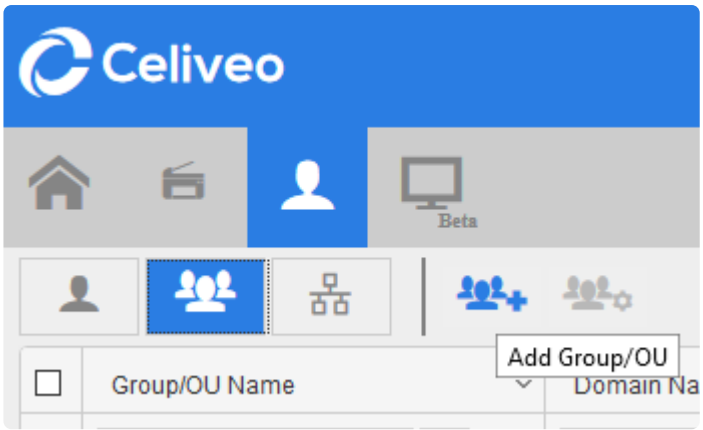
Configuring the Celiveo Authentication profile to connect to the AD LDS instance

- From the physical printer access control button create a PIN code or Card authentication profile.
- Do not activate “Self Enrollment” unless all users have a login/password defined in AD LDS and know it. Otherwise users will not be able to authenticate on MFPs to enroll their card or on the web portal to request a PIN code.
- Create an authentication profile matching the Connection Settings detailed in ADSI Edit tool mentioned above.

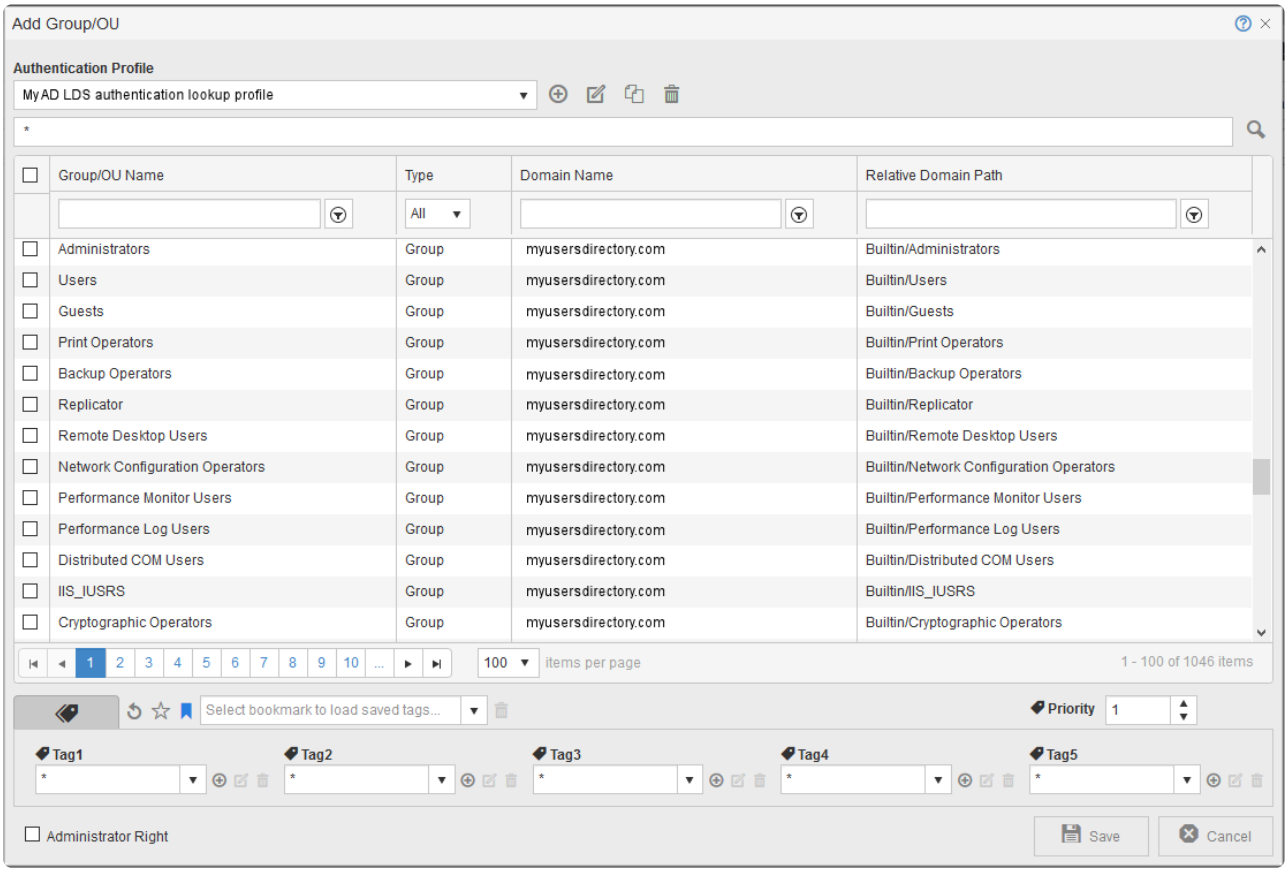


You can see all fields that by default are sAMAccountName have to be changed to *userPrincipalName* since *sAMAccountName* does not exist by default in AD DLS.

- Test the connection to AD LDS using the Test button, you should have successful status. If not, verify the settings and firewall to allow the LDAP host ports inbound and outbound communication.
- Go to the **Users Management** screen as shown below, select the user icon then the group icon then **add Group/OU**.



- Select the Authentication profile created earlier, then enter * below to select all group. If the connection is successful the list of groups shows up.



Adding users and their PIN code or Card number into AD LDS

- **From the UI**: use ADSI Edit to add users manually, enter their PC login name in the userPrincipalName attribute and their PIN or card number in the postOfficeBox attribute.
- **From CSV file**: use the **csvde** utility referenced earlier in that article.

Using the static users list in printer capability

- Some setup require the full list of users inside the printer memory, no connection to the AD LDS. Celiveo in the printer can connect to AD/ADLDS to extract a list of users and card number/PIN codes to authenticate them locally witout connecting to AD/ADLDS. Should a PIN/Card number be unknown the AD/AD LDS is still queried in case that's a new user not yet in the local list. All this is possible using the Full Cache in printer capability, activated in the authentication profile.
- We recommend to narrow the scope of AD extract to not extract the full directory, that will be more efficient and faster.
- Define a time range that's wide enough to not trigger all the extracts at the same time and ensure the PC or server that hosts AD/ADLDS is accessible at that time.

Last modified: 29 September 2022

12. Print Management

This topic will help you understand how the Celiveo solution can be used to manage and control the way documents are printed in your environment.

Printers Overview

Create Print Rules

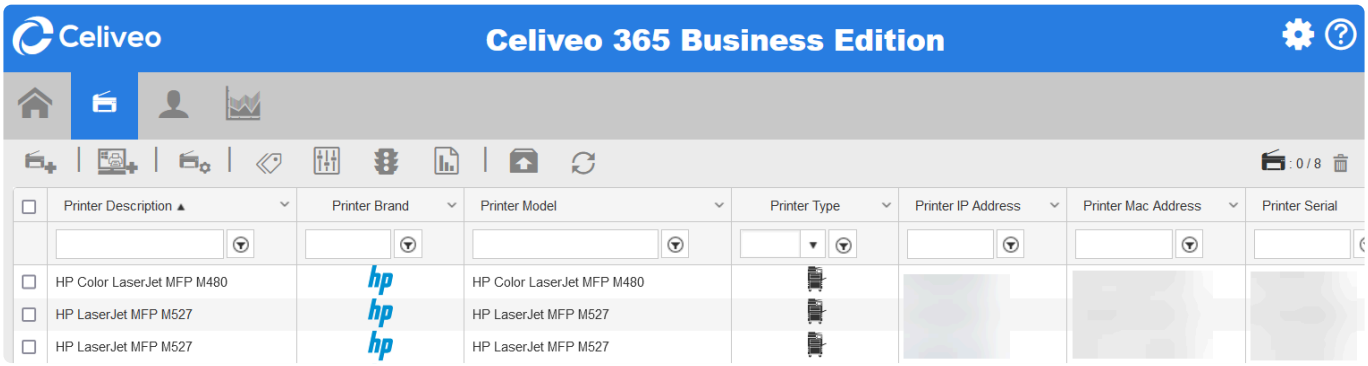
Last modified: 29 September 2022

12.1. Printers Overview

On this page, you can add or delete a printer. Or, simply get an overview of all the printers managed by Celiveo Web Admin. Click on one of the sections for details:

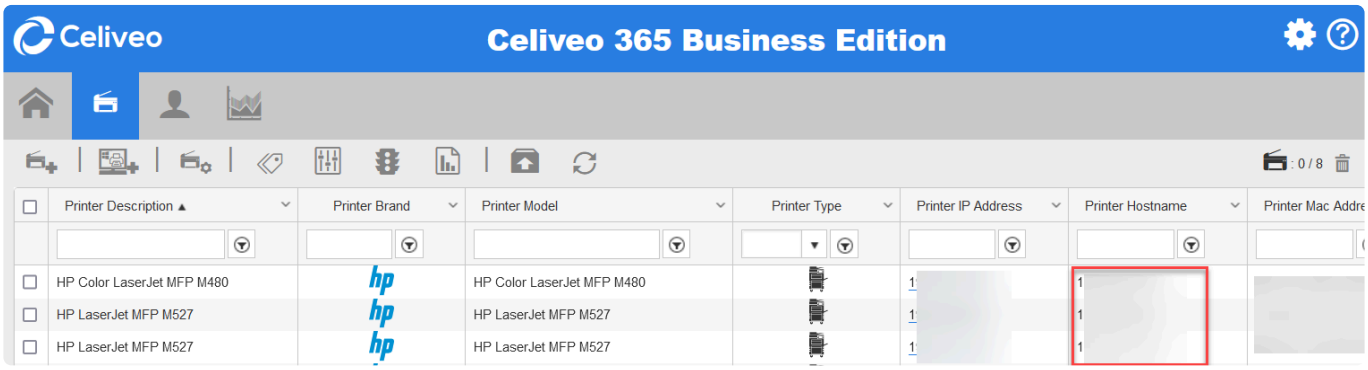
- About the printers list
- Add printers
- Edit printer settings
- Delete a printer

About the printers list



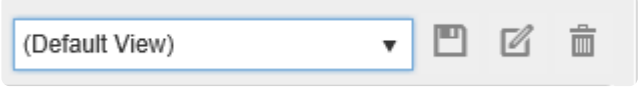
The printer list provides information on each printer added to Celiveo Web Admin. You can adjust the format of the printer list to suit your information needs. Save the order of the columns and access the same view the next time you log in.

> **Note regarding the Printer hostname column**: if the hostname is not resolved, the column will contain the IP address of the printer.



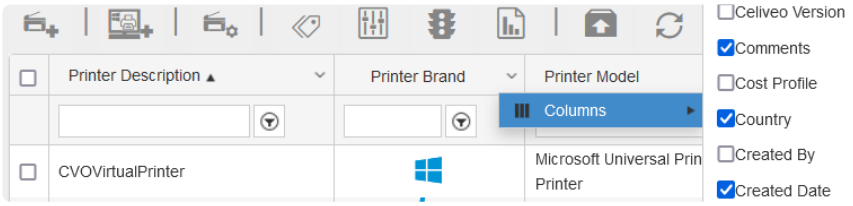
Create a customized printer list

1. On the right hand side of the screen, select the icon.



2. When prompted, enter the name for the customized view and click **[Save]**.
3. Make the adjustments (if required):

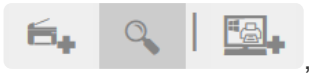
- **To reorder the columns**:
  Click and drag the selected column to the target location. Release to insert the column at the new location.
- **To show or hide a column**:
  Click on the down arrow next to the column label, select **[Columns]**. Check or uncheck the box next to each column header to show/hide.



- **To sort the fields under a column**:
  Click once on the column header, for example **[Printer Brand]**. Click on the column header again to sort in ascending or descending order.
- **To customize the labels of Tags 1 – 5**,
  Click on the icon on the top right corner of the screen. See the Help on Renaming Tags.
- **To search a printer by its printer properties or assigned tags**,
  Enter the required field in the search box under each column header and click Enter.

4. To save the changes, click on the Save icon.
   - **To rename the customized view**,
     Click on the icon.
     When prompted, enter the new name and click **[Save]**.
   - **To delete a customized view**,
     Click on the Delete icon.
     When prompted, click **[OK]**.

Add printers

1. At the Main Menu , click on the Printer icon.
2. At the Add Printer menu  , select one of the following methods to add printers:
   - **Manual**: upload printer information in a CSV file or enter the printer hostname manually.
   - **Discovery Agent**: allow Discovery Agent to automatically search and locate printers in the network.
   - **Virtual Printer**: set up a virtual printer where print jobs can be released to any printer in the network.

Edit printer settings

Under the printer list, select a printer and click on any of the icons on the printer taskbar.

Icon	Menu Option
	Edit printer settings.
	Edit tags and maps.
	Edit the language on the Celiveo menu and authentication screens on the printer.
	Edit access control and printing rules.
	Edit cost definition for the printer.
	For **Physical Printers**: Sync the selected printer again. For **Virtual Printers**: Download the MSI configuration file again.

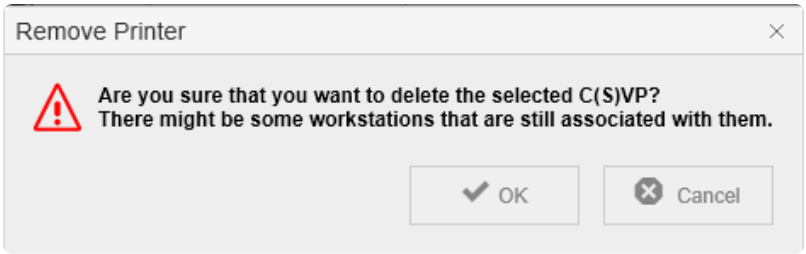
Edit printer description

You can change the description of any physical printer. As you move the cursor over a printer description that can be changed, the cursor changes to an edit icon ( ).

1. Double-click the printer description to change. The Edit Printer screen displays.
2. At **[Printer Description]**, specify the new description.
3. Click **[Save]**.

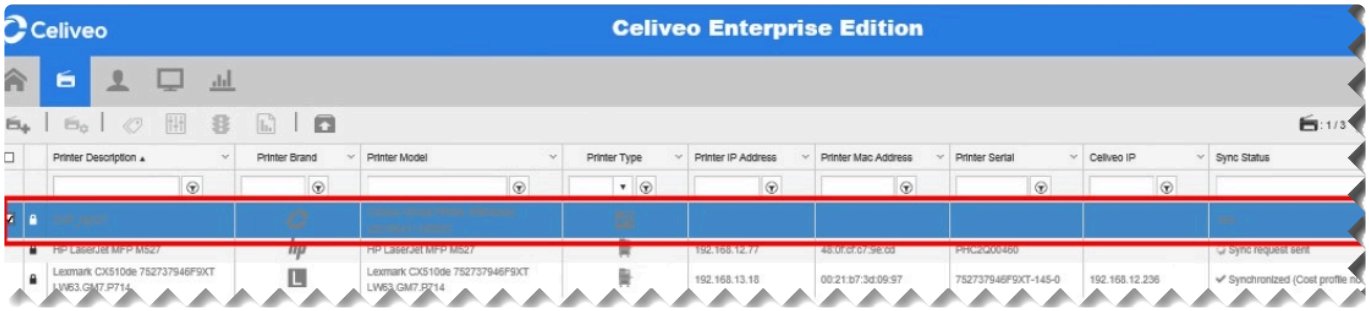
Delete a printer

1. Under the printer list, select a printer and click on the [Delete] icon.
2. When prompted, click **[OK]**.
3. When deleting a virtual printer (CVP/ CSVP), make sure there are no workstations associated to it. A prompt is displayed to confirm this action.



4. Click **[OK]**.

Note: A Sub Admin user (with lesser access privileges than a Super Admin user) cannot delete printer(s), created by a Super Admin user. The corresponding rows will be locked/ disabled for the Sub Admin user.



Last modified: 29 September 2022

12.2. Create Print Rules

PD B E

Print Rules let you define the availability of a printer and how a print job should be handled, depending on:

- The day of week/time of day.
- Who the sender is
- The value of an attribute of the print job (For example, the page count of a print job)

Notes:

- For Print Direct, you create Print Rules on a Celiveo Virtual Printer. The Celiveo Virtual Printer is a module you deploy on a user's workstation, in order to capture print jobs.
- For Pull Printing, if you want to apply a print rule universally for all printers, you place the rule on a Celiveo Virtual Printer. If you want to apply a rule to a specific printer only, you place the rule on that printer.
- Make sure that the maximum job file name size sent to a physical printer is 35 characters and 95 for a job sent to a virtual printer.
- **IMPORTANT**: Rules for a Celiveo Shared Virtual Printer must not have **USER OU** as a criteria.

Let's create print rules for the following examples:

1. Example 1 – Force behavior
2. Example 2 – Control printer availability
3. Example 3 – Override restrictions
4. Example 4 – Deactivation of Print queues drivers based on group and settings
5. Example 5 – Restrict Direct Printing to groups

Example 1:

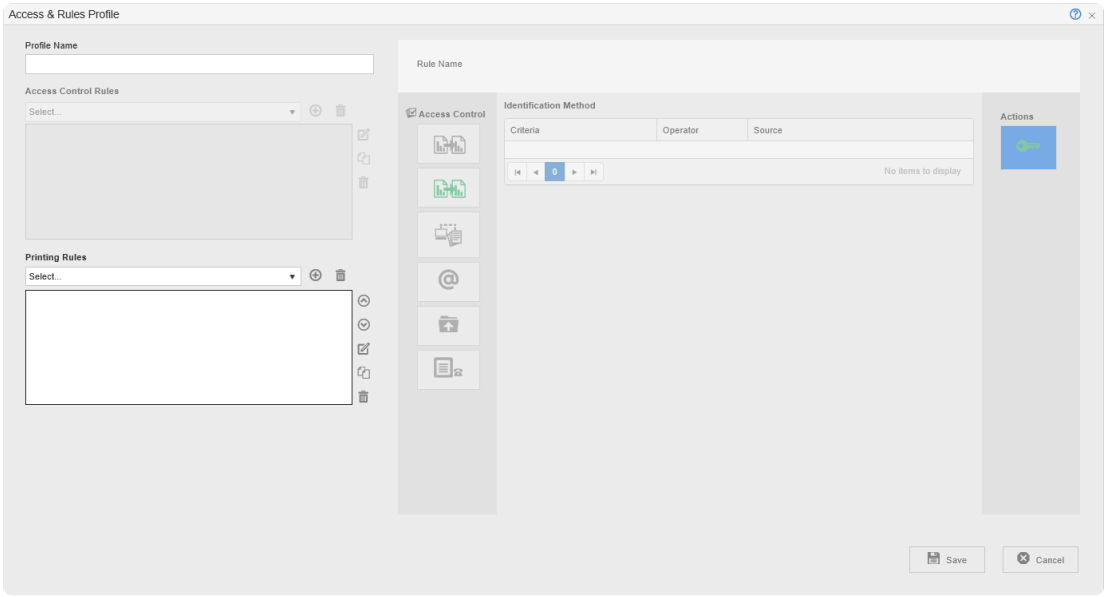
Force color print jobs to be converted to grayscale, if the page count is larger than 10 pages.

Stage 1: Select Printer

1. At the Main menu, click . The Printers List is displayed.
2. Select a Celiveo Virtual Printer you want to apply the rule to, and click . Access & Rules is displayed.

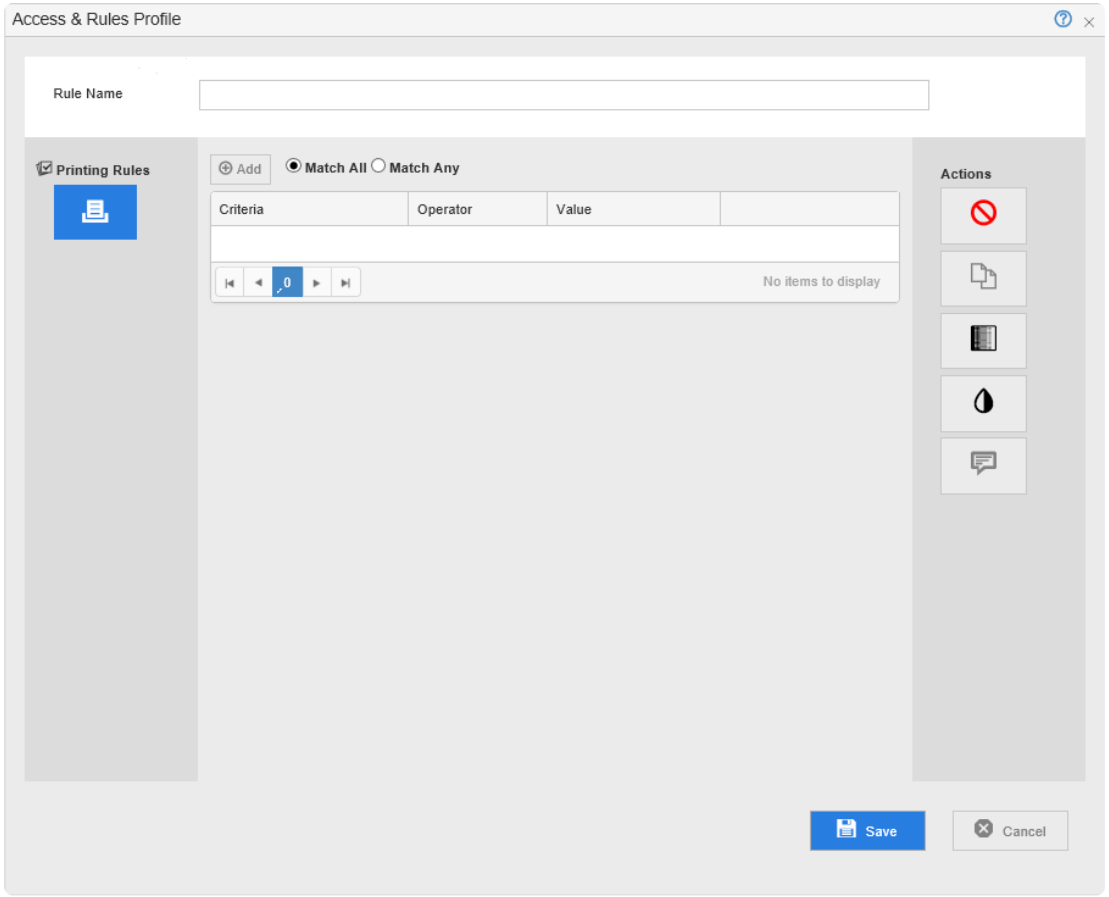
Stage 2: Create a New Access & Rules Profile

1. Click . The Access & Rules Profile for the new rule is displayed.

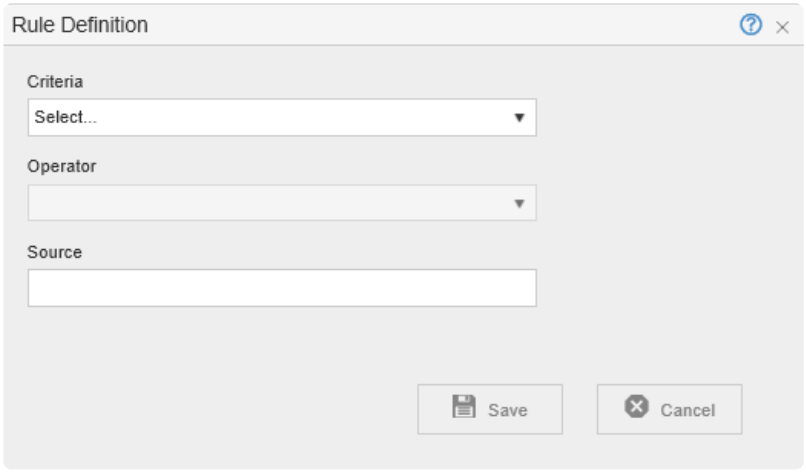


2. At **[Profile Name]** box, specify a unique name (for this example, we will use *Rules for Color Printing* as the name) for the Access & Rules Profile.
3. Click ⊕, located next to the **[Printing Rules]** drop-down, to add a new rule.

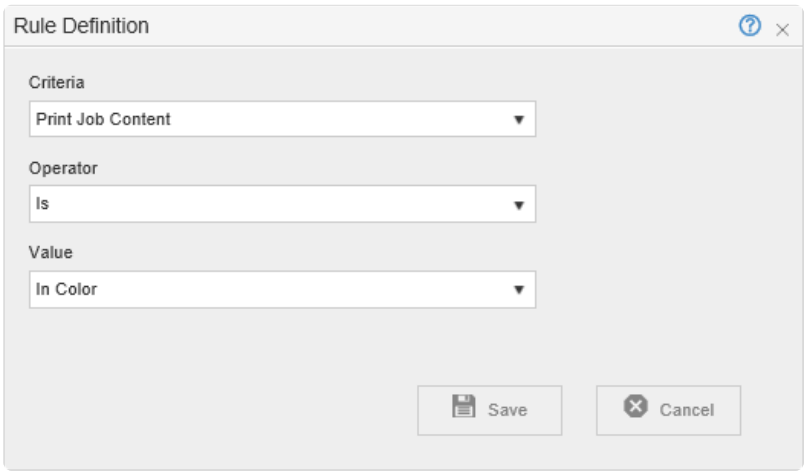
Stage 3: Configure the New Rule



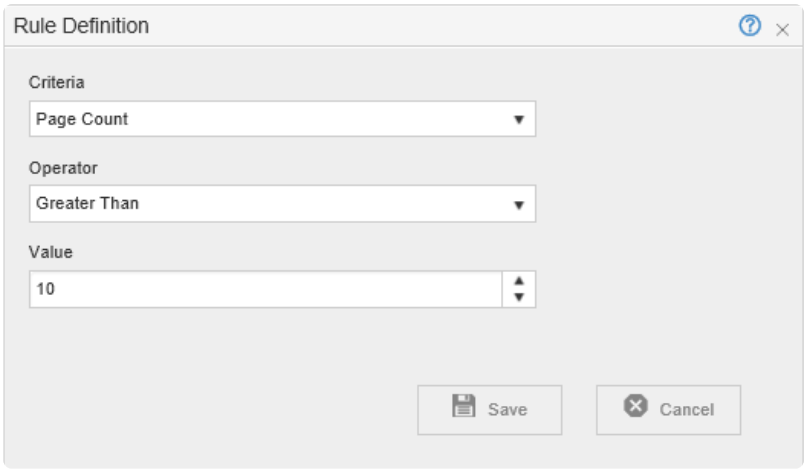
1. At **[Rule Name]**, specify a unique name for the rule (for the purpose of this example we will use *Large color jobs* as the name).
2. Click ⊕, located next to **[Add]**. The Rule Definition displays.



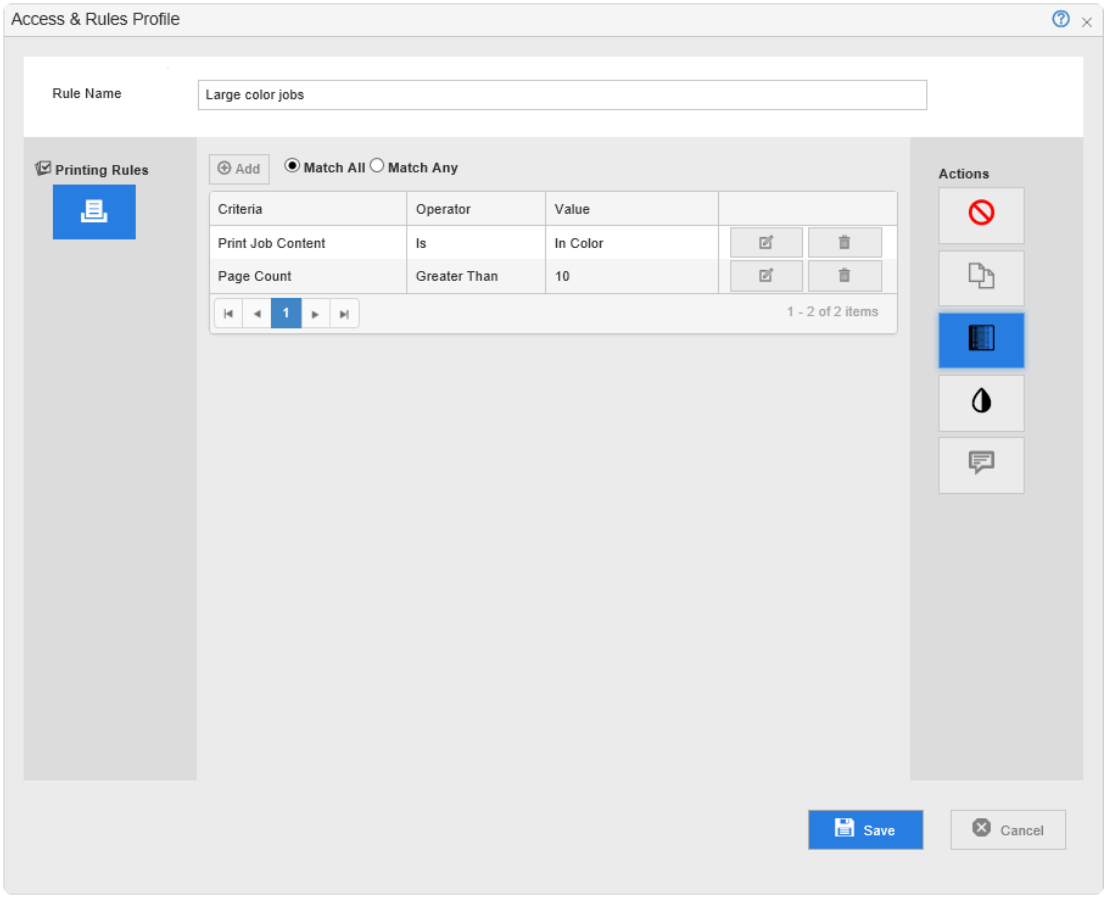
3. From the drop-down lists in the Rule Definition, select options as shown below and click **[Save]**.



4. Once again click ⊕, located next to **[Add]**. The Rule Definition displays.
5. Specify options as below and click **[Save]**.



6. In the **[Actions]** panel, click . The Access and Rules profile should now resemble the illustration below:



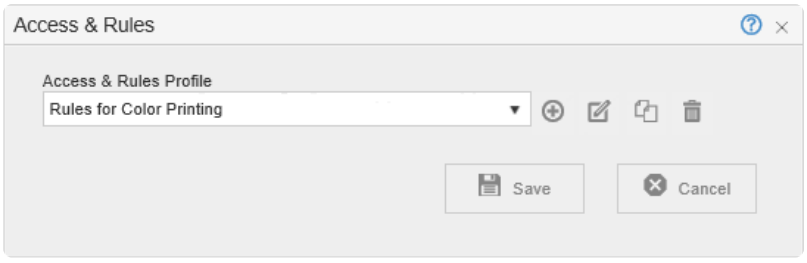
7. Click **[Save]**. Large color jobs rule is now listed under **[Printing Rules]**.

Example 2:

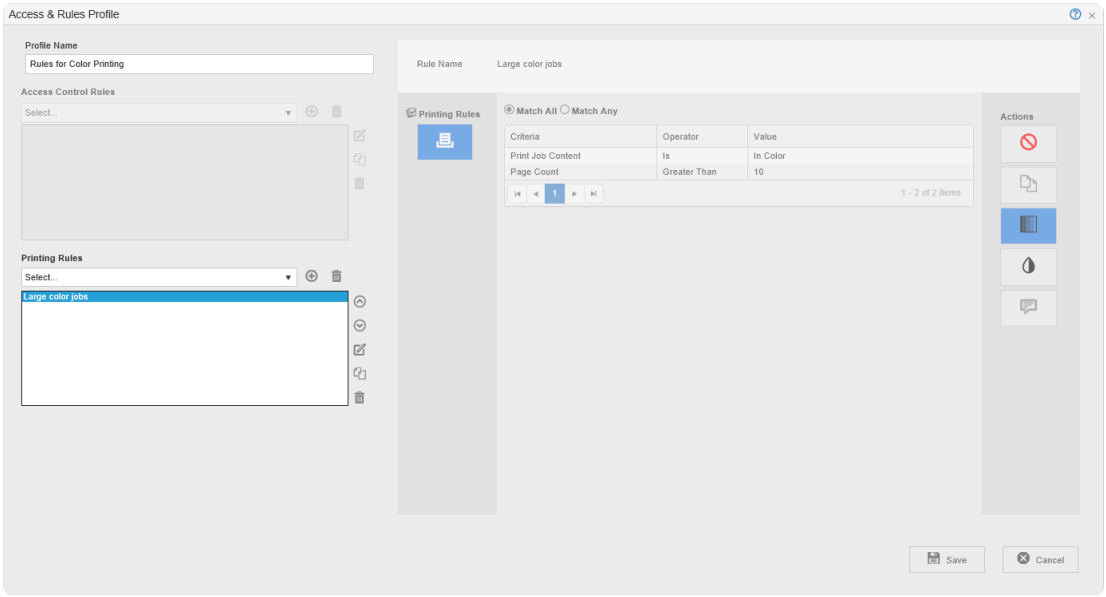
Make Printing unavailable outside regular office hours (8.30 AM and 7.30 PM). Notify users if they attempt to print.

Stage 1: Load Access & Rules Profile

1. From the Printer List, select the printer you modified in the last example and click . Access & Rules is displayed.



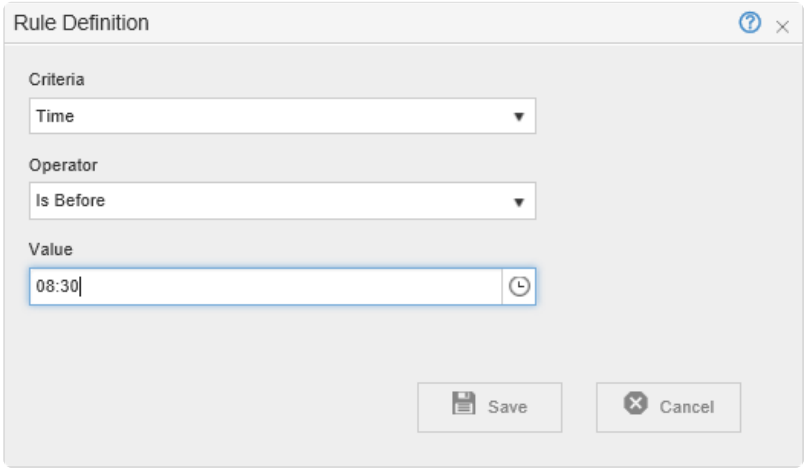
2. Click . The Access & Rules Profile displays.

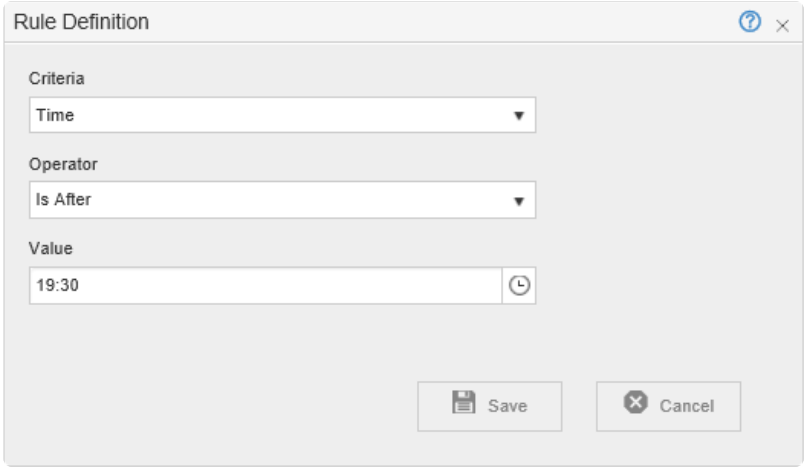


3. Click ⊕, located next to the [Printing Rules] drop-down, to add a new rule.

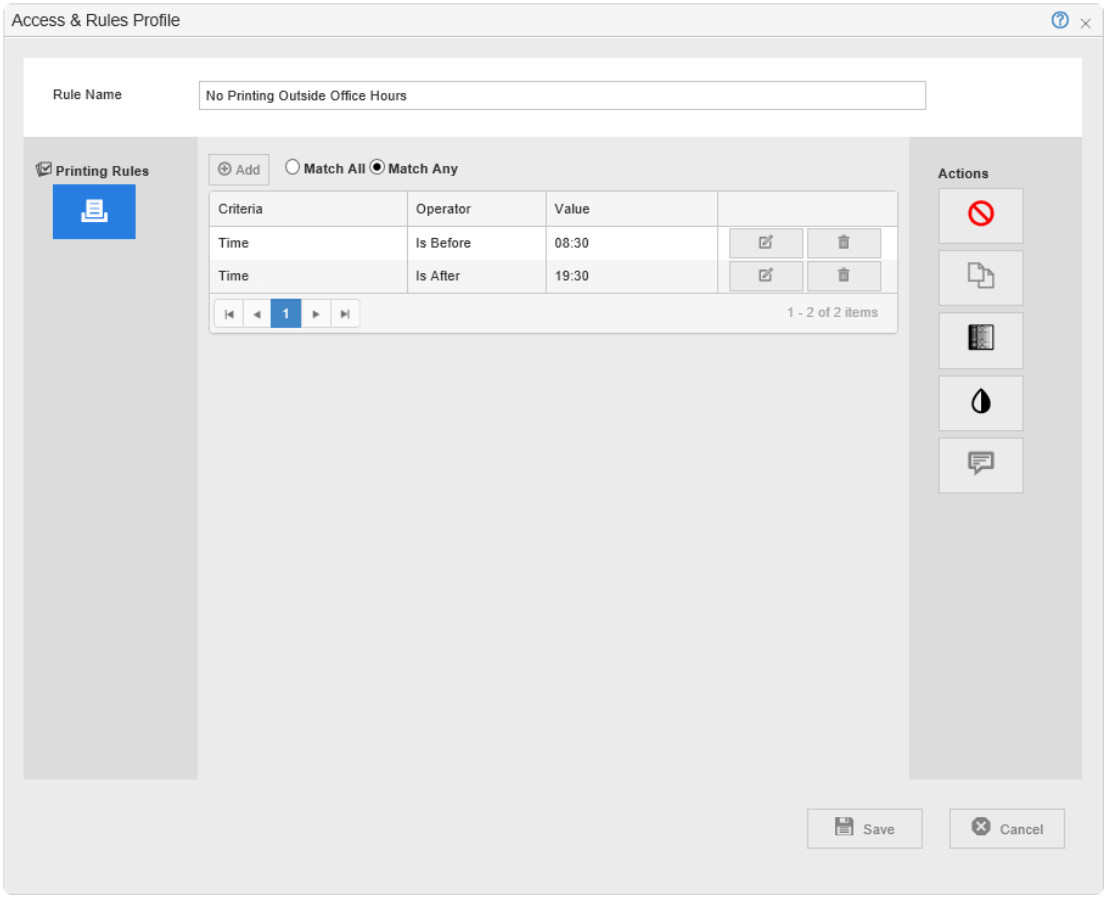
Stage 2: Configure the New Rule

1. At **[Rule Name]**, specify a unique name for the rule (for the purpose of this example we will use *No Printing Outside Office Hours* as the name).
2. Follow the workflow outlined in stage 3 of example 1 to create the two criteria shown below.

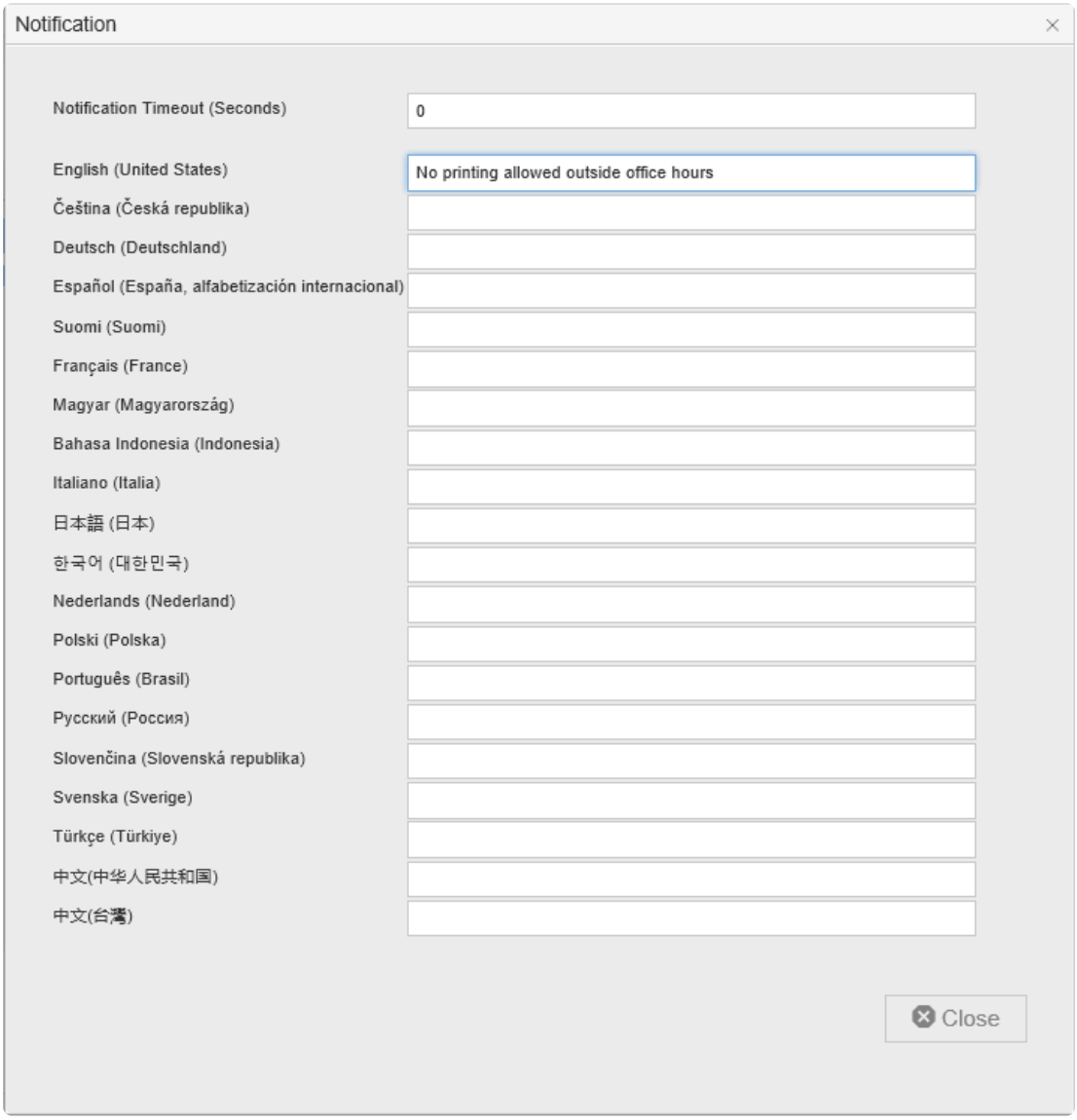




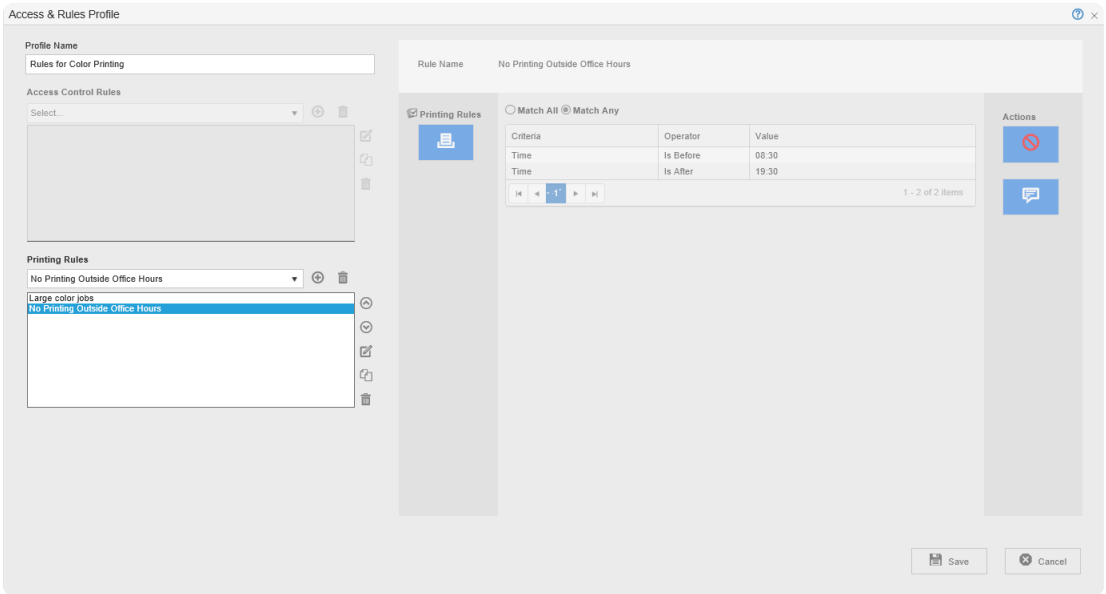
3. Select **[Match Any]**.



4. Click .
5. Click . The icon appears next to the button.
6. Click . and specify the notification as shown below:



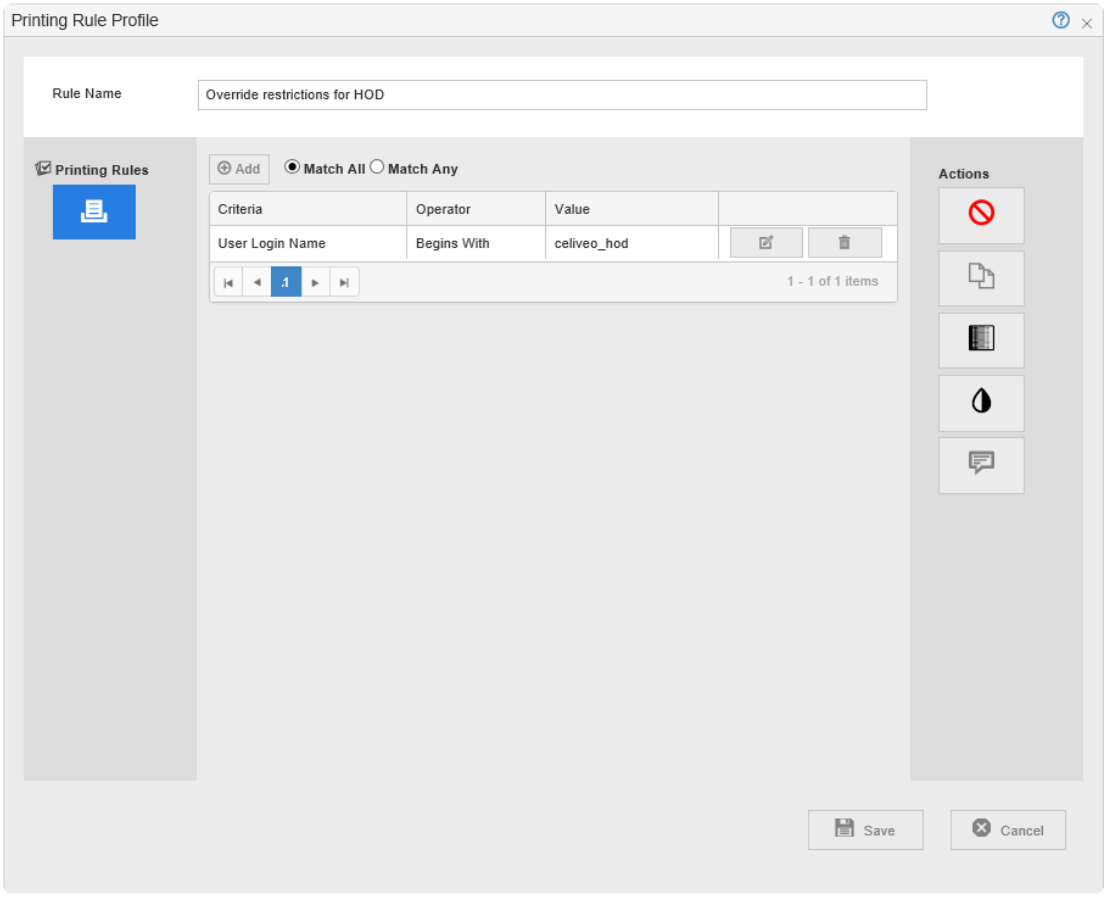
7. Click **[Close]**.
8. Click **[Save]**. The screen should now look like this:



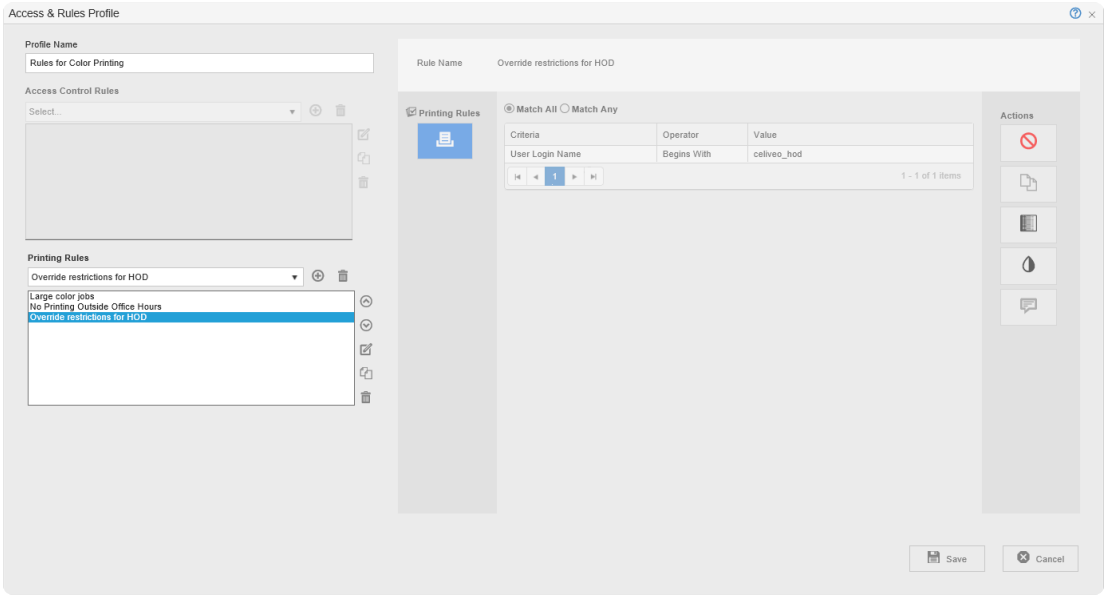
Example 3:

Remove all restrictions for head of department.

1. Follow the procedure outlined in example 2 and create a new rule as shown in the image below:



2. Click **[Save]**. You are returned to the Access and Rule Profile.



3. Click to ensure that the Override Restrictions for HOD rule is placed as the first rule.

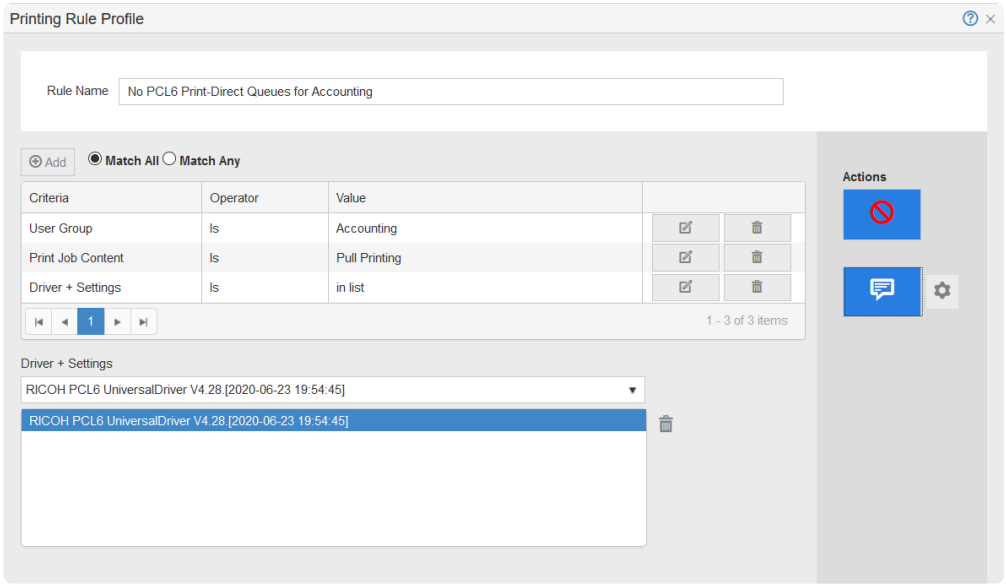
Note: The first rule is processed before all others. Because the rule triggered by the user name that

begins with Celiveo_hod is processed first, that user has unrestricted access. Hence, the subsequent rules do not apply to that user.

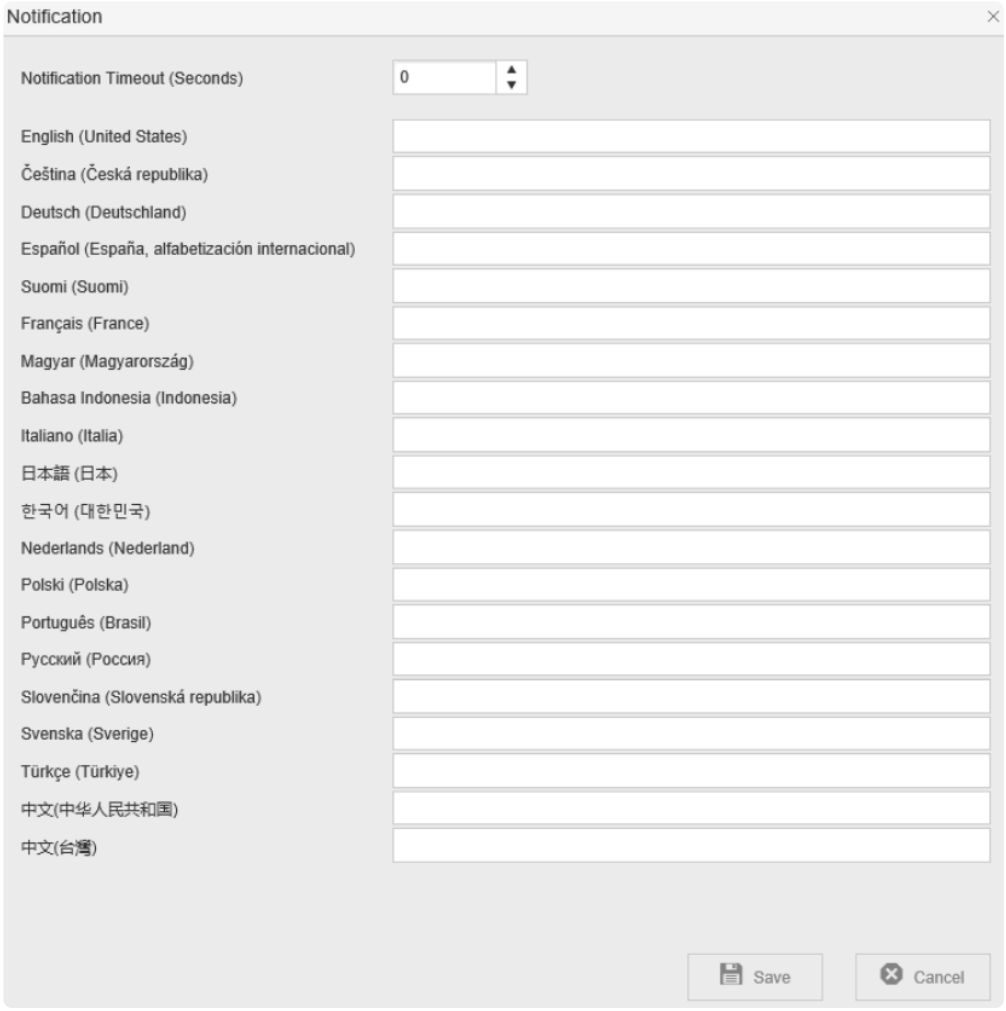
Example 4:

A print rule allows defining which ones of the virtual print queue default driver + settings are forbidden. When the rule applies (at login time and when the network connection is reset for VPN) the settings rule is computed and defines what drivers are available.
As an example, here we want to prevent people belonging to the “Accounting” group to print from Print-Direct queues with a PCL6 driver.

1. Create a rule condition for which:
   Criteria is: **User Group**
   Operator is: **Is**
   Value is: **Accounting**
2. Create a second rule condition for which:
   Criteria is: **Print Job Content**
   Operator is: **Is**
   Value is: **Print-Direct**
3. Create a third rule condition for which:
   Criteria is: **Driver + Settings**
   Operator is: **Is**
   Value is: **In List**
4. Select the driver(s) in the drop-down menu so that it appears in the list.



5. Enable the **Stop** button.
6. Enable the **Notifications** button
7. Click the **Notifications Settings** button to define the notification message displayed to the user when he tries to select a Print-Direct queue. Messages can be defined in 20 languages.

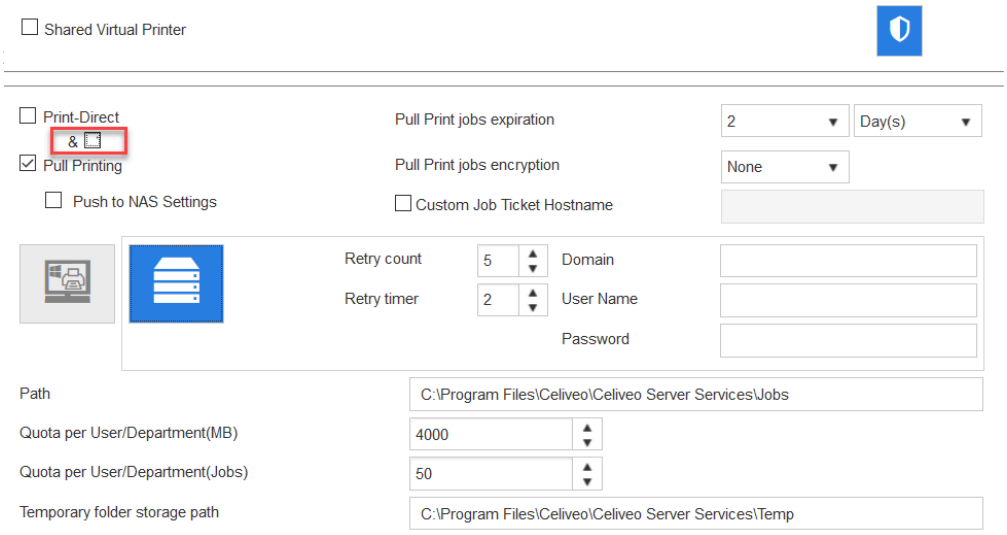


Example 5:

Celiveo Direct Printing will only be authorized if the user is in a group or Organizational Unit or has specific login (Client-Based Printing).

Define the printing methods available

In the Web Admin, the Celiveo Virtual Printer has a new setting to define if Print-Direct and Pull Printing can be used at the same time.
OR – “&” checkbox disabled: if Print Direct is activated, Pull Printing is deactivated, and the other way around.
AND – “&” checkbox enabled: Pull Printing and Print-Direct can be activated/deactivated independently and be available in parallel.



Assign Print Queues Rights using Print Rules

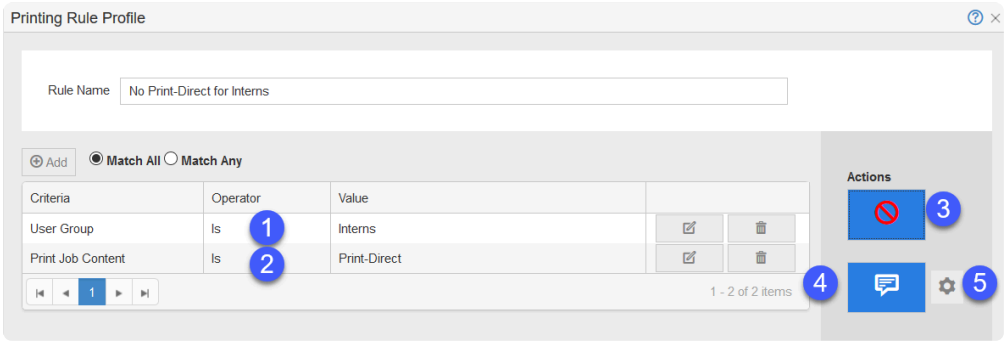
1. Select a printer and click the Access & Rules button.
2. Under Printing Rules, click + Add.
3. In the Rules Definition Window, select your criteria.

Understanding Criteria and the different possibilities

You can restrict or authorize different actions using criteria, operators, and values.

For example, to prevent users from a specific group to see a Print-Direct queue:

1. Create a first rule condition for which:
   Criteria is: **User group**
   Operator is: **Is**
   Value is: **[Name of the User group]**
2. Create a second rule condition for which:
   Criteria is: **Print Job Content**
   Operator is: **Is**
   Value is: **Print-Direct**



3. Enable the **Stop** button.
4. Enable the **Notifications** button
5. Click the **Notifications Settings** button to define the notification message displayed to the user when he tries to select a Print-Direct queue. Messages can be defined in 20 languages. You can also add the following variables to the notification messages:

Variable	Description

%JOBNAME%	Displays the job name.
%JOBSIZE%	Displays the print job size in MB (includes “MB”)
%USERNAME%	Displays the sAMAccountName.
%USERSNAME%	Displays the user’s name.
%COST%	Displays the total print cost with rules applied.
%BWCOST%	Displays the cost with Black and White printing applied.
%DUPLEXCOST%	Displays the cost with Duplex printing applied.
%TONERSAVINGCOST%	Displays the cost with toner saving applied.
%PRECOST%	Displays the cost before applying the rules.
%TOTALPAGES%	Displays the total number of pages.
%MONOPAGES%	Displays the total number of pages in black and white (Mono).
%COLORPAGES%	Displays the total number of pages in color.

Important information

The CVP rules and Printer print rules are complementary and do not replace one another.
CVP rules act and inform the user at the PC level, the admin-defined message (optional) shows up immediately in a popup window to inform the user the job has been canceled as it breaks the rules.
Printer print rules are run at the printer level and will inform the user (if a message is defined) on the jobs list (job list in color when the printer technology allows it, plus admin-defined message in job details).

Example:

You can define the corporate rules in the CVP:

- Printout from Outlook shall be duplex, toner saving, b&w
- Jobs with CONFIDENTIAL in title shall be stopped
- Any print job that may cost more than 10$ shall be stopped

Rules in printers are ideally device-centric, made to lower cost and avoid errors by end-users (trying to print a paper format not available on that printer model):

You can define the following rules on small non-duplex A4 printers:

- No print job of more than 25 pages
- No A3 paper print job
- No duplex job (printer is not duplex)

You can define the following rules on duplex and A3-capable printers:

- No print job of more than 100 pages, ask users to contact print room service

Limitations

Forced B/W, Forced Duplex, and Toner Saving actions are supported only by the following printers:

- HP
- Konica Minolta
- Ricoh Smart SDK (SOP2)
- Toshiba
- Lexmark
- Xerox

Last modified: 29 September 2022

Pull Print Delegation

What is Pull Print Delegation?

Celiveo Pull Print Delegation is part of the Celiveo Virtual Printer and allows Pull Print job delegation upon printing for another user to release.
In a few clicks, a user can delegate Pull Print to another Active Directory User chosen within a list accessible from a button in the Windows Taskbar.
The selected user can then collect the print jobs upon authentication on a Celiveo-enabled device.
Celiveo Pull Print Delegation is available with Celiveo Business+ and Enterprise Editions, part of the Celiveo Virtual Printer for Windows.

Installing Celiveo Pull Print Delegation

To install the Celiveo Pull Print Delegation you should run the Celiveo Virtual Printer installer in the command prompt followed with one of the arguments below.

- **Installer.exe -cppdsam** – This command will install and configure the Celiveo Pull Print Delegation to use the sAMAccountName as the username reference.
- **Installer.exe -cppdupn** – This command will install and configure the Celiveo Pull Print Delegation to use the userPrincipalName as the username reference.

User Interface

To access the Pull Print Delegation window

Click the desktop icon

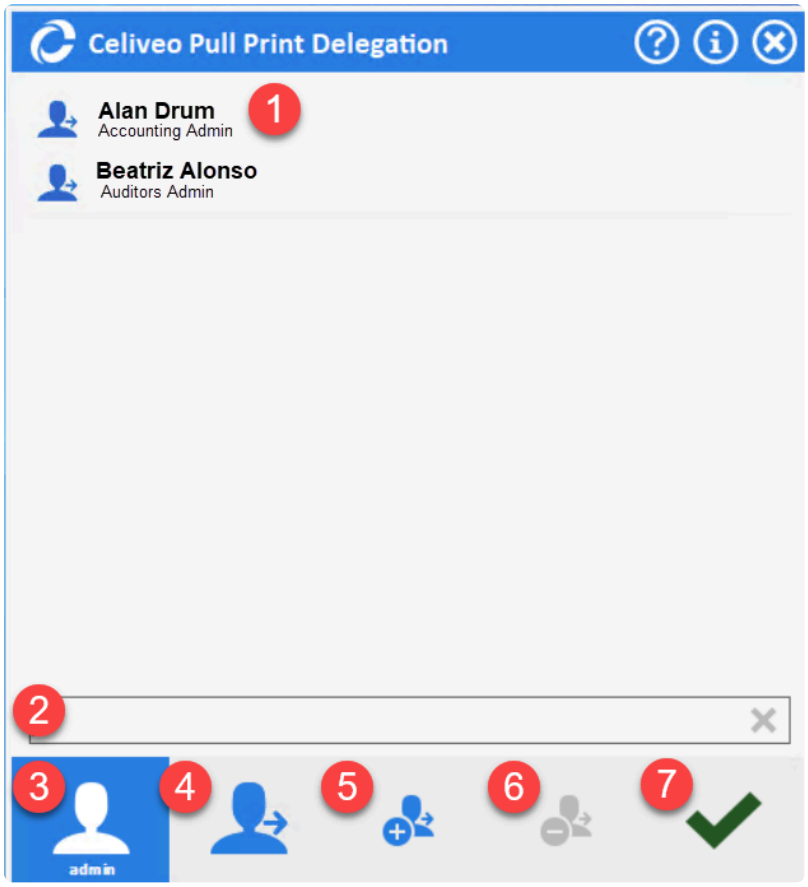
Notification/status Icon

The icon indicates the Redirection status:

- Redirection ON
- Redirection OFF

Application UI

The application is also accessible with an icon on the Taskbar. Right-clicking the icon opens a pop-up window.

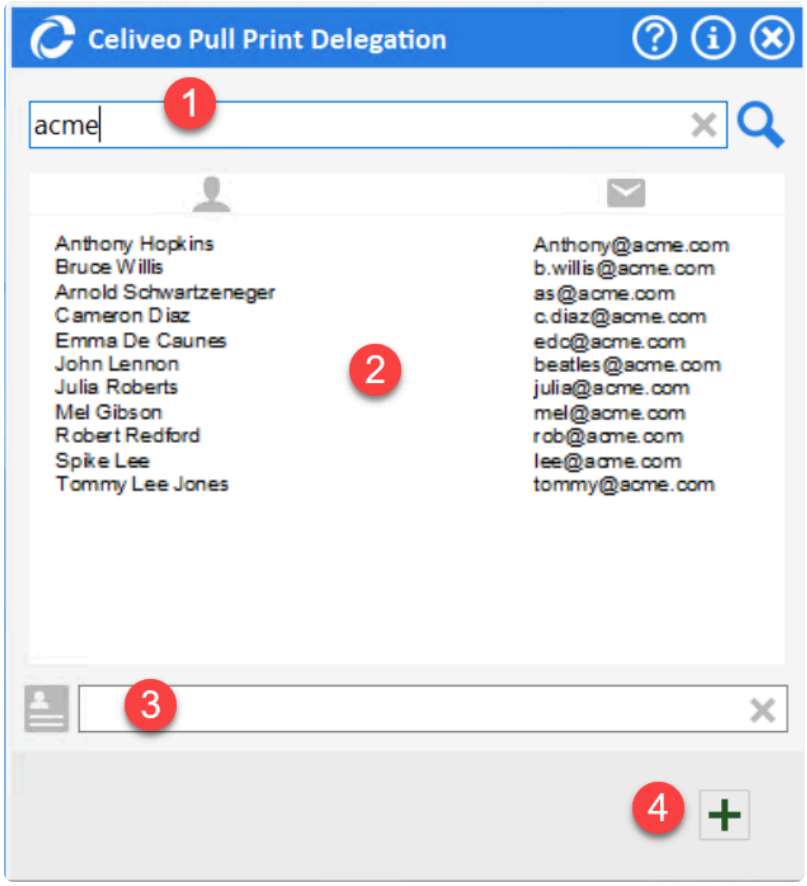


Menu option	Description
1	Choose an existing user in the list. Double-click to select and exit the window.
2	Filter the list by entering part of the wanted name.
3	Double-click to deactivate delegation and exit the window.
4	Select a user and double-click to activate delegation to this user and exit the window.
5	Click to add a user to the list.
6	Select a user and click to remove the user from the list.
7	Click to save the changes and exit the window.

Adding a user to the list

The icon allows adding a user to the list. A popup appears, as shown below.

It allows browsing the current user Active Directory connection to get a shortlist of users and select one.



Menu option	Description
1	Enter a minimum of 3 characters to search a user by name or email address.
2	List of all found users in alphabetical order.
3	Enter a comment for the user which will be visible under the user display name in the main window.
4	Click the + button to add the user and exit the window.

Frequently Asked Questions

What happens when the delegation is activated?

Subsequent print jobs are stored in the system for the user selected in the delegation process.
That user will see that document in his jobs list when he reaches an MFP to connect his print jobs.

How is that delegated user informed there is a print job for him?

The delegating user needs to use his standard communication methods (IM, direct communication) to ask the delegated user to collect his documents. The concept of email communication has been rejected by beta testers as they already have too many emails and this is not real-time. Using their existing IM such as Skype for Business or Teams had their preference.

Celiveo will continue to innovate and add more capabilities in the near future.

Can the delegated print jobs expire?
Yes, delegated print jobs are like the non-delegated print jobs and expire if not collected after the predefined time set by the administrator.

Who will be shown as the job owner in tracking?
The delegated user becomes the job owner as soon as the delegator prints for him/her.

If I have a quota in place, what quota will be used?
The delegated and delegator are usually from the same OU or quota group, the quota of the user who releases the document is the one debited with the pages cost/count. We don’t recommend applying a personal user quota if print delegation is installed for such users.

Last modified: 29 September 2022

13. User Management

This topic details everything you need to know about managing your Celiveo users and administrators.

Managing System Administrators
Add Domain Users for Print Direct

Last modified: 29 September 2022

13.1. Managing System Administrators

h4. Contents

1. About System Administrators
    a. The Super Admin
    b. What is a Community
    c. Regular Admins
    d. Print Rules and Access Control Rules
    e. Visibility of Users and Printers on Web Admin
    f. Effective Community
2. How to…
    a. Create a Non-Domain User as an Administrator
    b. Add Domain Users as Administrators
    c. Add Printers to a Community
    d. Label Tags

About System Administrators

The Super Admin

When you install Web Admin, an Administrator User (User Name = Admin) is automatically created. This user has administrative privileges over all users and all printers, and hence is referred to as Super Admins. Super Admins can appoint other users as Super Admins. The other users can be domain users, or they can be non-domain users who are created on the Celiveo database.

If communities are defined, Super Admins can appoint Regular Admins for a community rather than creating another Super Admin.

What is a Community?

A community is a group of users, workstations, printers, and administrators that have a common characteristic. For example, a group of users, workstations, printers, and administrators, located in the same building.

The community that a user or printer belongs to is determined by the tags assigned to them. We will use an example to illustrate the concepts behind system administrators and communities.

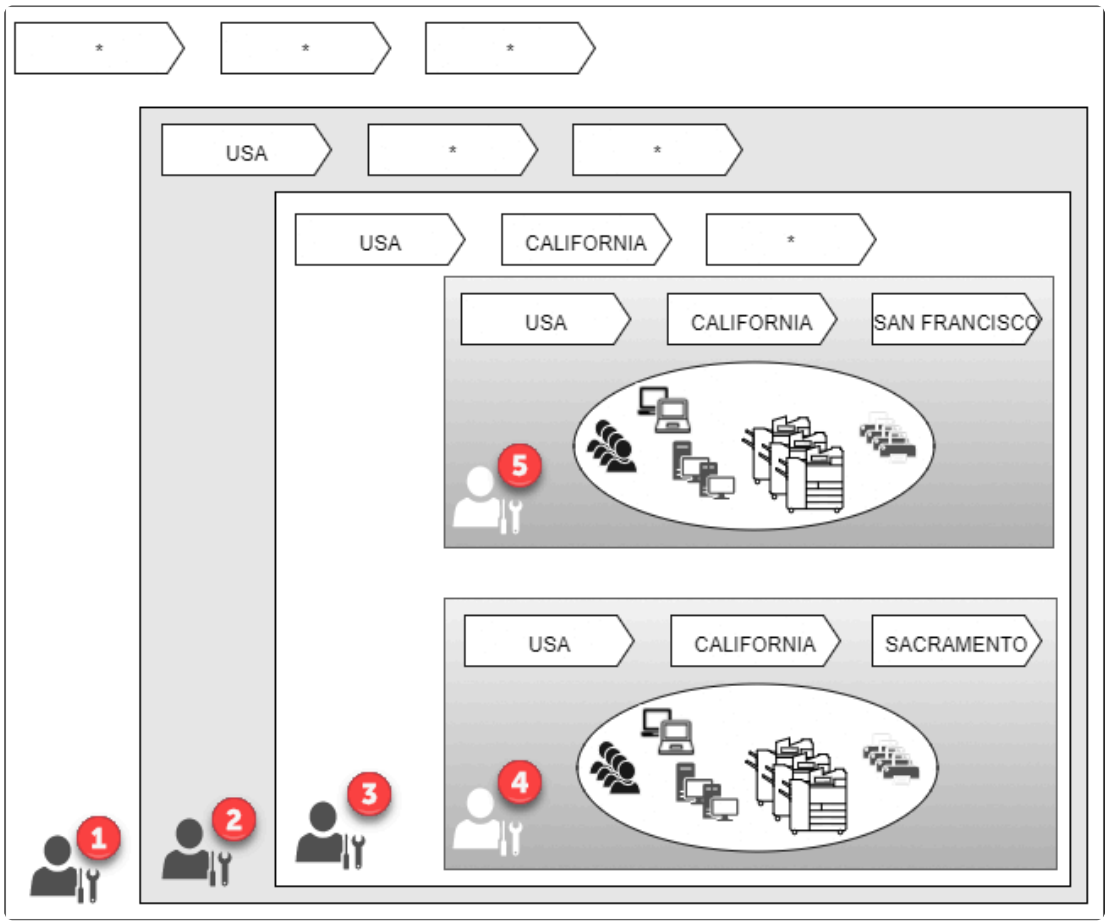
An example is a company distributed across several cities. The company uses tags to identify places. Although Celiveo supports up to five tags, they use only three, which identify Country, State and City. A user tagged USA, California, San Francisco, belongs to the San Francisco community. A user tagged USA, California, *, belongs to the California community, which is a super set of San Francisco and Sacramento.

Regular Admins

Super Admins can pick a user who belongs to the California community and make that user an

Administrator. That user then becomes an administrator for the California community. In this manner the Super Admin of a large organization is able to delegate administrative privileges for each community to regular admins who are responsible for their community.

The administrator for California can pick another user belonging to the California community and make that user an administrator. As such California will now have more than one regular administrator. In this manner the Admin for California is able to delegate duties to a peer to assist with administration. Additionally, California administrators can delegate administrative duties for the smaller community of San Francisco to a user who belongs to the San Francisco community. Using this technique of defining communities and appointing admins for each level of community, you can implement a multi-level admin strategy for an organization.



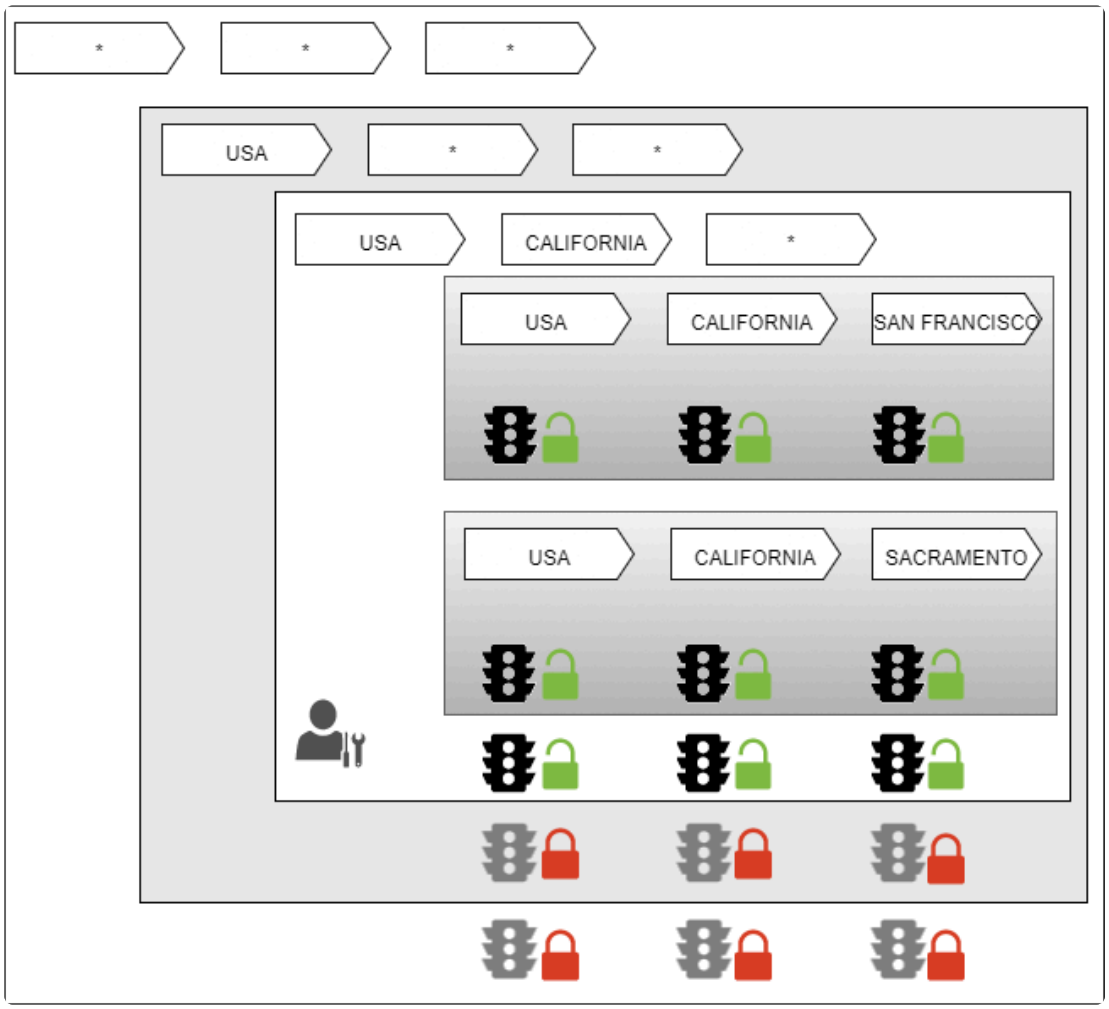
Legend

1- Default Admin – Super Admin created automatically at installation
2- Regular Admin – Can handle all communities within the USA
3- Regular Admin for California (including San Francisco and Sacramento)
4- Regular Admin for Sacramento.
5- Regular Admin for San Francisco.

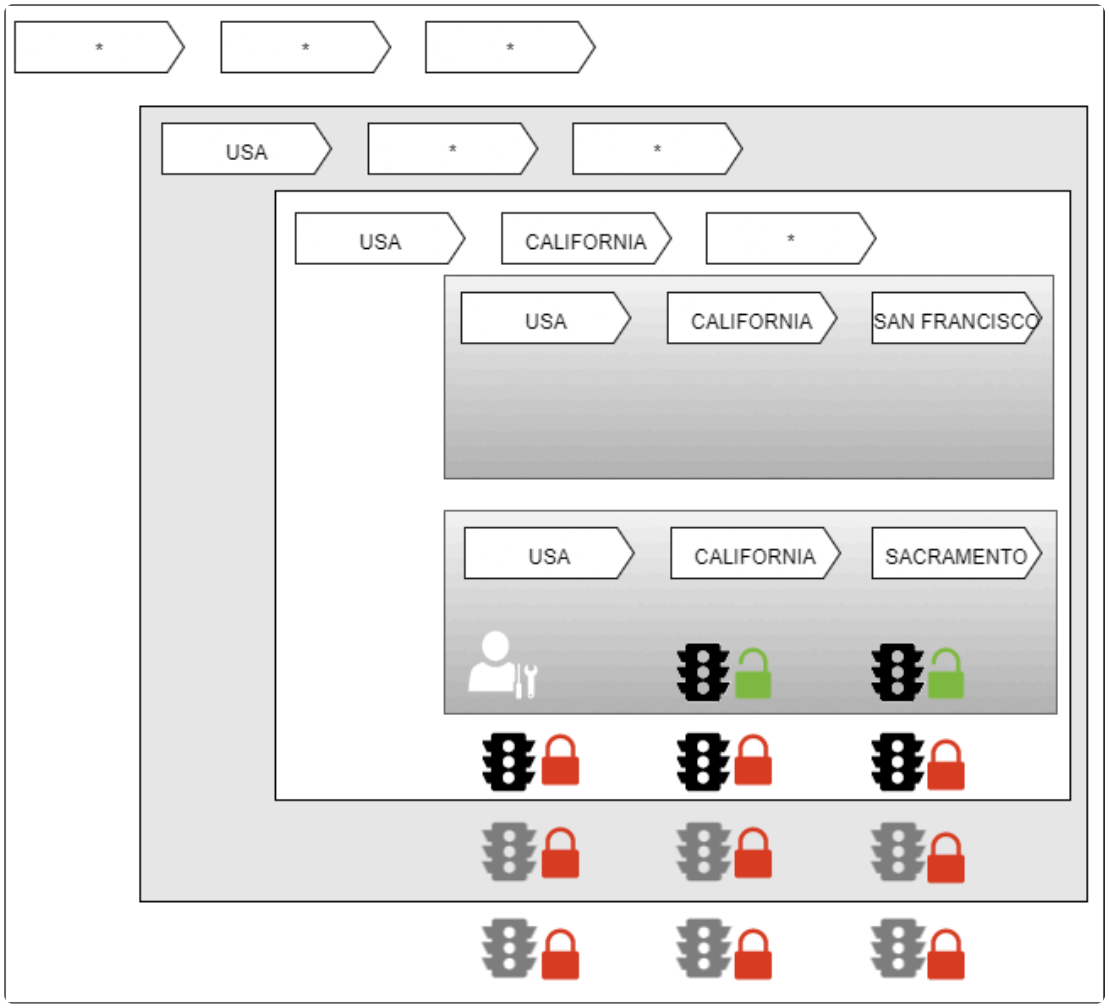
Print Rules and Access Control Rules

A regular admin has access to all Print Rules and Access Control Rules created by the administrators above them. However, they cannot modify these rules.

For example, the California administrator has access to, and can make use of all the rules created by the Super Admin and USA Admin. However, the California Admin cannot modify any of these rules. On the other hand, the California Admin can modify any rule that the San Francisco and Sacramento administrators have created.



The Sacramento administrator can see can make use of the rules created by the Super Admin, USA Admin and California Admin, but cannot modify them. The Sacramento administrator cannot access any rules that the San Francisco Admin created.



Visibility of Users and Printers on Web Admin

When a regular admin logs into web admin, in addition to the users and printers that belong to their community, they see the users and printers who belong to the larger communities they are part of. For example, when administrators of the Sacramento community log into Web Admin, in addition to the users and printers of the Sacramento community, they see the California users, USA users, as well as any untagged users and printers (users and printers that have * assigned to all tags). They however will not see any San Francisco users or printers.

Effective Community

An administrator user can inherit a community setting in more than one way.

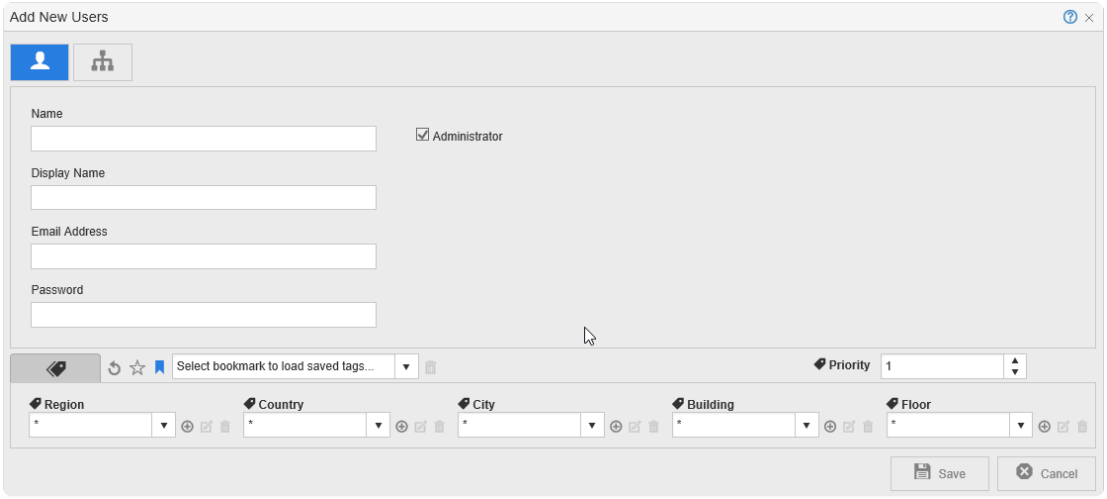
1. By the direct assignment of tags to their user account.
2. By assignment of tags to a user group. A user can be a member of more than one user group.

Whenever you assign a set of tags to a user or to a user group, you also assign a property known as “priority”. When a user inherits community settings from more than one source, the community (tag setting) with the highest priority takes precedence over the others.

How to…

Create a Non-Domain User as an Administrator

1. From the main menu, click .
2. Click . The Add New Users screen displays.



3. At **[Name]**, specify a unique name, which the user will use to log on to the Web Admin.
4. Select the **[Administrator]** check-box.
5. Specify the users name, email address and password in the appropriate boxes.
6. Specify the tags that define what community the user has admin privileges for.

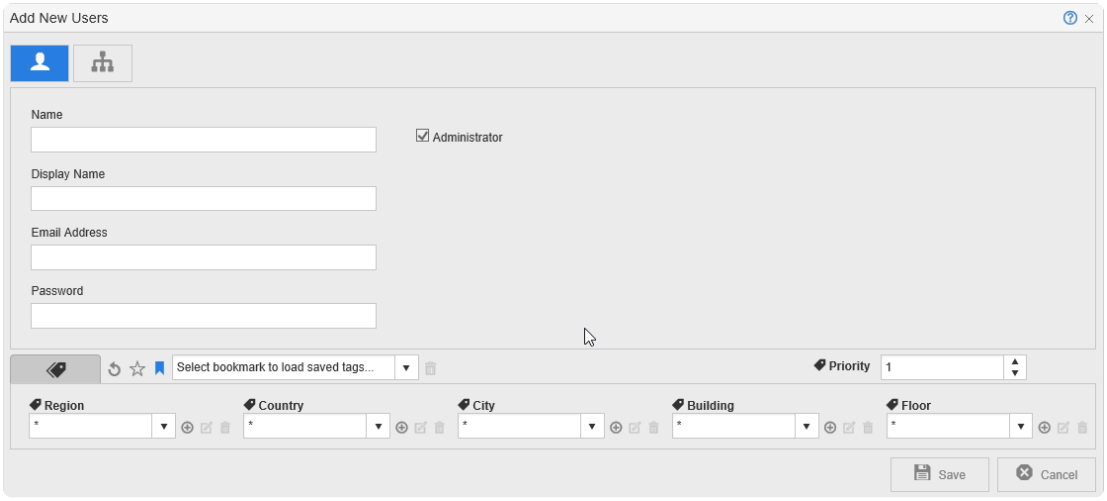
Notes:

- The new user inherits the same community as you, by default.
- You can change only those tags that are marked “*” in your own tag assignment, allowing you to make them administrators of a smaller community within your community.
- When the new user logs in to Web Admin, the user can access the printers, users and user groups that are part of the specified community.

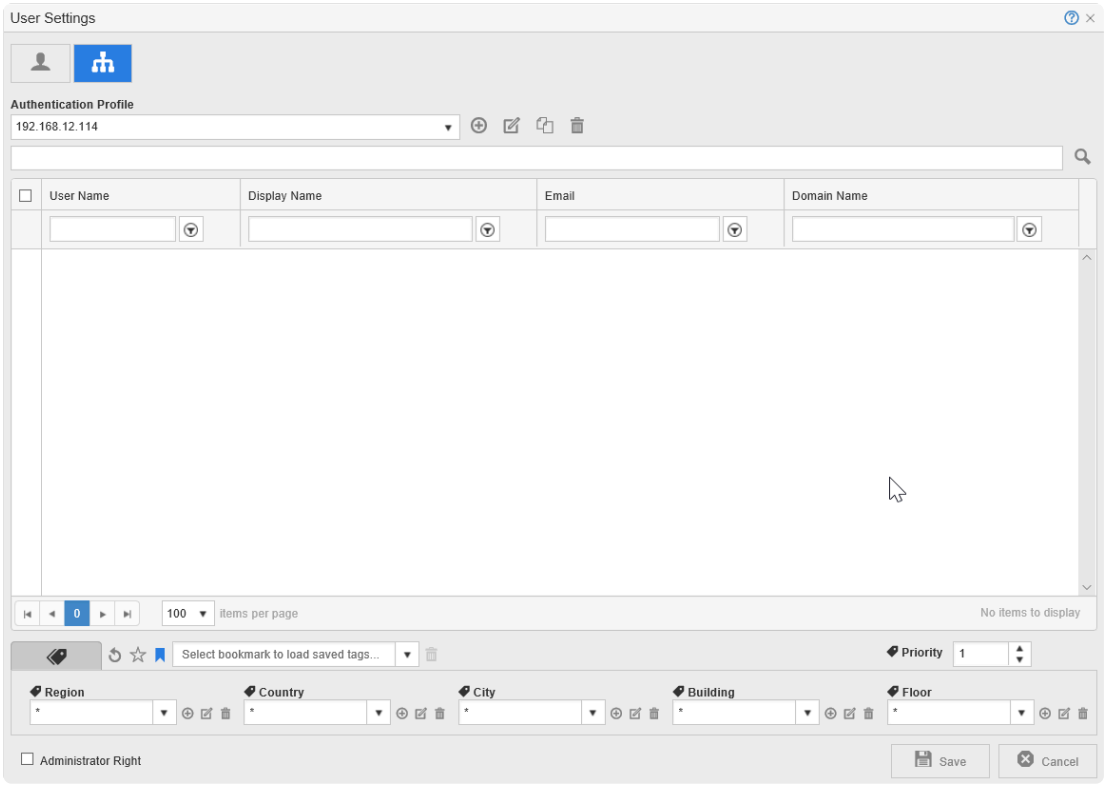
7. Click **[Save]**.

Add Domain Users as Administrators

1. From the main menu, click .
2. Click . The Add New Users screen displays.

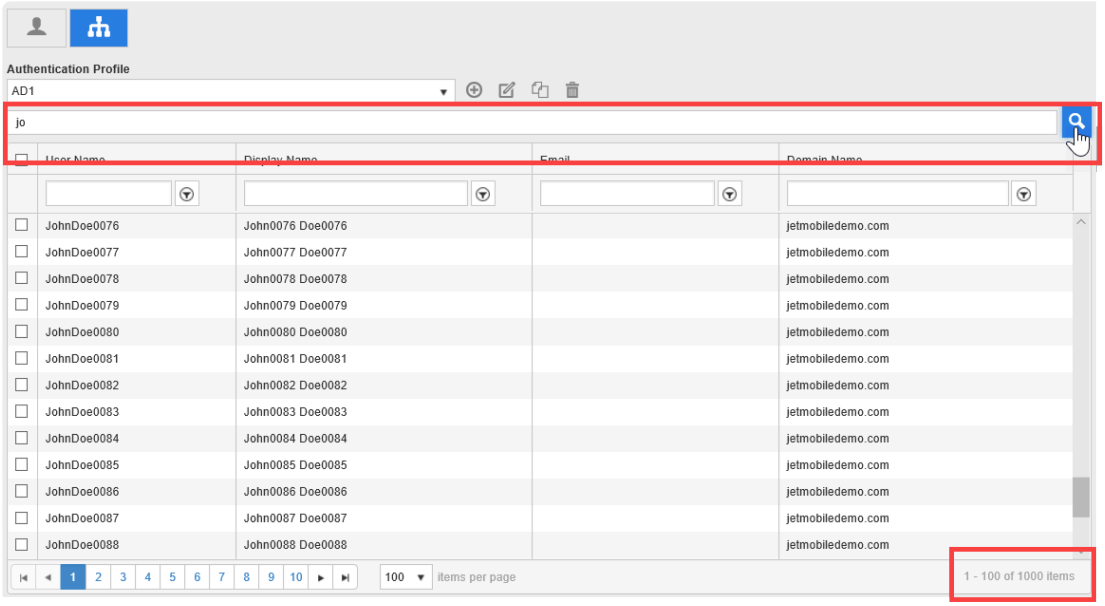


3. Click .



4. From the [Authentication Profile] drop-down, select the profile to fetch the list of domain users. If this is the first time setting up the **Authentication Profile** check on how to configure it here.
5. Click the icon next to the **[Search box]**, to list first 1000 users belonging to the selected domain. You can also search for particular user/ users by providing short names or characters.

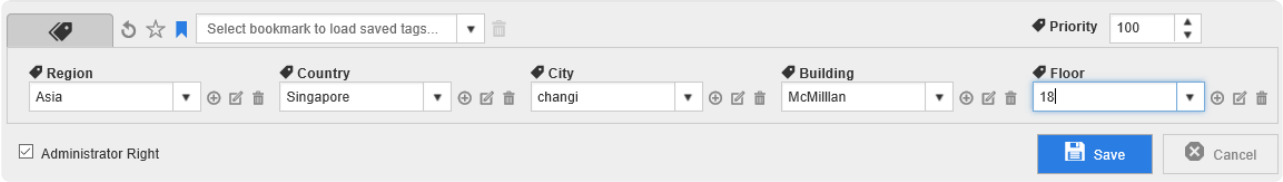
Note: Wild / Special characters cannot be used for Search.



6. Select the users you want to add to the user list.
7. Select the **[Administrator Right]** check box at the bottom-left.
8. Specify the tags that define what community the selected users are part of.

> **Notes:**
> ** The new user inherits the same community as you, by default.
> ** You can change only those tags that are marked "*" in your own tag assignment, allowing you to make the new users a part of a smaller community within your community.
> ** When the new users attempt to print via Print Direct, only the printers that are part of the specified community are listed.
> ** If the new users have admin rights, whenever they log in to Web Admin, they can access the printers, users and user groups that are part of the specified community.

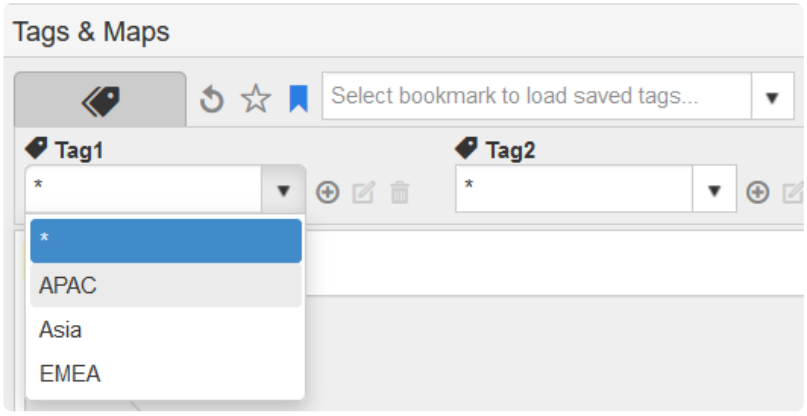
9. At **[Priority]**, assign a priority setting for the community (tag assignment) to be assigned to the new users. The highest priority is 100, and lowest is 1. When a user inherits a community from more than one source, the community with the highest priority overrides the others.



10. Click **[Save]**.
11. Now Domain Users can be used to login on the Web Admin.

Add Printers to a Community

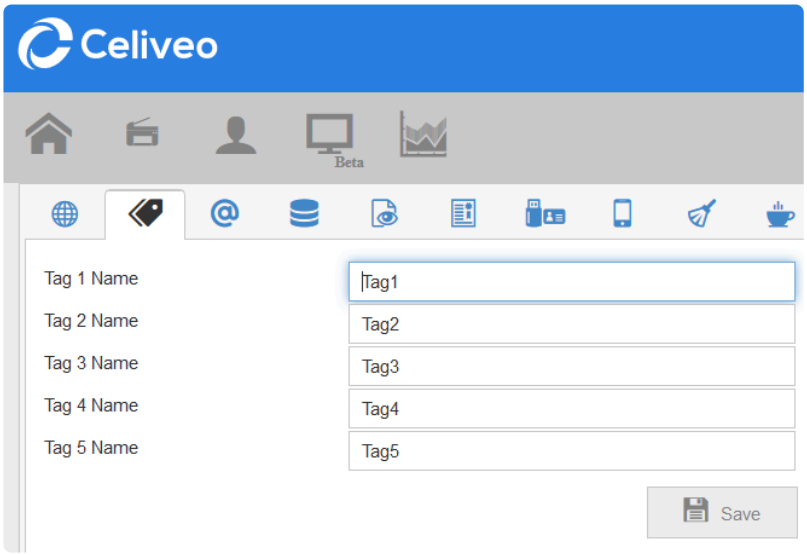
1. From the List of Printers, select the printers you want to specify tags for and click .
2. Select the tags for the printers.



3. If any tag drop-down list is empty, or does not contain the value you need:
   a. Click ⊕ next to the drop-down.
   b. Specify the new value for the tag and click **[Save]**.
4. Click **[Save]**. The tags are assigned to the printers.

Label Tags

1. Click ⚙.
2. Click 🏷



3. Label the tags as required and click **[Save]**.

Last modified: 29 September 2022

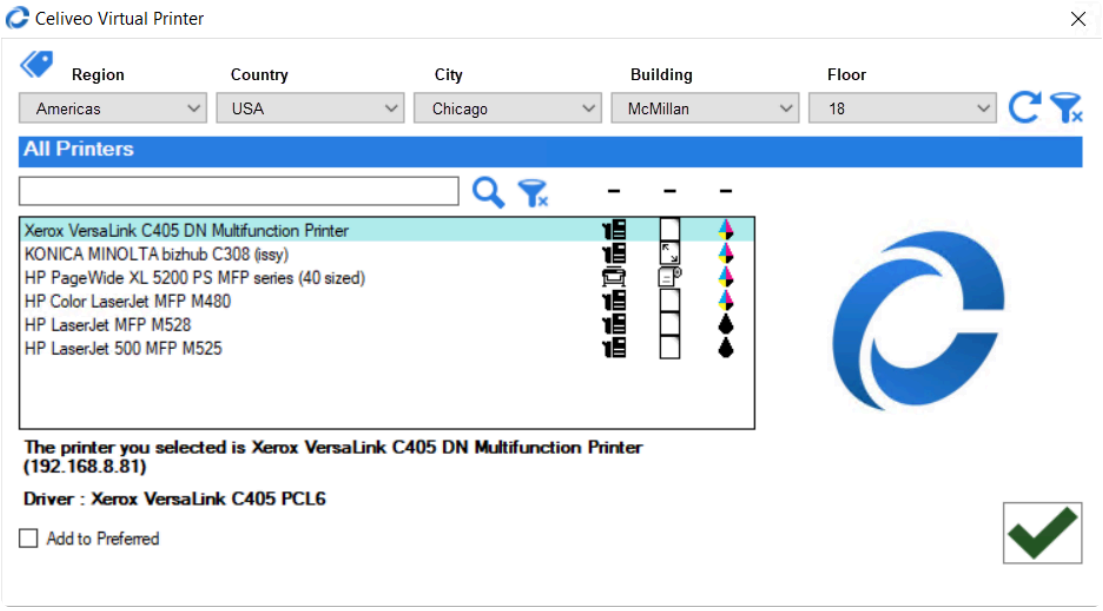
13.2. Add Domain Users for Print Direct

1. Why Add Domain Users to a Community?
2. What if I am a member of several groups/OU?
3. How to…
    a. Add Domain Users to a Community
    b. Add User Groups/OUs to a Community

Why Add Domain Users to a Community?

The User Experience for Print Direct can be enhanced greatly by adding Domain Users to a Community.

Celiveo is able to map you to a community based on AD/LDAP attributes such as Name, Organizational Unit, and Group. Thereby, when you attempt to print using Print Direct, the list of printers is filtered to display printers that are within your community, thereby reducing screen clutter.



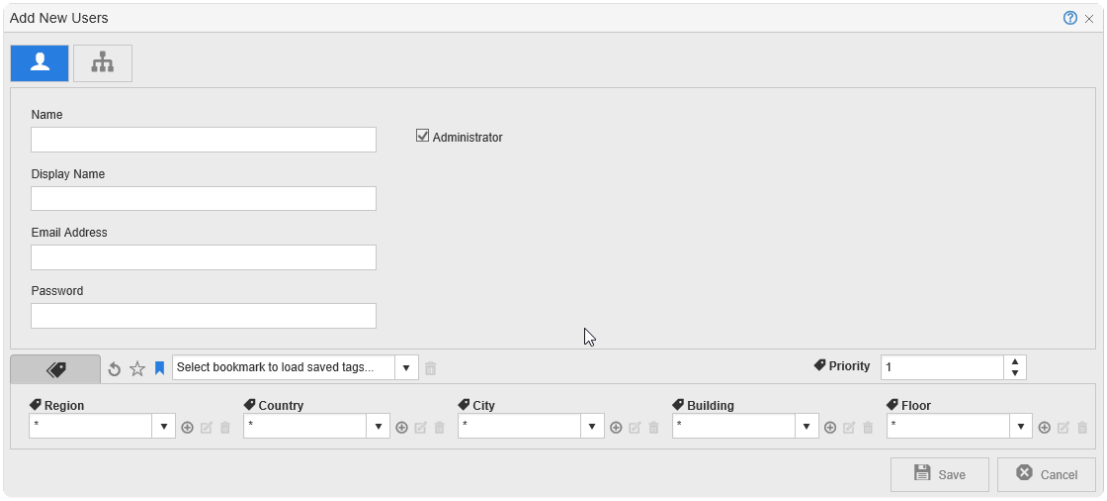
What if I am a Member of Several Groups/OUs?

If you are a member of more than one Group/OU, and each Group/OU is mapped to a different community, the community setting of the Group or OU with the highest priority value is assigned to you. The same principal applies if your user name is assigned to a community and you inherit a community from the groups you belong to. It is the community with the highest priority that is assigned to you.

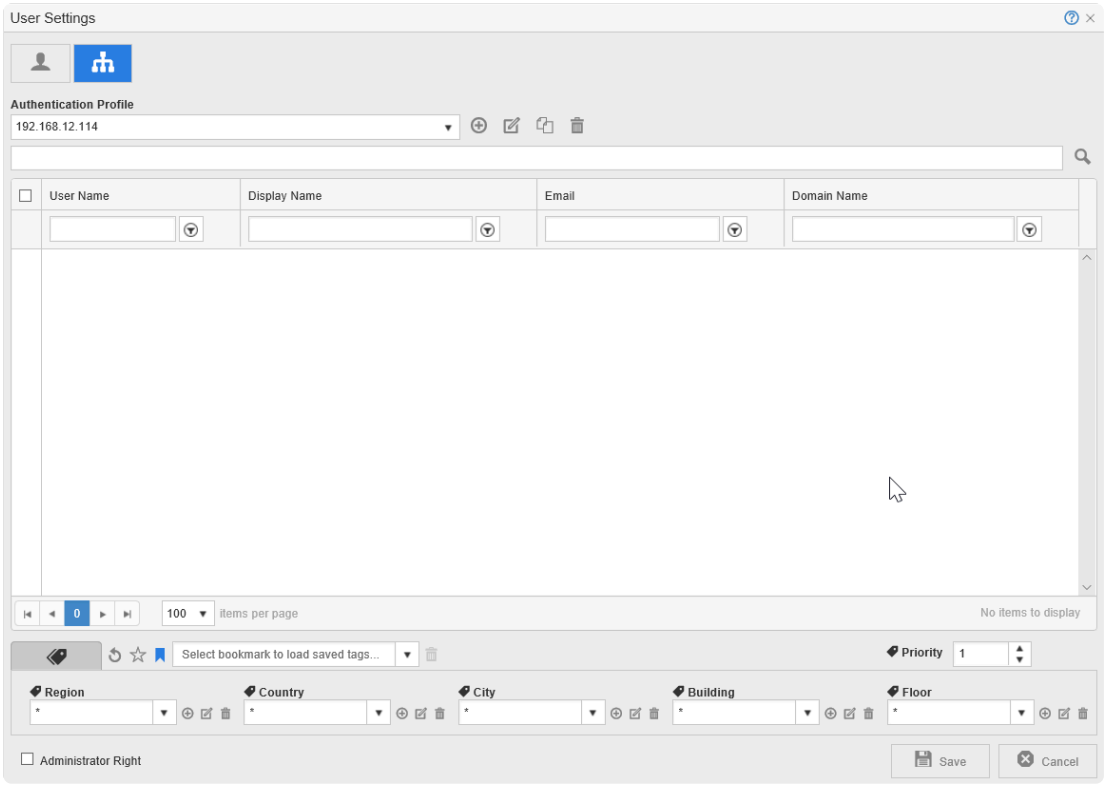
How to…

Add Domain Users to a Community

1. From the main menu, click .
2. Click . The Add New Users screen displays.



3. Click .



4. From the **[Authentication Profile]** drop-down, select the authentication profile to fetch a list of domain users.
5. Select the users you want to add to the user list.
6. Specify the tags that define what community the selected users are part of.

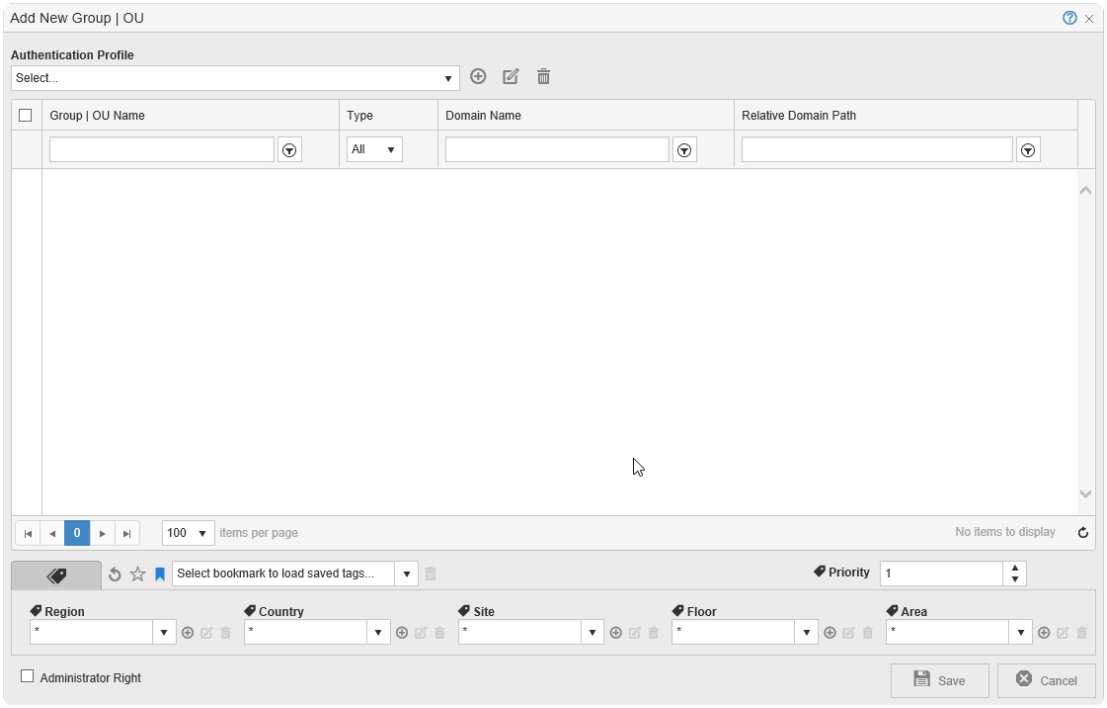
Notes:

- The new user inherits the same community as you, by default.
- You can change only those tags that are marked “*” in your own tag assignment, allowing you to make the new users a part of a smaller community within your community.
- When the new users attempt to print via Print Direct, only the printers that are part of the specified community are listed.
- If the new users have admin rights, whenever they log in to Web Admin, they can access the printers, users and user groups that are part of the specified community.
- You can also create bookmarks for frequently used tags; show or hide bookmarks as per convenience.

7. At **[Priority]**, assign a priority setting for the community (tag assignment) to be assigned to the new users. The highest priority is 100, and lowest is 1. When a user inherits a community from more than one source, the community with the highest priority overrides the others.
8. Click **[Save]**.

Add User Groups or Organizational Units to a Community

1. From the main menu, click .
2. Click . The Add New Group | OU screen displays.



3. From the **[Authentication Profile]** drop-down, select the authentication profile to fetch the Group or Organizational Unit from the Active Directory.
4. Select the Groups/OUs you want to add to the community.
5. Specify the tags that define the community.

Notes:

- The groups inherits the same community as you, by default.
- You can change only those tags that are marked “*” in your own tag assignment, allowing you to make the new users a part of a smaller community within your community.
- When the new users attempt to print via Print Direct, only the printers that are part of the specified community are listed.
- If the new users have admin rights, whenever they log in to Web Admin, they can access the printers, users and user groups that are part of the specified community.
- You can also create bookmarks for frequently used tags; show or hide the bookmarks as per convenience.

6. At **[Priority]**, assign a priority setting for the community (tag assignment) to be assigned to the new users. The highest priority is 100, and lowest is 1. When a user inherits a community from more than one source, the community with the highest priority overrides the others.
7. Click **[Save]**.

Last modified: 29 September 2022

14. Track and Report Print Jobs

Celiveo offers a powerful Tracking and Reporting tool. This section will help you understand it.

[Configure Quota Settings]
[Configure Default Cost Definitions]
[Configure Cost Definition Profiles]
[Using Celiveo Reporting tool – TGS 10]
[Downgrade from TGS 10 to TGS 8]
[Configure Embedded Tracking for Print-Direct]

Last modified: 29 September 2022

14.1. Configure Quota Settings

What are Quotas?

Print Quotas are used to control and reduce print costs by restricting users' prints to a certain cost or a certain number.
Quotas are supported as follows, depending on the serverless or server-based print flow:

- Serverless print flow (using a Celiveo Virtual Printer, CVP):
  User individual quota
  OU/group quota shared by individual users
  Combination of both types of quota for one user

- Server-based print flow (using a Celiveo Shared Virtual Printer, CSVP):
  User individual quota

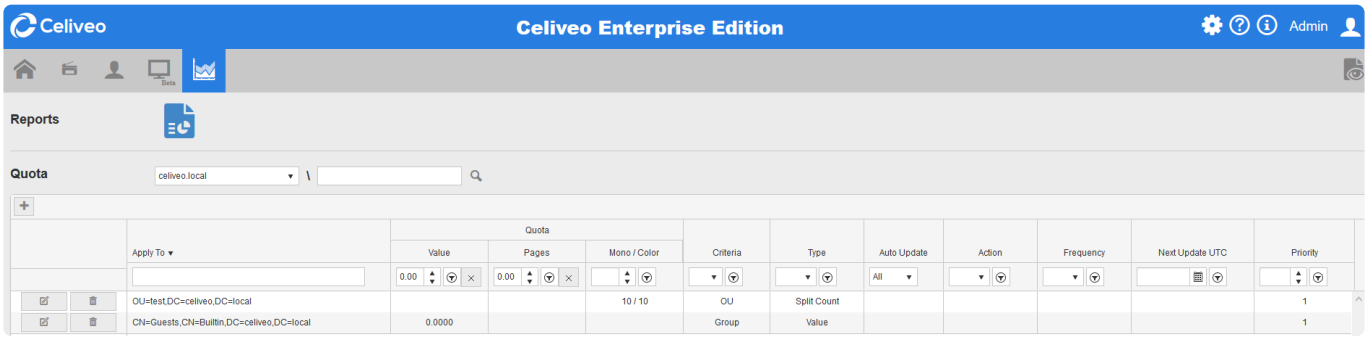
This difference is due to the inability to query Active Directory fast enough for each print job within the Windows Print spooler without potentially creating a significant bottleneck with stability side-effects.

You can define the quota settings to be applied to domain users.

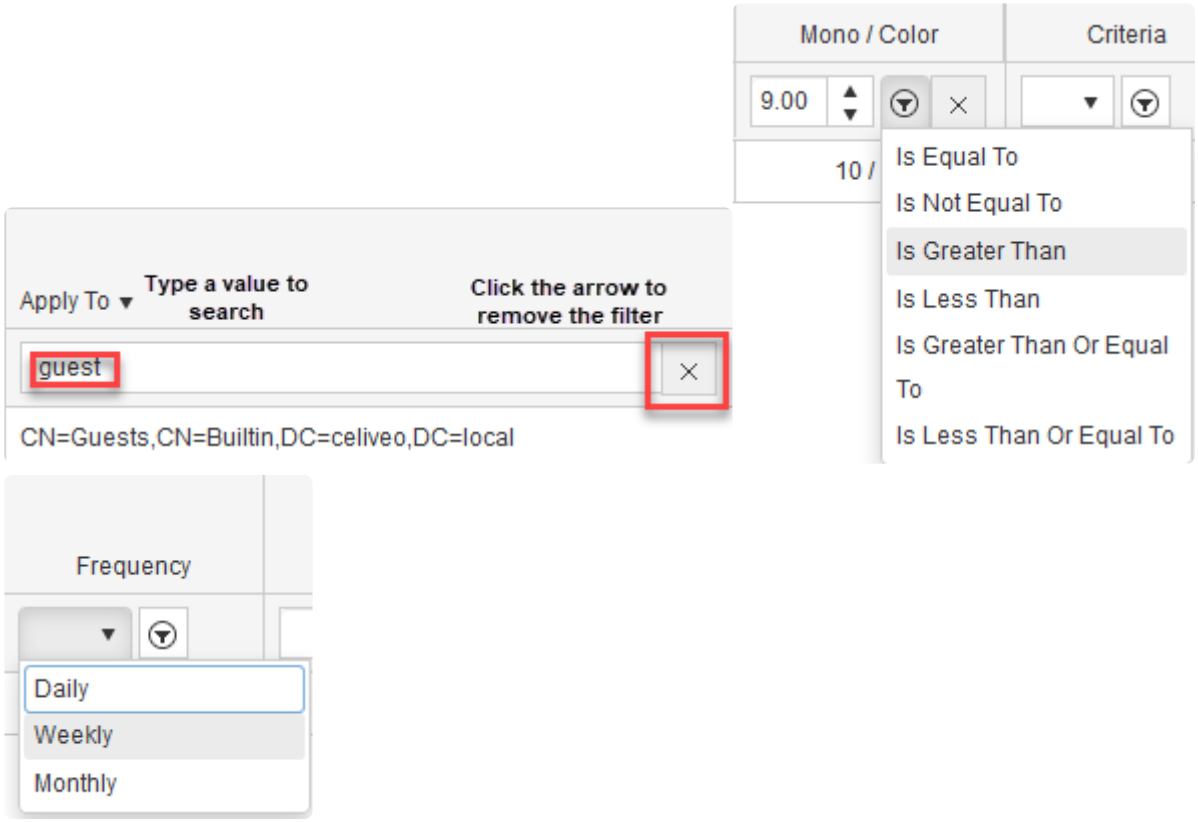
Important note: Usage quota rules only apply for CVP, not for CSVP (shared virtual printer).

To access the Quotas section:

1. On the Web Admin home page, click the **Tracking/Reporting** icon .
   The Quotas rules list is displayed.



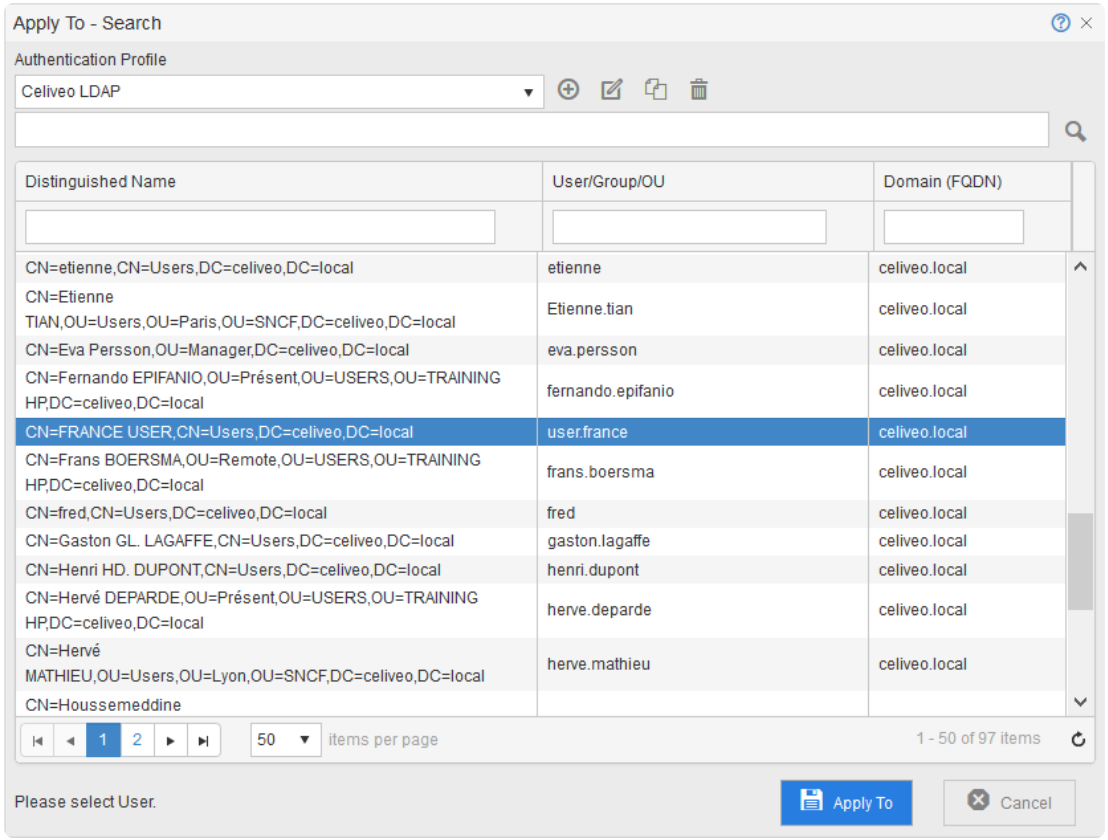
You can sort the existing rules in the list using either search fields, filters or drop-down lists:



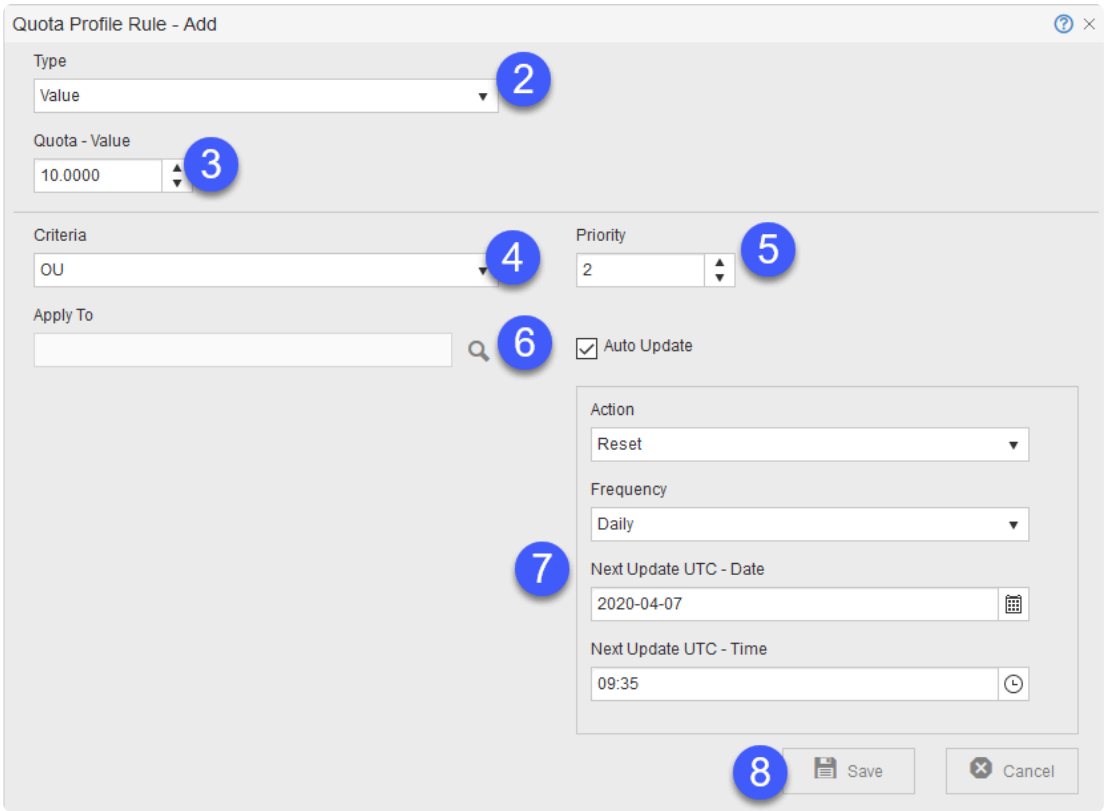
The objective of this search area is to find a specific user and check if this user has assigned quota either by the process of OU/Group or User directly.

To create a quota rule:

1. Click on the + icon.
2. In the drop-down list, select **Value**, to limit usage by the cost of printed pages, **Count**, to limit usage by the number of printed pages, or **Split Count**, to limit usage by the number of printed pages, sorted according to black and white or color prints.
3. Enter the quota value.
4. In the **Criteria** drop-down list, select what to apply the quota to: User, Group or OU.
5. Set the Rule priority
6. Click the Search button next to the **Apply to** field to select the User, Group or OU to apply the rule to.
    a. Select an Authentication profile or click the ⊕ icon to add one.
    b. Click the Search button next to display all Users/Groups/OUs in the authentication profile, according to what was selected in step 4.
    c. Select a value and click **Apply to**.



7. Check the **Auto Update** checkbox if you want your rule to be automatically updated on a regular basis.
   a. In the **Action** drop-down list, select Reset if you wish the quota to be reset or Add if you want it to be increased.
   b. In the **Frequency** drop-down list, select how often you want the quota to be updated.
   c. In the **Next Update UTC – Date** and **Next Update UTC – Time**, set the next update date and time.
8. Click **Save** to save the rule.



IMPORTANT NOTES:

- The first time a user authenticates on Celiveo, the user balance is displayed as “0.00” even if this user has quota. This is due to user initialization process. Once the user logs in again, the quota balance is updated to the correct value. For example, when a user reaches a 0 Copy Quota, the copy will continue but at the next login, the quota will be updated and the user will not be able to copy anymore.
- Quota stop rules must match the quota applied to the user otherwise it is not considered.

Example 1:

A credit in number of page is defined for user John Smith, and the MFP he is using has a print rule that contains a usage limit rule based on the credit value. That rule won’t be applied when John Smith uses the MFP.

Example 2:

A credit in a number of pages is defined for user John Smith, and the Celiveo Virtual Printer he is using has a print rule that contains a usage limit rule based on the credit value. That rule won’t be applied when John Smith uses that CVP.

When SQL Server is not reachable and a print rule uses quota value to decide if printing is authorized, then the printing will be blocked. This applies to push and pull printing.

Last modified: 29 September 2022

14.2. Configure Default Cost Definitions

The default cost definitions are applied if the administrator does not customize any cost definitions settings in a profile.

B E

Note: For direct storage of print jobs inside printer, the default paper type for cost pre-calculation is A4/Letter. The post printing cost/calculation will use the cost of the paper format actually used to output the print job. A future version of the driver plugin will improve the cost prediction .

Add new default cost definition

1. In the **[Cost Definition Settings]** window, click on the + sign.
2. Enter the paper type, dimensions and cost settings for the new cost definition.
3. Once settings are complete, click **[Save]**.
   The new cost definition is added to the default cost definition profile.
4. To return to the cost definition profile window, click **[Close]**.

Edit default cost definition

1. At the cost definition to edit, click on the Edit icon.
2. Edit the required settings and click **[Save]**.
   The cost definition is updated.
3. To return to the cost definition profile window, click **[Close]**.

Delete default cost definition

1. At the cost definition to delete, click on the Delete icon.
2. When prompted, click **[OK]** to proceed. To cancel, click **[Cancel]**.
3. To return to the cost definition profile window, click **[Close]**.

Last modified: 29 September 2022

14.3. Configure Cost Definition Profiles

B E

A **cost definition profile** comprises of a collection of cost definitions for the various paper types.

A **cost definition** refers to the cost of printing a single sheet for the selected paper type.

When a user prints a document, these cost definitions are applied to calculate the cost of the print job. For example, the cost of printing an A4 document in black and white is $0.05/sheet. If a user sends a print job comprising of 10 single-sided A4 sheets in black and white, the print job costs $0.50 in total.

You can also customize and apply cost definitions specifically for a printer or printer group.

1. Add a new cost definition profile

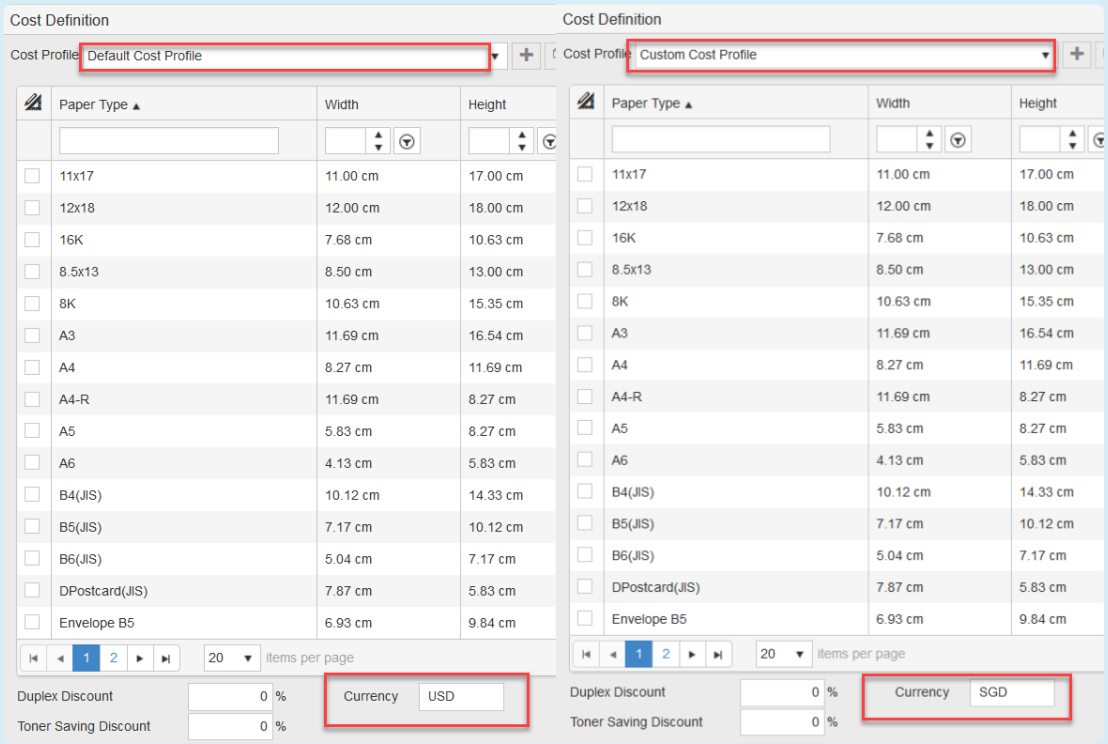
1. At **[Cost Definition Profile]**, click on the + sign.
2. When prompted, enter the new profile name and click **[Add]**.
   The new profile is added to the **[Cost Definition Profile]** drop menu.
   The default cost definitions are applied to this profile.

2. Customize a cost definition in a selected profile

You can create different profiles for one profile and customize the cost definition in each profile.

1. From the **[Cost Definition Profile]** drop menu, select the profile to edit.
2. To edit the cost definition for a specific paper type (e.g. A4), click the Edit icon.
3. Enter the new cost values and click **[Save]**.
   The new cost definition applies only when this cost profile is selected.
   When a profile containing customized cost definitions is selected, the customized cost definitions in this profile are highlighted.

NOTE: When using Pull Printing with a Celiveo Virtual Printer, if you want a customized Cost Definition to be applied, you need to update the CVP Cost Definition Profile with it. Otherwise, it is the Default Cost Definition Profile information that will be applied, such as the currency, which is USD by default – but can be changed if necessary.



3. Apply Duplex Discount

Cost savings result from duplex printing and you can apply the savings applicable to calculate this.
At **[Duplex Discount]**, enter the percentage discount to apply when calculating two-sided print jobs.

4. Apply Toner Saving Discount

Cost savings result from printing jobs using less toner for draft prints.
At **[Toner Saving Discount]**, enter the savings in percentage to apply when calculating print jobs printed in this mode.

To save all settings, click **[Save]**. To cancel, click **[Cancel]**.

NOTE: Ricoh printers do not propose toner saving mode, therefore the toner saving discount is not applicable on those devices.

Additional Information

Revert a customized cost definition to default

1. At the customized cost definition, click the Edit icon.
2. Uncheck the tick next to the paper type, then click **[Save>]**.
   The customized cost definition is removed from this profile. The default cost definitions settings are applied.

Delete a cost definition profile

A cost definition profile may become irrelevant due to a change in IT policies. If a cost definition profile is deleted, the default cost profile will apply on the affected the printers.

1. From the **[Cost Definition Profile]** drop menu, select the profile to delete.
2. When prompted, click **[Delete]** to confirm. To cancel, click **[Cancel]**.
   The profile is deleted.
3. Click **[X]** to exit.

Last modified: 29 September 2022

14.4. Using Celiveo Reporting tool – TGS 10

Contents

1. What is TGS 10?
2. Accessing the Reporting tool
3. TGS 10 Dashboard
4. Types of reports
5. Generating a report

1. What is TGS 10?

Celiveo Track-GreenSaver (TGS) 10 is an independent reporting tool of Celiveo that helps create detailed reports from the data collected from printer and MFP usage. These reports make it possible to monitor printing costs and influence user behavior. Detailed web-based reports help to identify sources of waste and fine-tune the printing environment to reduce costs and prevent misuse. You can also use the recorded data to forecast costs allowing you to better plan your budget.

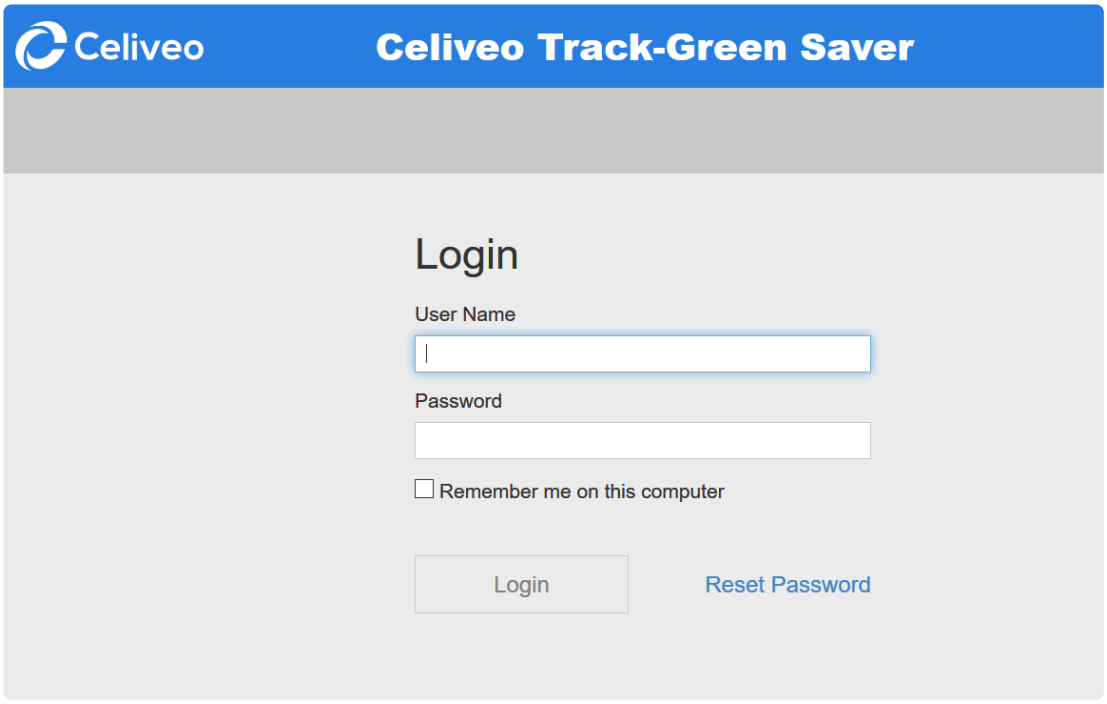
Reports are created based on the following data collected:

- Network data collected includes: user name, workstation name, server name, printer name, and printer group.
- Print job data collected includes: time/date printed, document title, document type, page count, sheet count, copy count, page size, print job size, black and white output, color output, duplex, etc. The SQL Server tracking database is in flat format with one event – one record. The table name is dbo.TrackingData in the SJPS database.
  That table can easily be queried with big data analysis and reporting software. For those who prefer, Celiveo propose its standalone Celiveo TrackGreen Saver software (TGS 10), a web application that computes the tracking table to generate dashboard and usage reports.

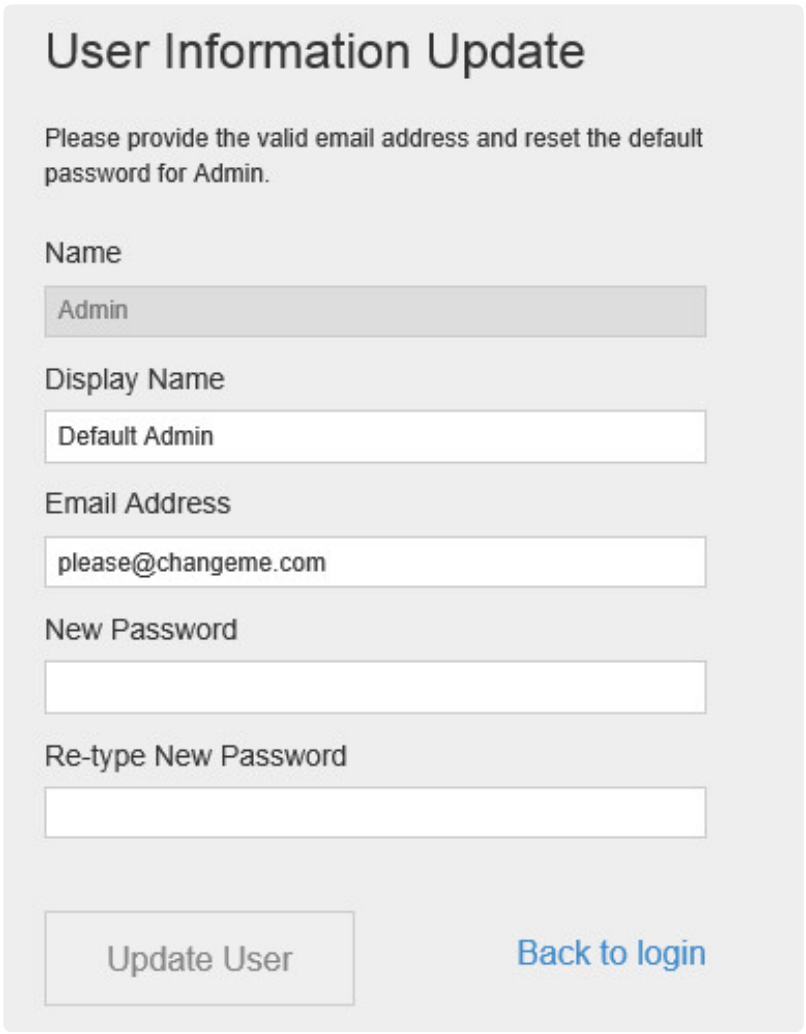
> ! **Note:** when printing from a Konica Minolta device, document names should not exceed 30 characters.

2. Accessing TGS 10

1. Double-click the Celiveo Reporting tool icon on the desktop. The initial login screen of the Reporting tool displays.



2. Specify admin as both the **[User Name]** and **[Password]**.
3. Click **[Login]**. The User Information Update screen displays.



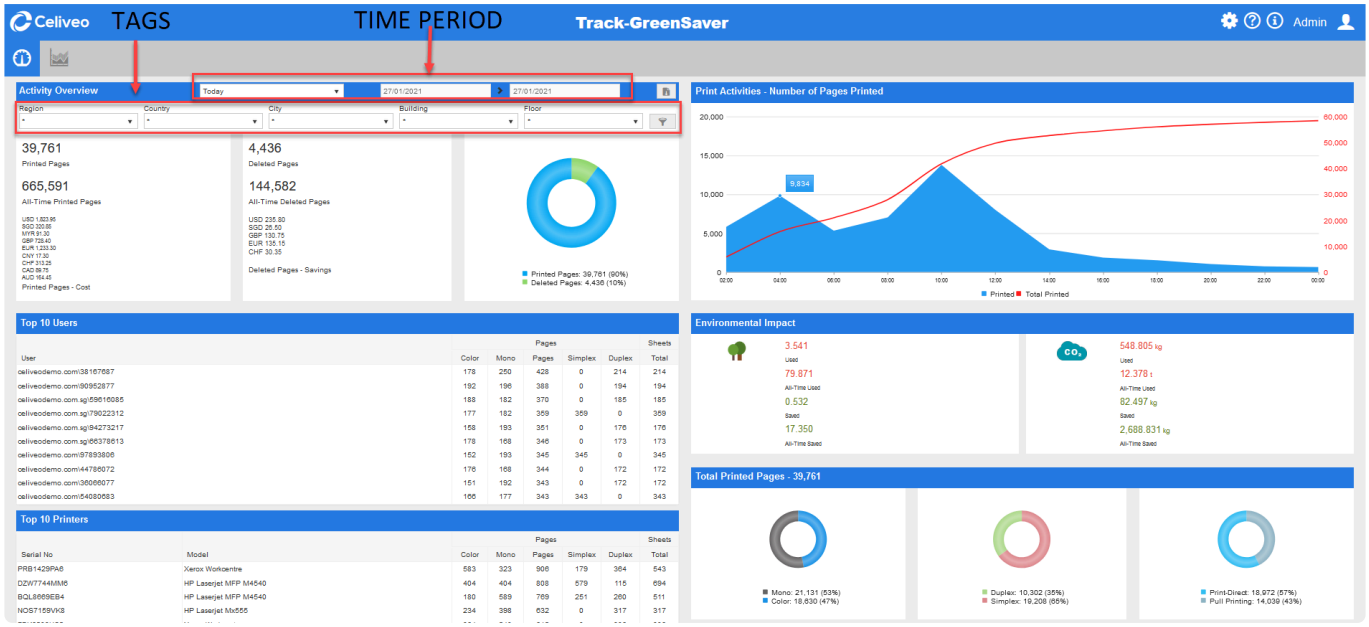
4. At **[Email Address]**, specify a valid email address.
5. Specify a new password for the default Admin user account.
6. Click **[Update User]**.

3. TGS 10 Dashboard

3.1 Settings

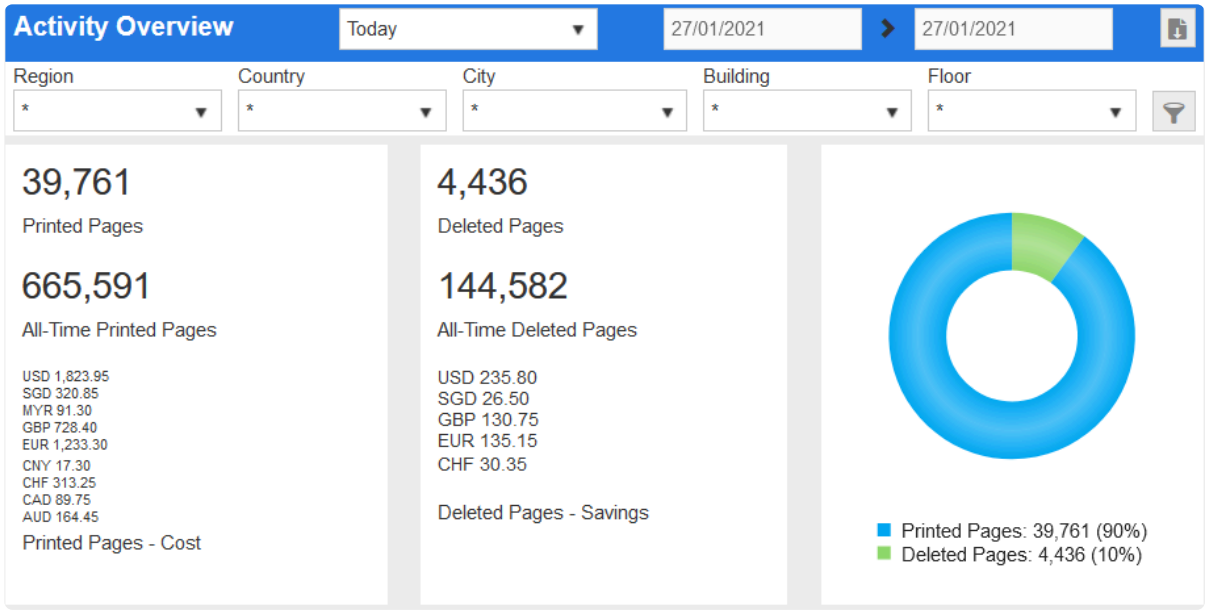
You can define the time period of your dashboard: you can choose to see the activity of the day, the last 7 days, or the last 30 days by clicking the buttons located at the top of the **Overview** section.

You can also choose to use tags to see data based on tag combinations.



3.2 Information provided

3.2.1 Activity Overview



This section details the number of pages that have been printed and deleted on the time period and geographical area you defined. It also indicates the cost of all printed pages and the savings allowed by

deleted pages in different currencies.

3.2.2 Top Users

Top 10 Users

	Pages					Sheets
User	Color	Mono	Pages	Simplex	Duplex	Total
celiveodemo.com\38167687	178	250	428	0	214	214
celiveodemo.com\90952877	192	196	388	0	194	194
celiveodemo.com.sg\59616085	188	182	370	0	185	185
celiveodemo.com.sg\79022312	177	182	359	359	0	359
celiveodemo.com.sg\94273217	158	193	351	0	176	176
celiveodemo.com.sg\66378613	178	168	346	0	173	173
celiveodemo.com\97893806	152	193	345	345	0	345
celiveodemo.com\44786072	176	168	344	0	172	172
celiveodemo.com\36066077	151	192	343	0	172	172
celiveodemo.com\54080683	166	177	343	343	0	343

This section provides printer usage information about the most active users on the time period and geographical area you defined.

Note: click on the column titles to sort the data in this column.

3.2.3 Top Printers

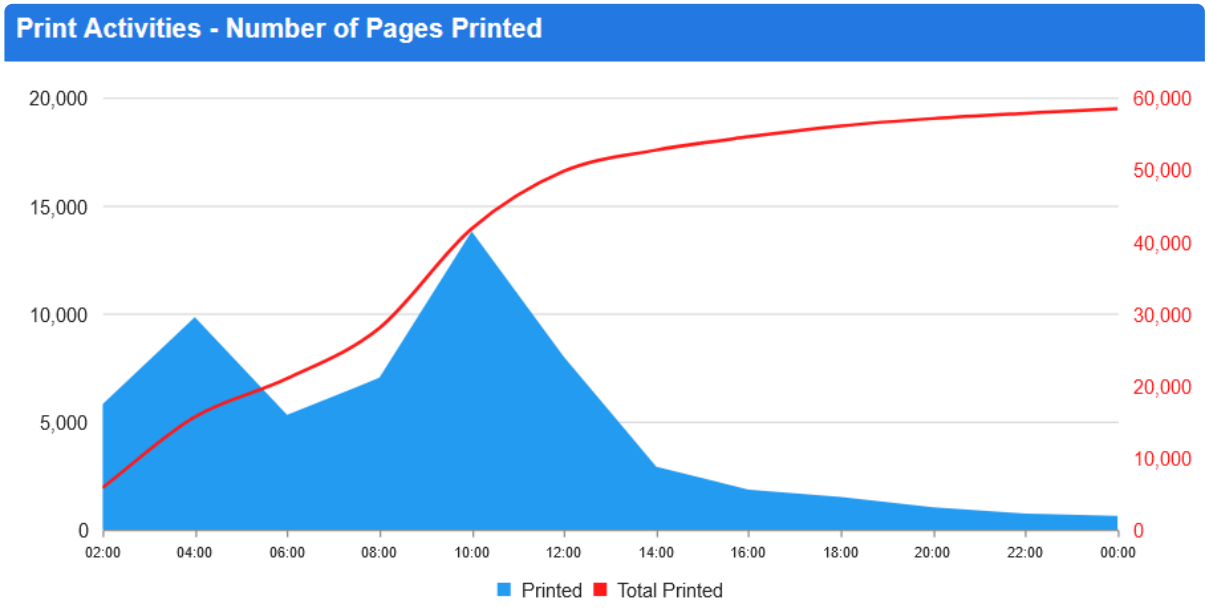
Top 10 Printers

		Pages					Sheets
Serial No	Model	Color	Mono	Pages	Simplex	Duplex	Total
PRB1429PA6	Xerox Workcentre	583	323	906	179	364	543
DZW7744MM6	HP Laserjet MFP M4540	404	404	808	579	115	694
BQL8669EB4	HP Laserjet MFP M4540	180	589	769	251	260	511
NOS7159VK8	HP Laserjet Mx555	234	398	632	0	317	317
FBK6203HC2	Xerox Workcentre	364	248	612	0	306	306
FNQ4925ZY7	Xerox Workcentre	264	324	588	448	70	518
MGB7880OY4	HP Laserjet MFP M4540	289	268	557	0	279	279
SLK5084XS8	Ricoh MP 300	339	218	557	557	0	557
AKK9087LR8	Ricoh MP 300	257	282	539	323	108	431
ISY5695MU1	HP Laserjet Mx555	224	302	526	297	115	412

This section provides usage information about the most active printers on the time period and geographical area you defined.

Note: click on the column titles to sort the data in this column.

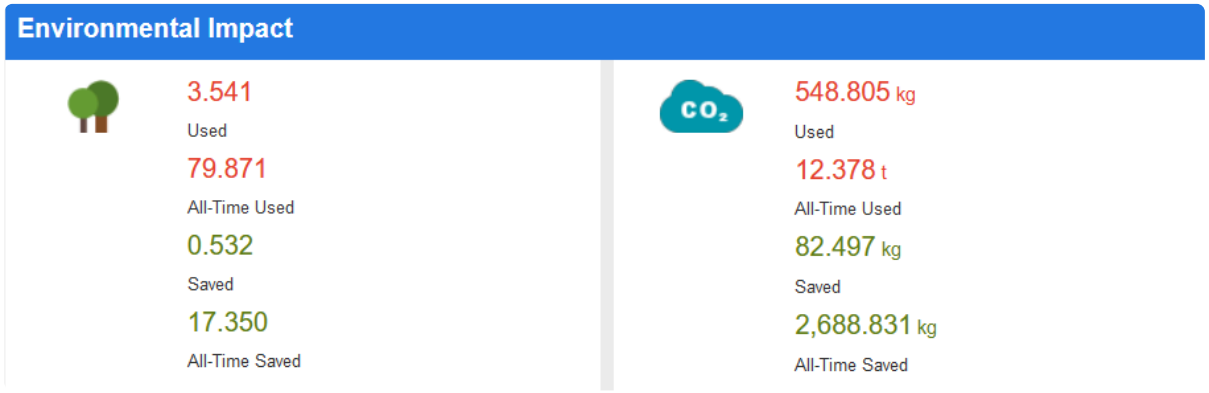
3.2.4 Print Activity



This section provides a chart indicating the number of printing pages over the time period and geographical area you defined.

> **Note**: Hover your mouse on the chart to obtain the exact numbers.

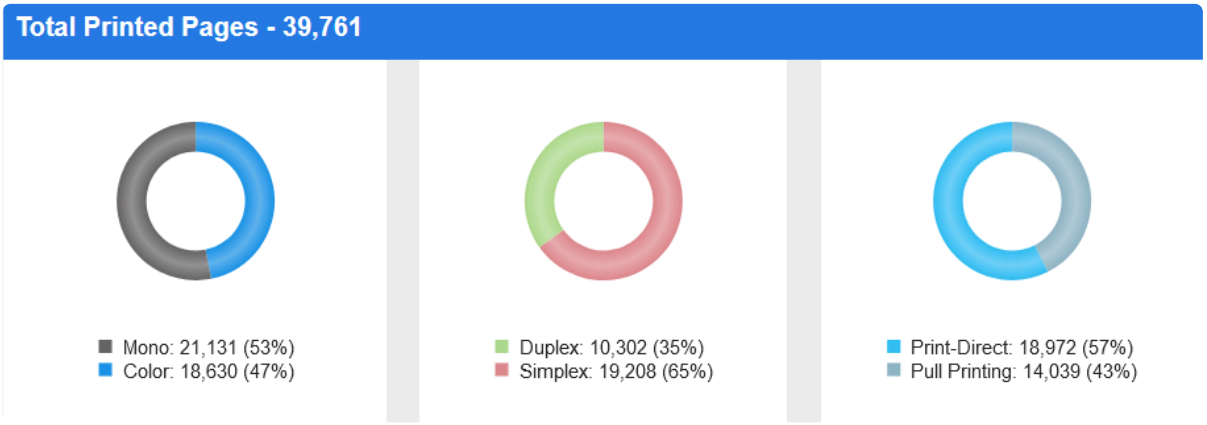
3.2.5 Environmental Impact



This section provides a diagram indicating the number of trees saved or used and the amount of CO2 saved or used over the time period and the geographical area you defined.

> **Note**: Hover your mouse on the diagram to obtain the exact numbers.

3.2.6 Total Pages



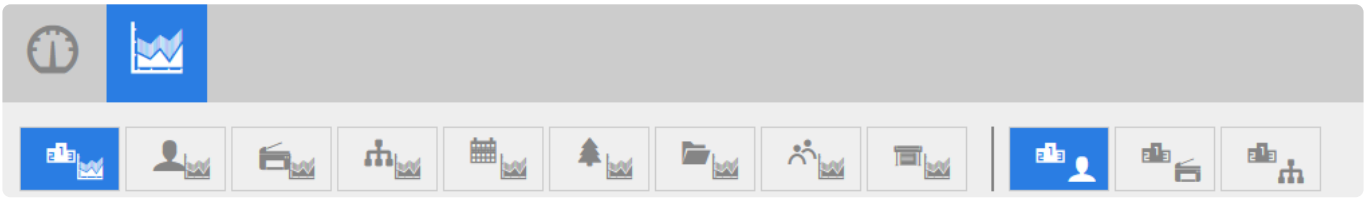
This section provides the total number of printed pages over the time period and geographical area you defined.

It also details how many pages were printed in black & white or color, in Simplex or Duplex and which type of job it corresponded to – Scan Job, Print-Direct or Pull Printing.

> **Note**: Hover your mouse on the diagram to obtain the exact numbers.

4. Types of Reports

TGS 10 produces the following types of reports:



4.1 User Reports

These reports allow you to view and compare printer usage for all users or a specific user.

- User Summary – displays print history of all users. You can also choose a specific user to view the user's printer usage statistics.
- User Summary by Printer – displays print history of users on the basis of the printer(s) used.
- User Summary by Page size – displays print history of users on the basis of page size of print jobs.

4.2 Printer Reports

These produce reports based on printer usage.

- Printer Summary – displays print history of all printers. You can choose a specific printer to view printer usage statistics

- Printer Summary by User – displays print history of printers on the basis of its users.
- Printer Summary by Page size – displays print history of printers on the basis of the size of the page.

4.3 Top Reports

Only available in Celiveo Enterprise Edition

These allow you to produce reports for the most active users, printers or departments.

- Top users – displays print history of the 10, 20 or 50 most active users.
- Top printers – displays print history of the 10, 20 or 50 most active printers.
- Top departments – displays print history of the 10, 20 or 50 most active departments.

4.4 By Month Reports

Only available in Celiveo Enterprise Edition

These reports allow you to view and compare printer usage by month.

- User by month – displays print history of all users by month. You can also choose a specific user to view the user's printer usage statistics by month.
- Printer by month – displays print history of all printers. You can choose a specific printer to view printer usage statistics.

4.5 Saving Reports

Only available in Celiveo Enterprise Edition

These reports allow you to view savings by user.

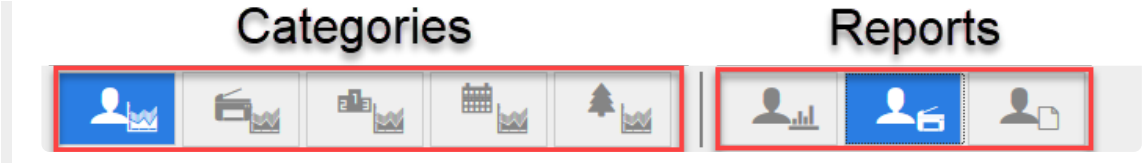
- Savings by user – displays savings realized by all users or a specific one.

5. Generating a report

5.1 To view reports

> **IMPORTANT**: in order to display correctly, the reports need to be first generated on a device that is connected to the Internet. This operation needs to be repeated every time the cache is cleared.

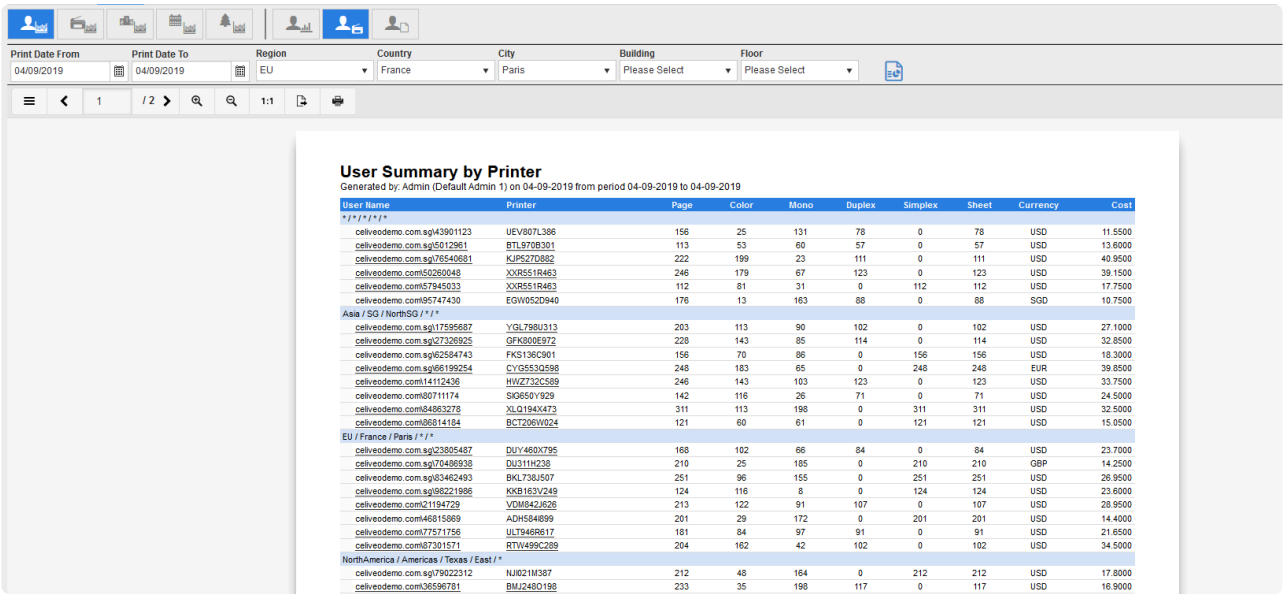
1. At the **[Reports]** menu, click one of the categories.



2. Then choose a report to view.
3. For demonstrative purpose, let's choose User Summary by Printer .
4. Choose the dates in the **[Print Date From]** and **[Print Date To]** fields using the **[Calendar]** icons to specify the date range to generate the report.
5. You can also choose from tags to display the records based on the tag combination selected.

> **NOTE**: A Super Admin can configure the tag names for TGS 10 via Web Admin.

6. Click the **[Generate]** icon to view the report.
7. The report generated will be displayed as in the image shown below:



User Name	Printer	Page	Color	Mono	Duplex	Simplex	Sheet	Currency	Cost
//*/*/*									
celiveodemo.com.sg\43901123	UEV807L386	156	25	131	78	0	78	USD	11.5500
celiveodemo.com.sg\5012961	BTL970B301	113	53	60	57	0	57	USD	13.6000
celiveodemo.com.sg\76540681	KJP527D882	222	199	23	111	0	111	USD	40.9500
celiveodemo.com\50260048	XXR551R463	246	179	67	123	0	123	USD	39.1500
celiveodemo.com\57945033	XXR551R463	112	81	31	0	112	112	USD	17.7500
celiveodemo.com\95747430	EGW052D940	176	13	163	88	0	88	SGD	10.7500
Asia / SG / NorthSG / */*									
celiveodemo.com.sg\17595687	YGL798U313	203	113	90	102	0	102	USD	27.1000
celiveodemo.com.sg\27326925	GFK800E972	228	143	85	114	0	114	USD	32.8500
celiveodemo.com.sg\62584743	FKS136C901	156	70	86	0	156	156	USD	18.3000
celiveodemo.com.sg\66199254	CYG553Q598	248	183	65	0	248	248	EUR	39.8500
celiveodemo.com\14112436	HWZ732C589	246	143	103	123	0	123	USD	33.7500
celiveodemo.com\80711174	SIG650Y929	142	116	26	71	0	71	USD	24.5000
celiveodemo.com\84863278	XLQ194X473	311	113	198	0	311	311	USD	32.5000
celiveodemo.com\86814184	BCT206W024	121	60	61	0	121	121	USD	15.0500
EU / France / Paris / */*									
celiveodemo.com.sg\23805487	DUY460X795	168	102	66	84	0	84	USD	23.7000
celiveodemo.com.sg\70486938	DU311H238	210	25	185	0	210	210	GBP	14.2500
celiveodemo.com.sg\83462493	BKL738J507	251	96	155	0	251	251	USD	26.9500
celiveodemo.com.sg\98221986	KKB163V249	124	116	8	0	124	124	USD	23.6000
celiveodemo.com\21194729	VDM842J626	213	122	91	107	0	107	USD	28.9500
celiveodemo.com\46815869	ADH584I899	201	29	172	0	201	201	USD	14.4000
celiveodemo.com\77571756	ULT946R617	181	84	97	91	0	91	USD	21.6500
celiveodemo.com\87301571	RTW499C289	204	162	42	102	0	102	USD	34.5000
NorthAmerica / Americas / Texas / East / *									
celiveodemo.com.sg\79022312	NJI021M387	212	48	164	0	212	212	USD	17.8000
celiveodemo.com\36596781	BMJ248O198	233	35	198	117	0	117	USD	16.9000

8. Click the **[User Name]** or **[Printer Name]** in the report page to view the print history of the user in detail.

5.2 Additional Viewing Options

Icon Description

Click to toggle between navigation pane.

Click to go to previous page of the report

Denotes the current page number. You can also click to specify a page number to view.

Click to go to the next page. The number denotes the total number of pages for the report.

Click to zoom in

Click to zoom out

 Displays the page in 100% resolution

Click to export the report in any of the following formats: Adobe PDF, XHTML/CSS, Multi-Mime HTML,

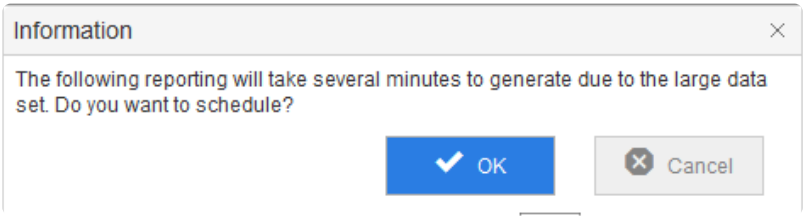
Excel, Word, RTF, XPS, TIFF, PNG, JPEG, Bitmap, Metafile (EMF), HTMLjQueryMobile, Powerpoint, Pinwriter (TTY),

SVG, Text(CSV), Text (Layout), XML

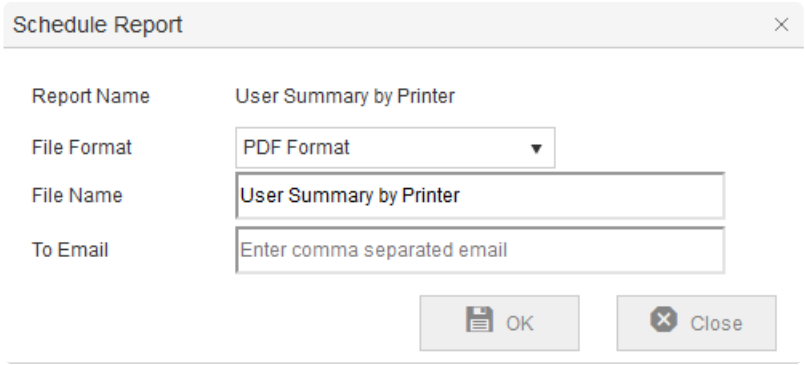
Click to print the report

5.3 Schedule and Email Reports

The optimal response time to display the report is about few seconds to couple of minutes, but if the report generation takes longer due to large data set, then a prompt will be displayed to schedule report viewing for later.



1. Click **[OK]**. This provides an option for the report to be sent via email so that you can view it at your convenience.
2. You can choose the format of the report to email, modify the filename, and email the report to more than one recipient.



Last modified: 29 September 2022

14.5. Downgrade from TGS 10 to TGS 8

1. Download the “TGS 8 manual rights script.sql” file.
2. Open it in SQL Server Management Studio.
3. Replace these 3 lines as follows:

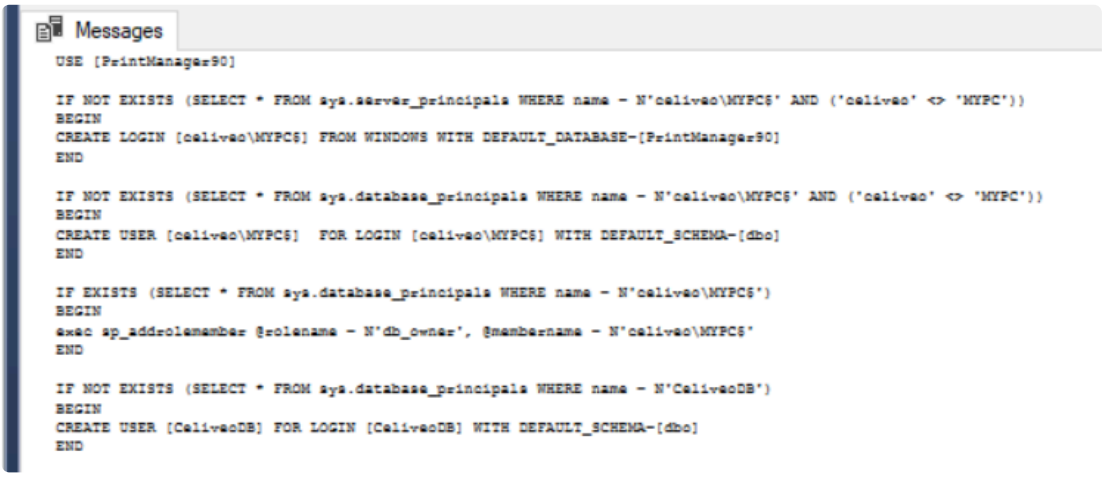
```
USE PrintManager90


print 'USE [PrintManager90]' + + CHAR(13) + CHAR(10) + + CHAR(13) + CHAR(10)

Declare @cmd nvarchar(MAX), @domainName nvarchar(500), @computerName nvarchar(500), @cvoSer
SET @domainName = '<domain>'
SET @computerName = '<computerName'
SET @cvoServiceUserForWA = '<DBUserName>'
```

For @domainName – put the machine where TGS 8 is installed domain name.

For @computerName – put the computer where TGS 8 is installed hostname.

For @cvoServiceUSerForWA – put the DB service account name which is used to install Web Admin.

4. Run the script on SSMS.
5. Copy the script from the “Messages” window in SSMS and run it again using SSMS.

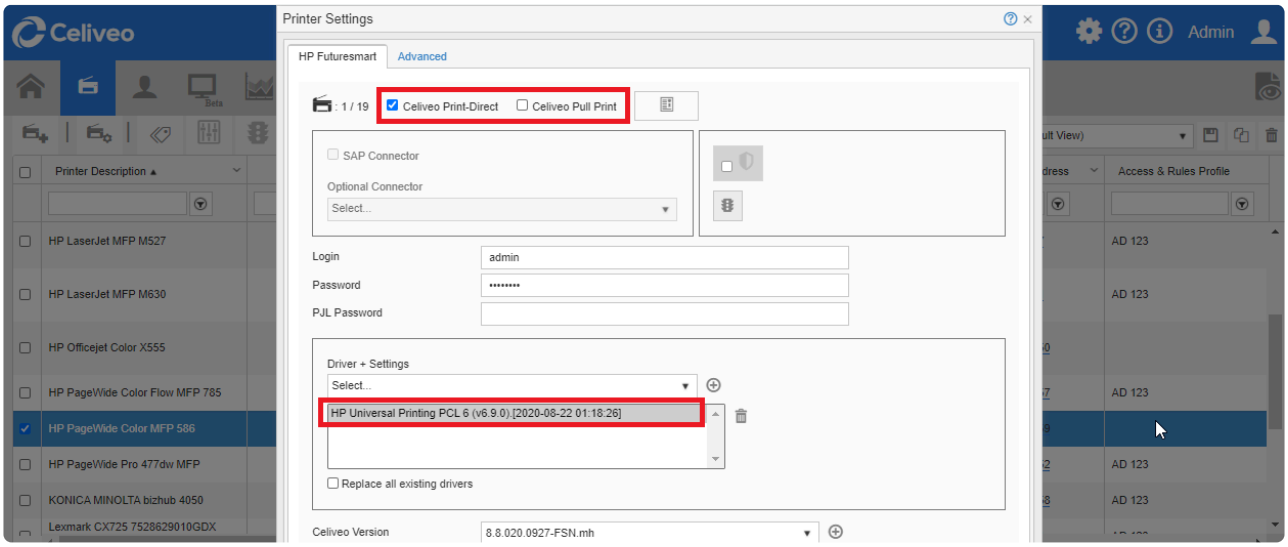


Last modified: 29 September 2022

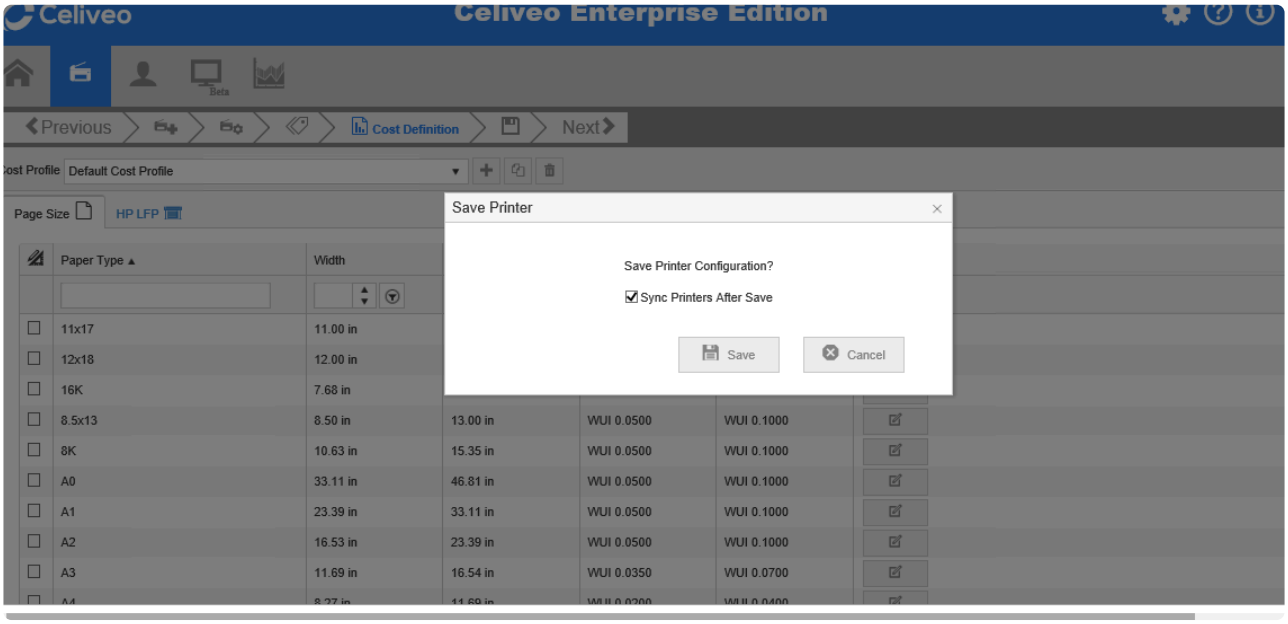
14.6. Configure Embedded Tracking for Print-Direct

Embedded tracking with Print-Direct is available for HP FS printers. It is available with a Print-Direct license to provide tracking information without deploying a CVP on the client machine.

1. When adding a Printer, in the Printer Settings, load the HP FS embedded agent and save it.
2. Uncheck the **Pull Print** checkbox and ensure the **Print-Direct** checkbox is enabled.



3. Save the settings.



Notes:
- After syncing the printer, the Printer status is **Synchronized (Print rules not set)**.
- In TGS 10, tracking data is labelled as Print-Direct.

Last modified: 29 September 2022

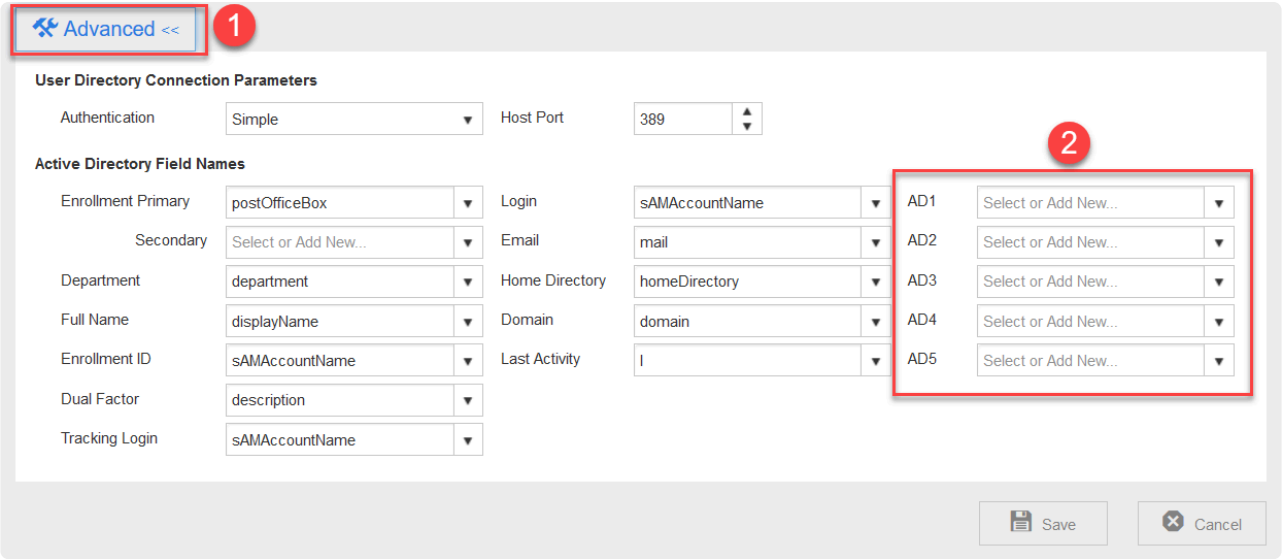
14.7. Add AD Attributes to User Enrollment Schema

This feature allows up to 5 custom Active Directory Attributes to be included into the user profile during enrolment in order to have the corresponding data included in tracking reports.

Configuration

Configure the information gathered for the tracking by printers.

1. In the **Authentication Source Profile** settings, select **Advanced**.
2. In the **Active Directory Field Names** section, select or enter an attribute in the **AD1, AD2, AD3, AD4** and/or **AD5** drop-down lists.

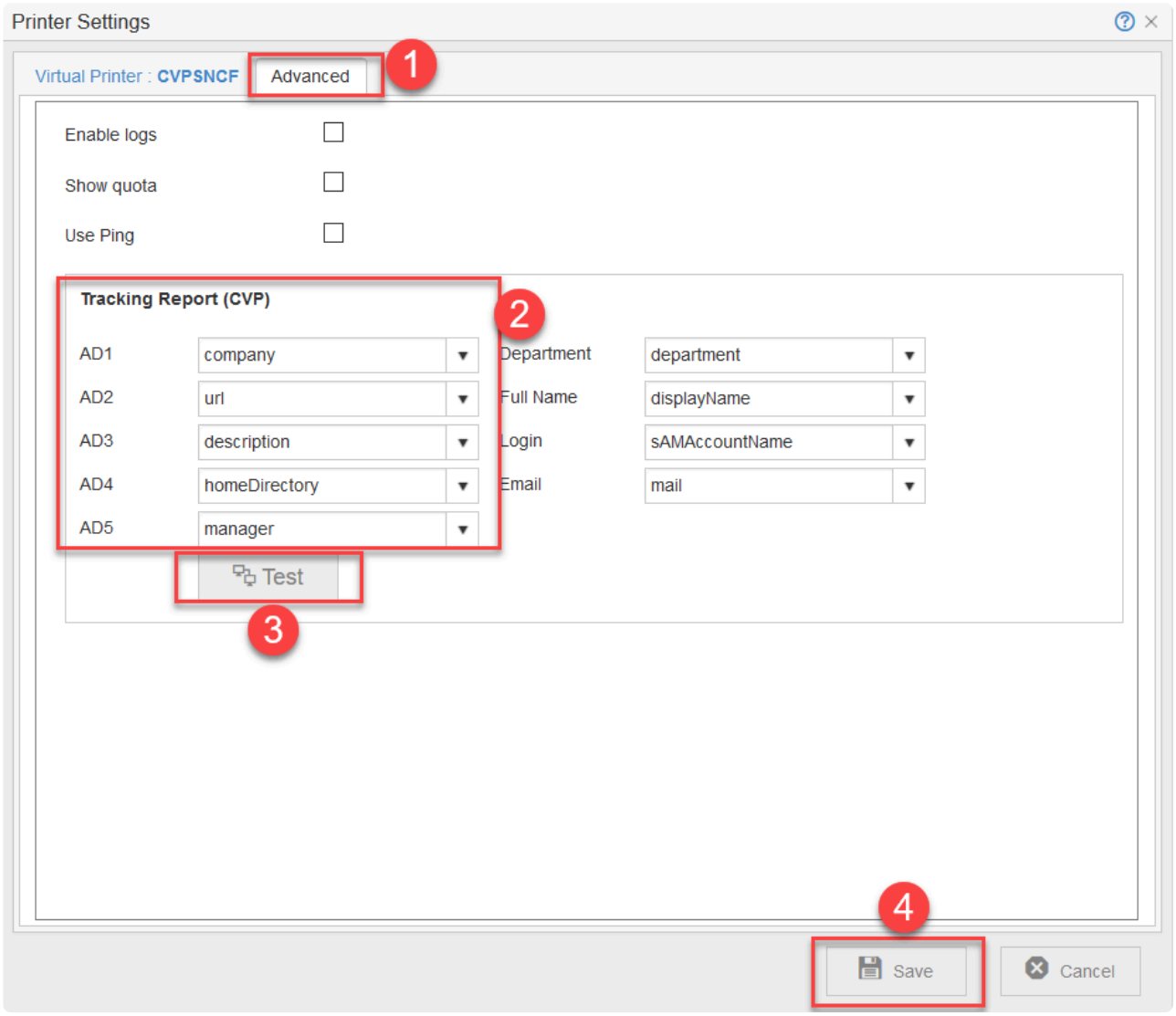


3. Click **Save**.

Configure the information gathered for the tracking by the Celiveo Virtual Printer

> ! After upgrading the CVP, the Department, Full Name, Login and Email fields are reset and a value needs to be selected again for these fields.

1. In the Celiveo Virtual Printer settings, select the *Advanced *tab.
2. In the **Tracking Report (CVP)** section, select or enter an attribute in the **AD1, AD2, AD3, AD4** and/or **AD5** drop-down lists.
3. Click the **Test** button to check these attributes against the configured LDAP.



4. Click **Save**.

Last modified: 29 September 2022

15. Celiveo.me

What is Celiveo.me?

Celiveo.me (Mobile Extension) is a SaaS cloud service from Celiveo that enables users to send documents for Pull Printing from any email sending capable device and Chromebook Enterprise laptops, all fully secured.
Celiveo.me is built around Zero Trust architecture, it seamlessly and securely interfaces the cloud services that verify user identity and intake user documents sent by email with the customer on-premise infrastructure with a dedicated Celiveo Mobile Extension enabled Celiveo Shared Virtual Printer that receives these documents, securely stores them and makes them available for release on any Celiveo enabled printer.

Celiveo.me Zero Trust Architecture

Print via Email

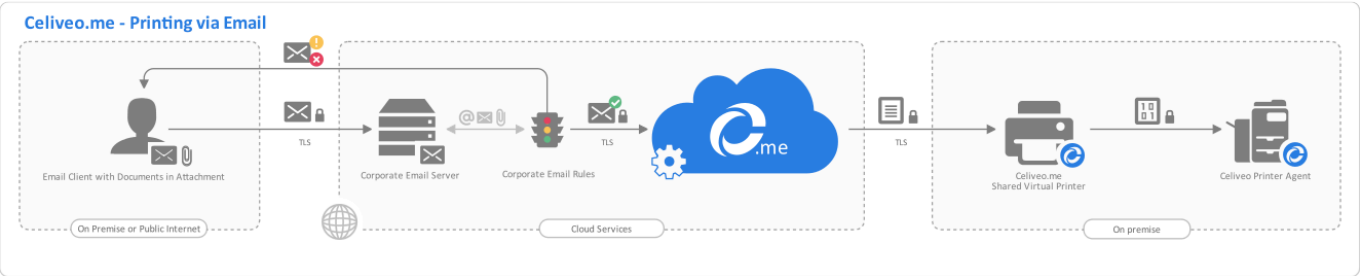
This feature allows users to submit documents to pull print as email attachments and can be done from any email client in any Operating System.

1. These documents are sent to a corporate email address created by the customer e.g. celiveome@company.com
2. This email inbox then applies all the corporate policies to validate anti-spoofing, email forwarding, file size limit 25MB and other corporate rules.
3. The email is then redirected to a unique and automatically generated email address by Celiveo.me that is provided when subscribing to the product and shown in the Celiveo Mobile Extension enabled Celiveo Virtual Printer. e.g. CVOME9848418115730863957.2@region.celiveo.me

Supported File Types

- pdf, doc, docx, xls, xlsm, xlsx, pps, ppsx, ppt, pptx ,odp, ods, odt (unprotected)
- epub, eml, msg, htm, html, md, tif, tiff

Architecture

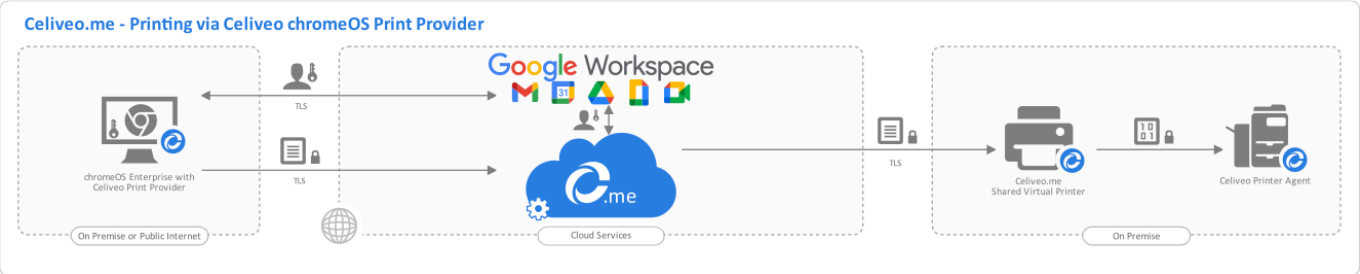


Print via Celiveo ChromeOS Print Provider

This feature aims to natively perform pull print from chromeOS Enterprise in a secure and seamless fashion using the built-in TPM chip and Google User Validation Services to avoid user identity and

password input.
The Celiveo.me Print Provider is installed to manage chromeOS Enterprise devices using ChromeOS Device Management that defines which users will get Celiveo.me Print Provider deployed.
Once installed, users can print from any printing capable application by going to **File > Print > Select Celiveo.me Print Provider > Print**.

Architecture

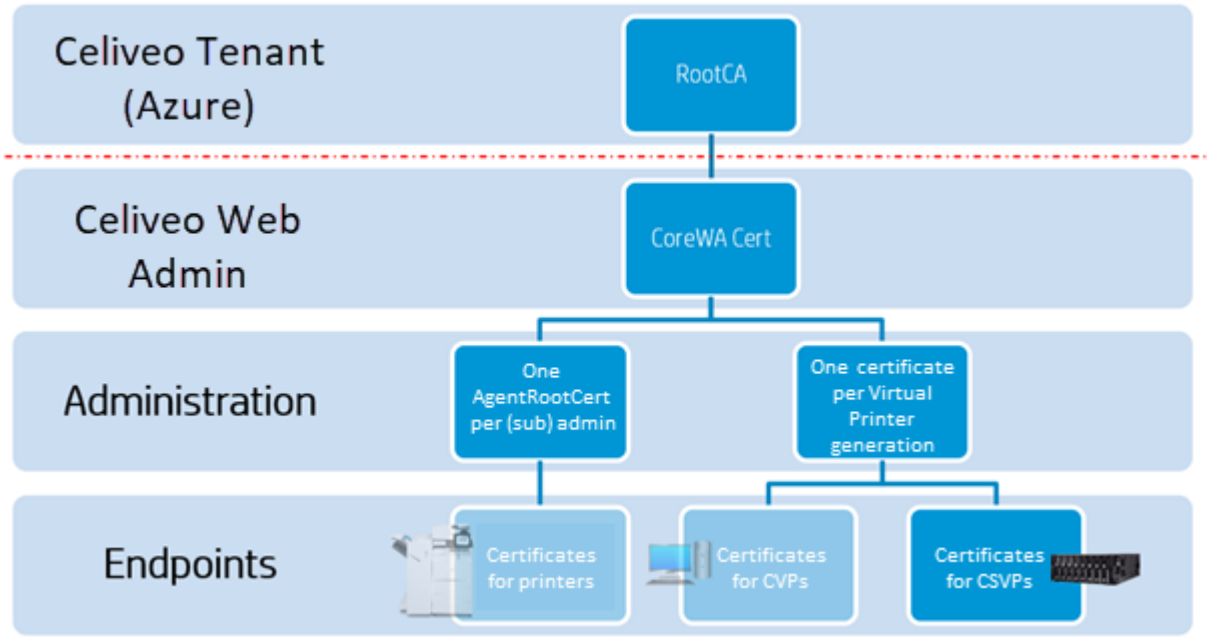


Service Scalability

Each Celiveo.me enabled CSVP has an estimated bandwidth to process 60 documents per minute and the processing throughput is shared by both email and chromeOS Print Provider connectors.
Additional Celiveo.me enabled CSVP can be added to increase processing throughput up to 20 CSVPs.
When the Celiveo.me enabled CSVP reaches the processing limit documents are not lost, they remain in the queue and are processed as other documents leave the processing queue to storage. If documents take longer to show in the printer front panel additional Celiveo.me enabled CSVP might be required to improve the overall user experience.

Zero Trust Access

Celiveo 8 uses a 4-levels certificate chain that protects the Web Admin, the CSVP endpoints – shared print queues – and the Cloud. This protection will be extended to Celiveo agents Celiveo for printers and to CVPs (Serverless) in 2022.
The Celiveo company only has Root CA (level 1) and chain public certificates.
The level 2 certificate is generated with a long random key, never stored at Celiveo, and immediately transferred in an encrypted form by email to the admin defined in the use license.
During the configuration of the Celiveo Shared Virtual Printer CSVP, a new level 4 certificate is generated with an encrypted PFX. Its key is displayed on screen for the last time and will be required during the CSVP installation on the Windows Print Server. This CSVP public key is stored in the installation SQL database and transferred to the Celiveo.me Cloud for this print queue.



Last modified: 29 September 2022

15.1. Zero Trust Activation

This article focuses on activating the Zero trust for Celiveo 8. For more detailed information on what is Zero Trust, please visit this chapter.

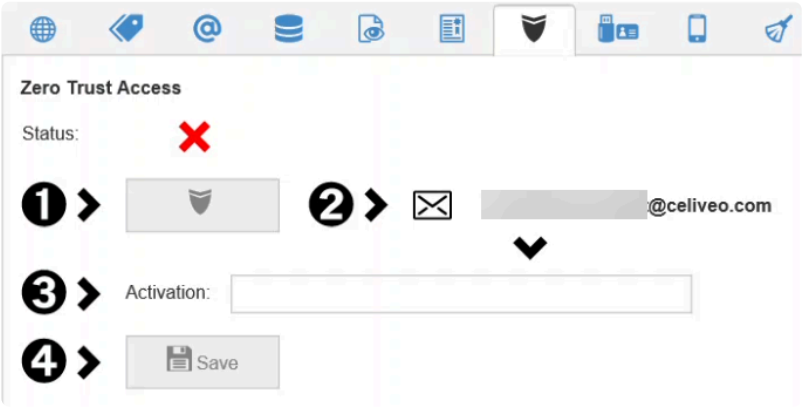
Requirements

In order to be able to use the Zero trust architecture, you first need to have it activated in the license.

How to activate

Once you have opened the Web Admin, navigate to the WA settings, and click on the Zero Trust icon

Here is what this tab looks like

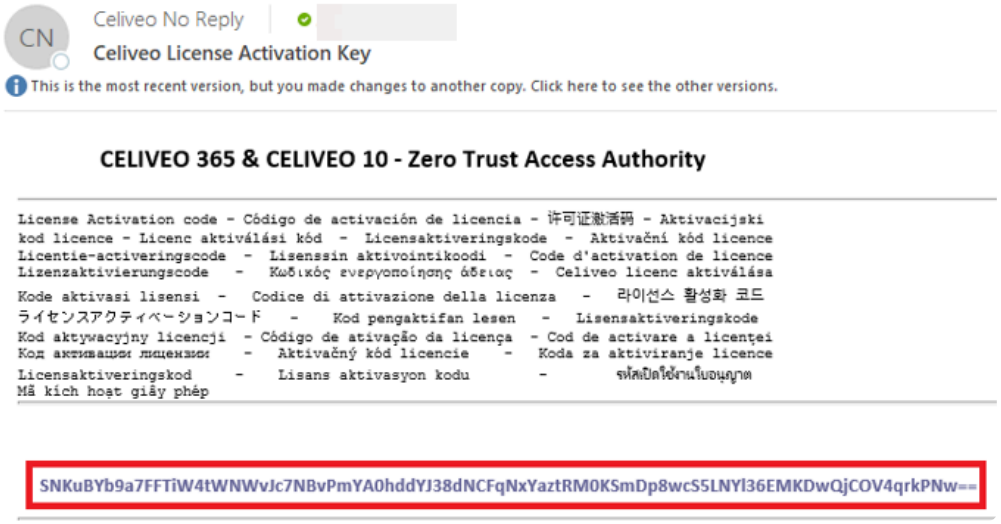


You can see the status of the Zero Trust and the steps to follow to start the activation.
The email address showing is the one the Zero Trust key will be sent to once you start the process.

> ! It is very important to contact CELIVEO if the email is wrong. Do not start the activation as it can only be done only once, for security reasons!

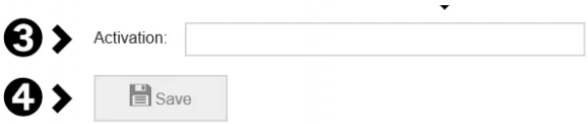
Once you are ready to begin the process, click on the first icon.

By doing so, an email will be sent to the email address specified in step 2.
This email will contain the key to use to activate Zero Trust.

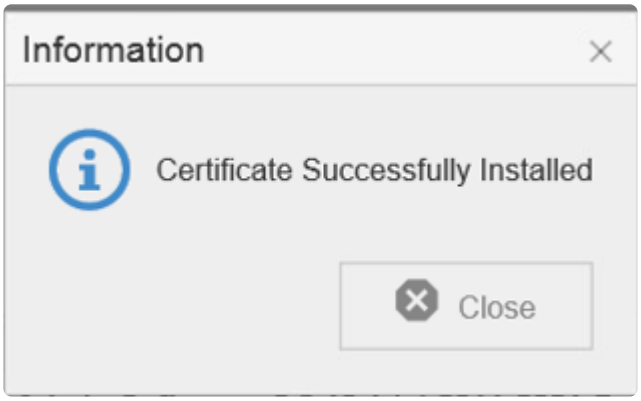


This key should be saved in a secure environment, as it will be generated only once, and only the receiver has it (CELIVEO cannot access or recreate it).
It will be used in the future to reactivate Zero Trust in case of a reinstallation of the Web Admin.

Finally, input the key into step 3 and click **Save**.



Zero Trust is now activated.



Last modified: 29 September 2022

15.2. Creation and installation of a Celiveo Shared Virtual Printer

The Celiveo mobile extension (Celiveo.me) is used for Celiveo integration with Chromebook but also for mobile printing.

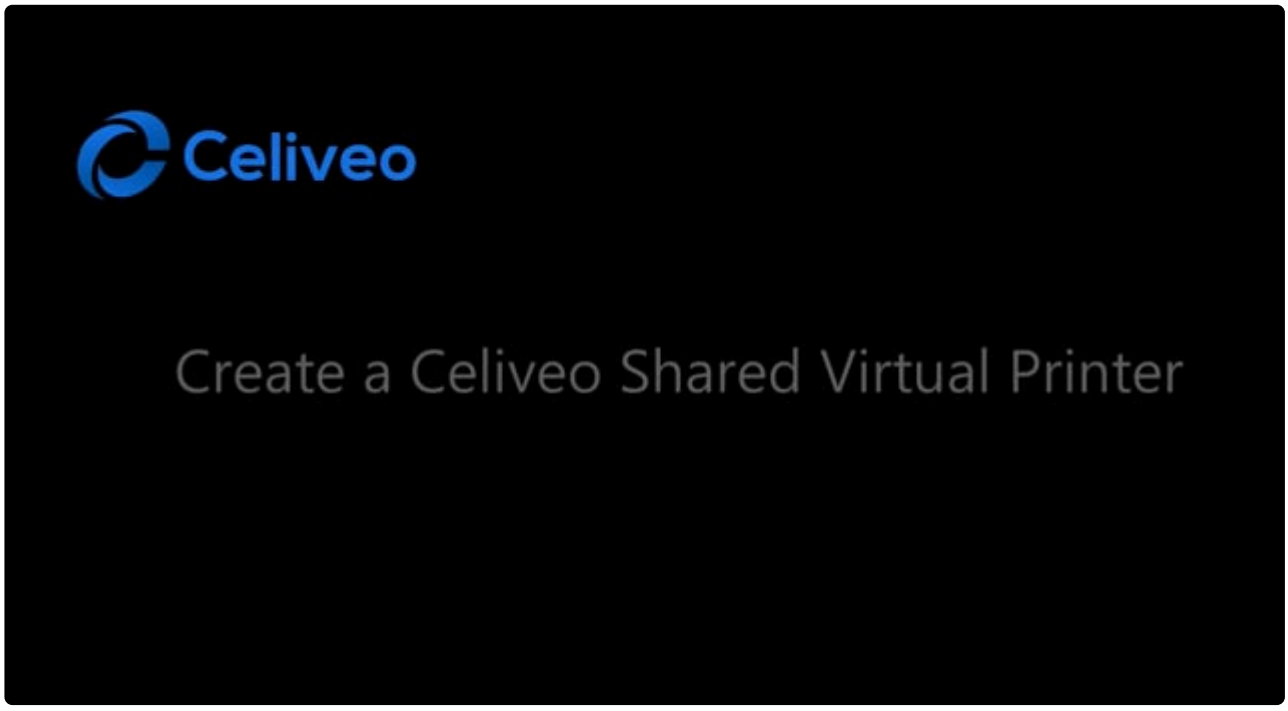
There are two prerequisites:

- An outgoing connection to https://*.celiveo.me:443 needs to be open. This will allow the CSVP to contact our cloud services and download the jobs files.
- Having the Zero Trust architecture activated.

This article focuses on the creation of the Celiveo.me CSVP and its installation on a print server.

Creation of the Celiveo.me CSVP

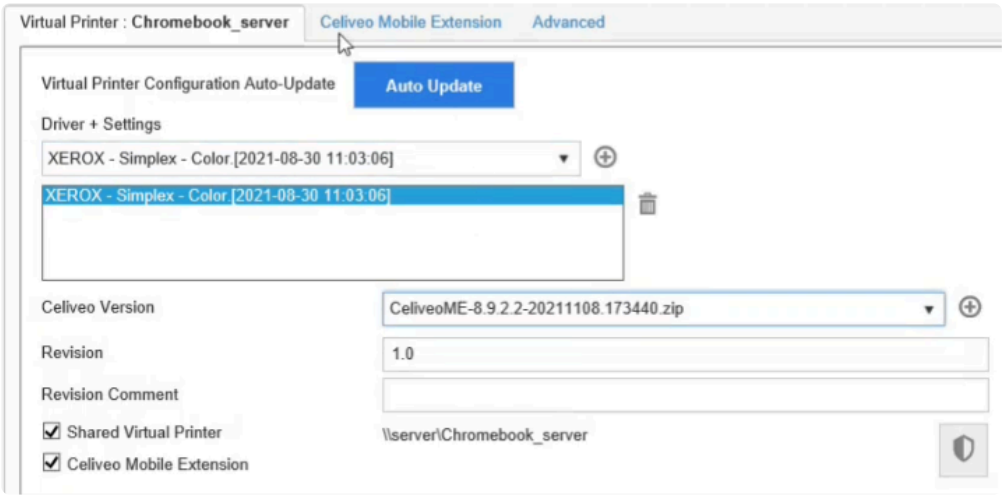
Watch the process in the following video:



https://player.vimeo.com/video/652803959

First, create a CSVP.
To do so, click on the virtual printer creation wizard.

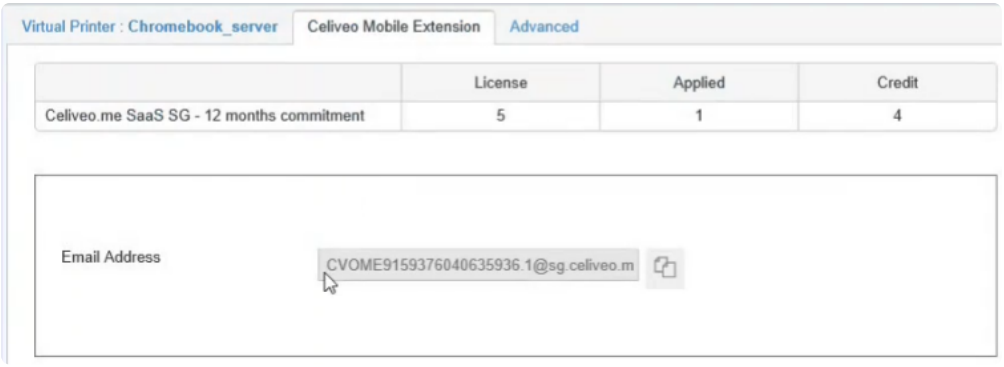
Choose the name of your virtual printer and click **Next**.



On the next page:

- Select the driver to use.
- Select* Shared virtual printer* and **Celiveo mobile extension**.
- In the **Celiveo version** drop-down list, select the Celiveo.me package.

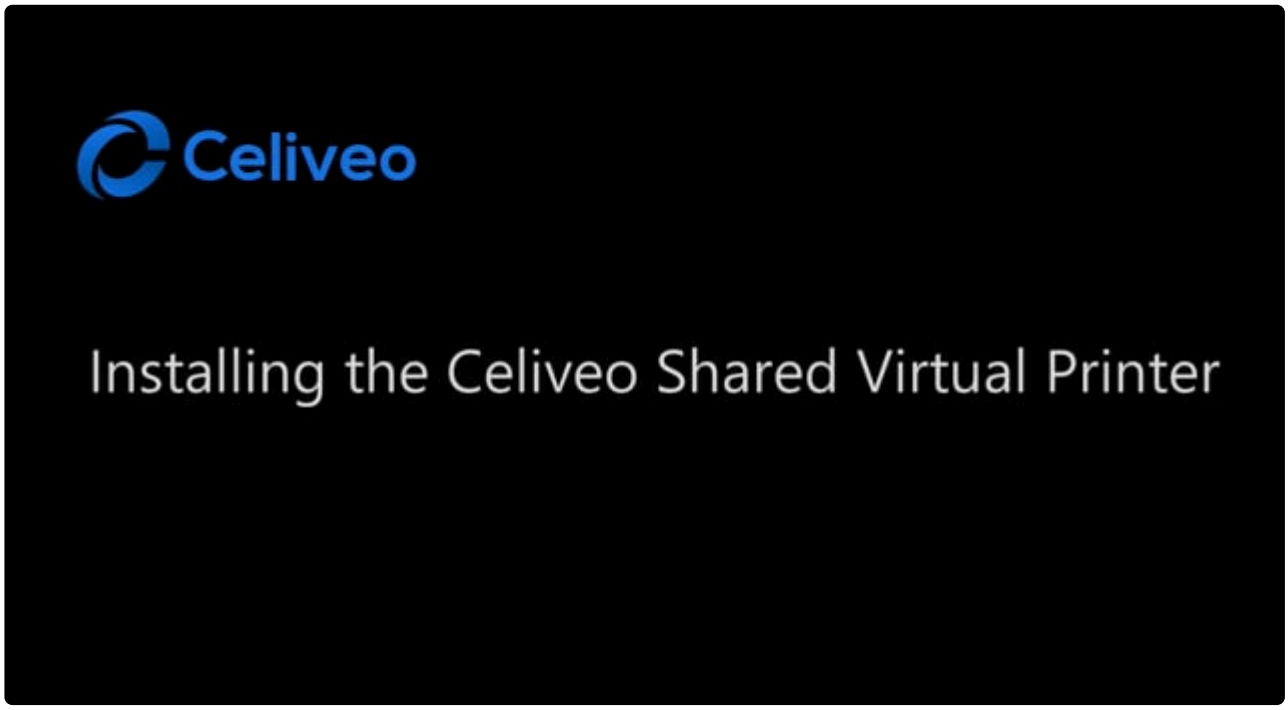
The **Celiveo mobile extension** tab appears



It shows the number of licenses, how many have already been used, and how many are still available.
The number of licenses indicates how many CSVP can be created with the mobile extension.
The email address is an address associated with this CSVP, in our cloud services, where the print jobs will be sent.
It will be used later with mobile printing.
The next steps of the wizard let you set up the printing rules and the cost profiles.
At the end of the wizard, the “certificate password” is delivered.
This password needs to be securely saved as it will only be displayed once. It will be used to install the CSVP on a print server.

Once saved, click the **Test** button to make sure the CSVP is working properly.
Once the test is successful, save and download the new CSVP.

Installation of the CSVP



https://player.vimeo.com/video/652803974

To install the Celiveo.me CSVP, place the downloaded package on your print server and unzip it. This folder contains all the required certificates and installation files.
Open the command-line tool and navigate to this folder.
To start the installation, launch the “installer.exe” application with the parameter “-ztapwd=” followed by the certificate password you previously saved.

Last modified: 29 September 2022

15.3. Chromebook Printing

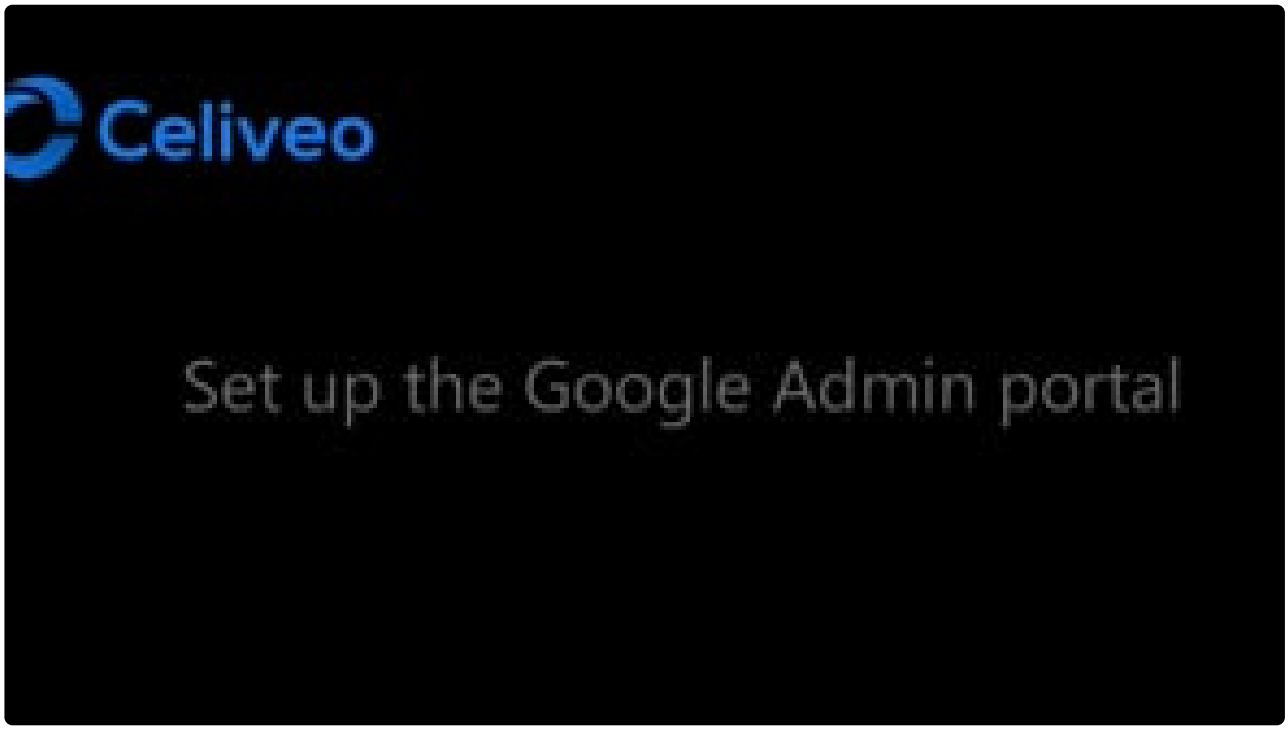
The Celiveo.me extension can be used alongside Chromebooks for printing.
Some settings have to be applied first in the Google Administration Portal.

In this article, we will see how to set up the Google Administration part and make an example of how the printing is done on the Chromebook side.

Requirements

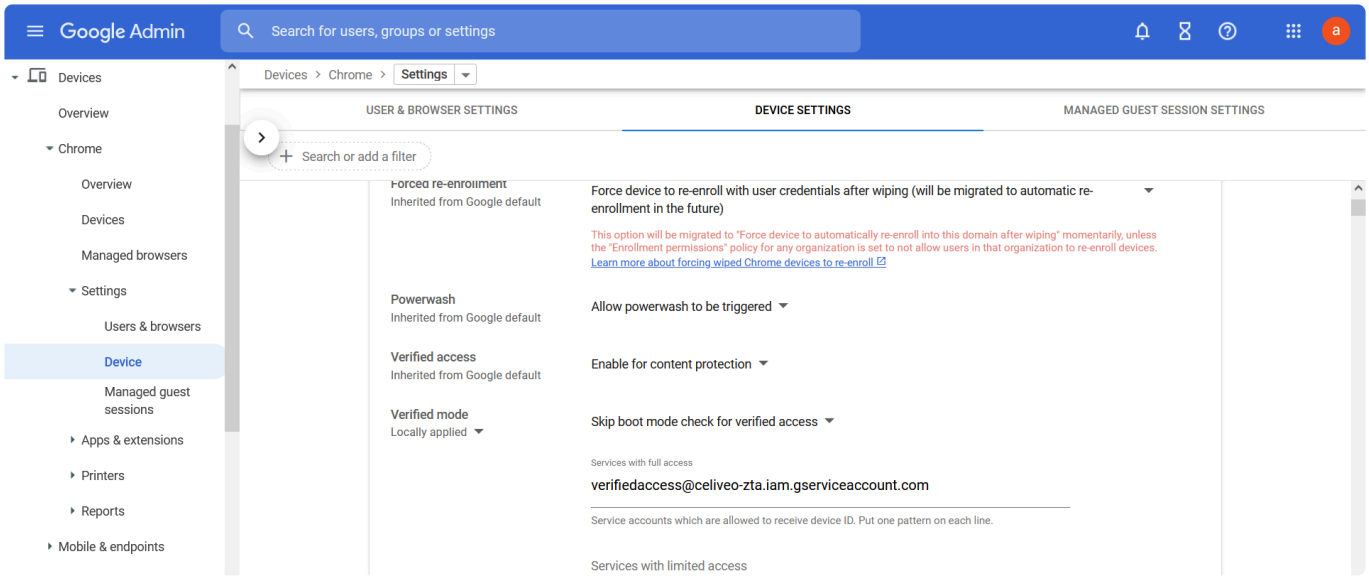
- Zero Trust activated
- A print server with the Celiveo.me CVSP installed

Google administration portal



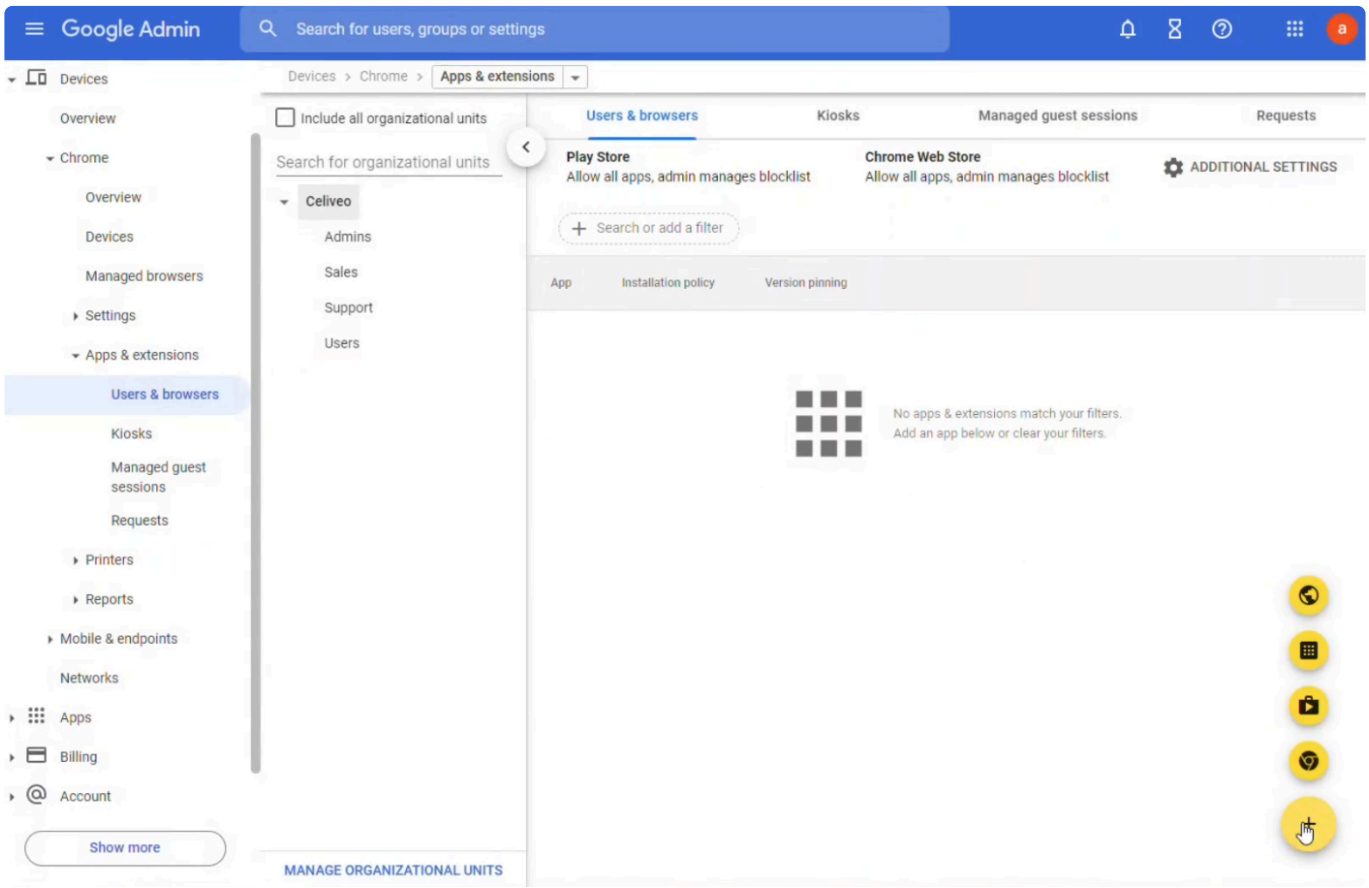
https://player.vimeo.com/video/652803997

Everything takes place on the website: admin.google.com
Log in with your Google Admin account and navigate to the menu **Devices / Chrome / Settings / Device**.

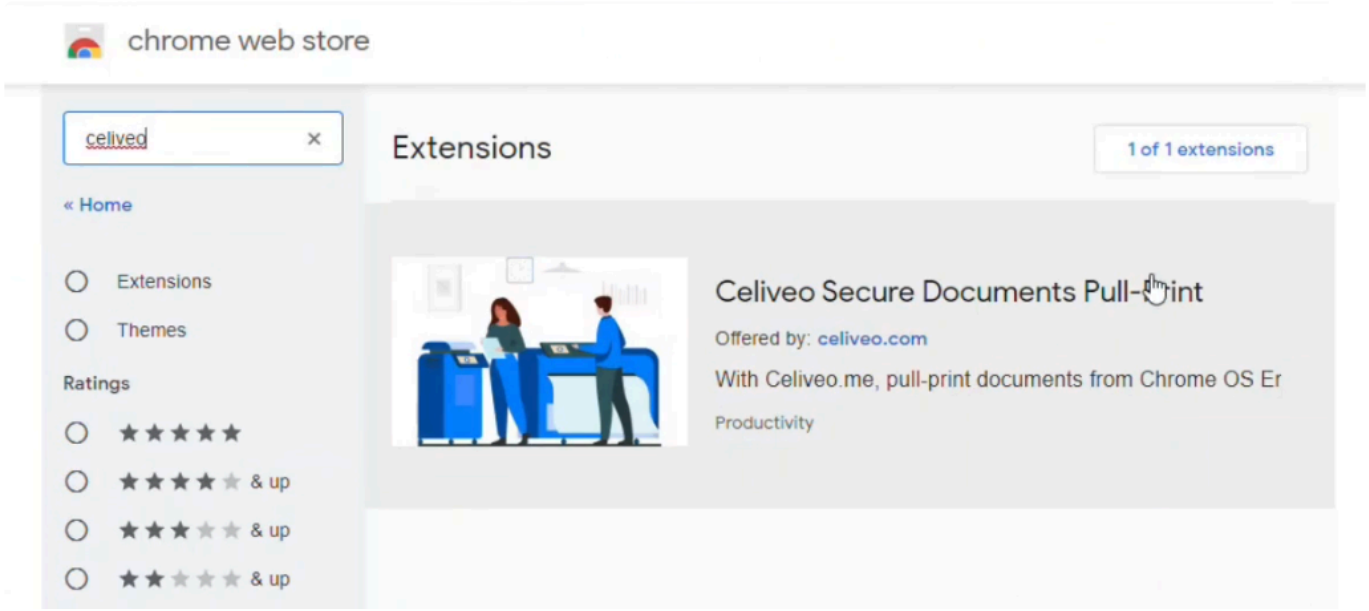


There, under **Verified Access**, add the Celiveo service account: verifiedaccess@celiveo-zta.iam.gserviceaccount.com
By doing so, you will allow the Celiveo.me cloud services to verify the users' identity.

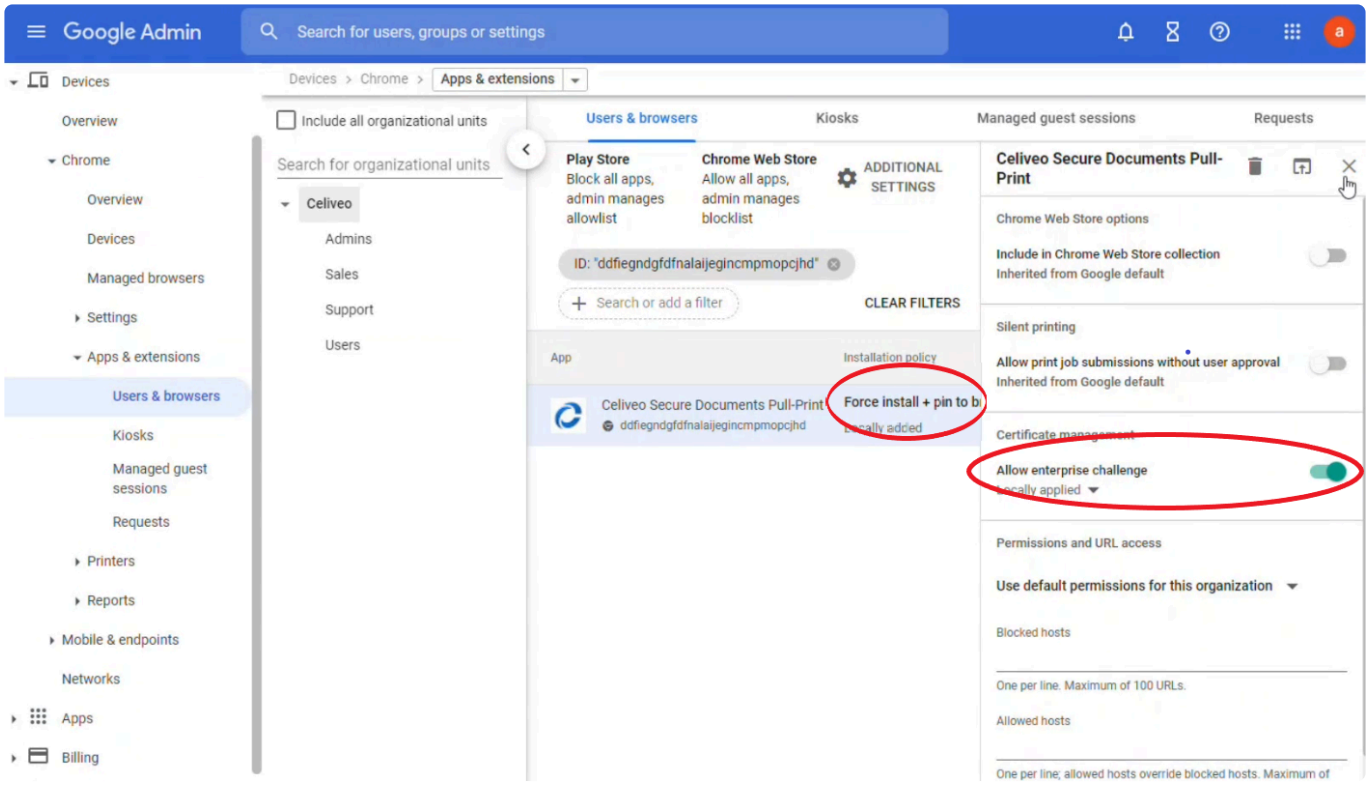
Once done, go to **Devices / Chrome / Apps&extensions / Users and Browers**, to install the **Celiveo Secure Documents Pull Print** extension:
Click the + button, and select **Add from Chrome Web Store**.



In the Chrome Web Store, search for the **Celiveo Secure Documents Pull Print** extension:

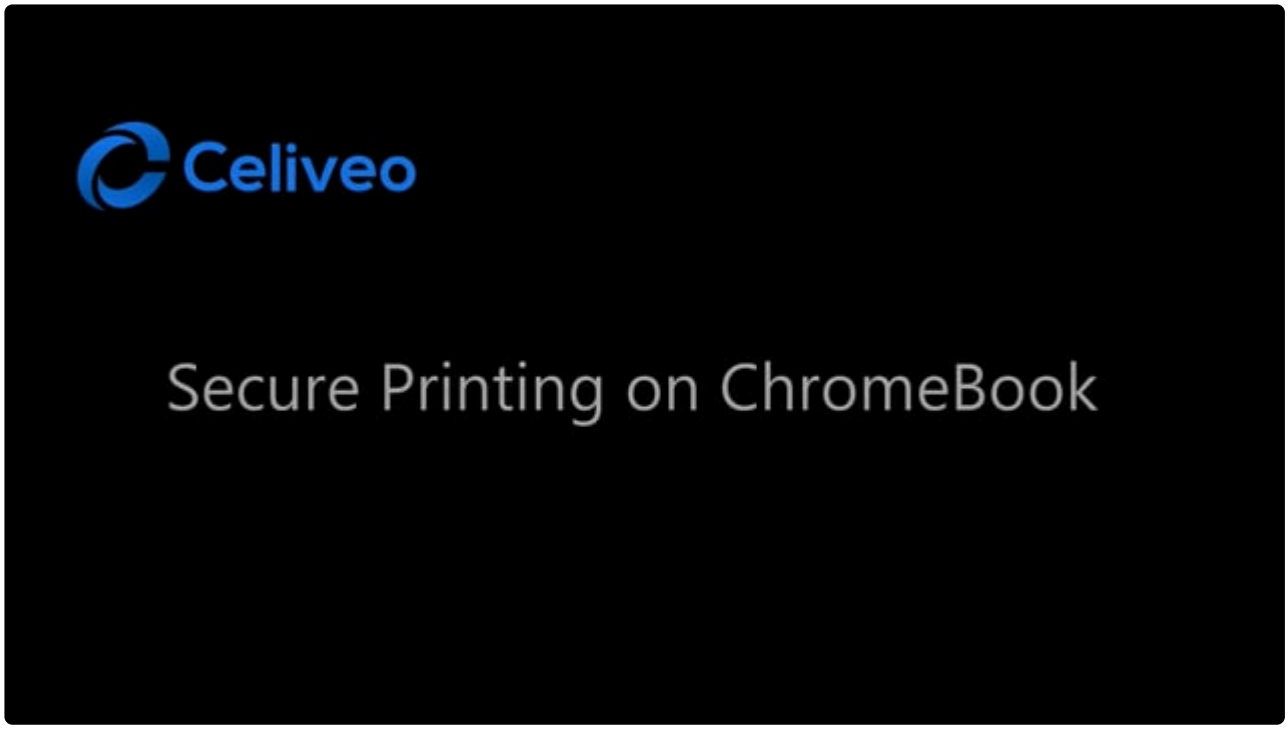


Add this extension to the administration portal by clicking **Select**.



Once added, select **Allow enterprise challenge** and **Force install + pin to taskbar**, as shown in the image above.
Your Chromebook users will now be able to print with their Chromebook using Celiveo secure printing.

The following video shows the printing from a user's point of view:



https://player.vimeo.com/video/652804017

Last modified: 29 September 2022

15.4. Mobile Printing

The Celiveo mobile extension can be used for mobile printing.

Requirements

- Zero Trust activated
- A print server with the Celiveo.me CVSP already installed

How does it work?

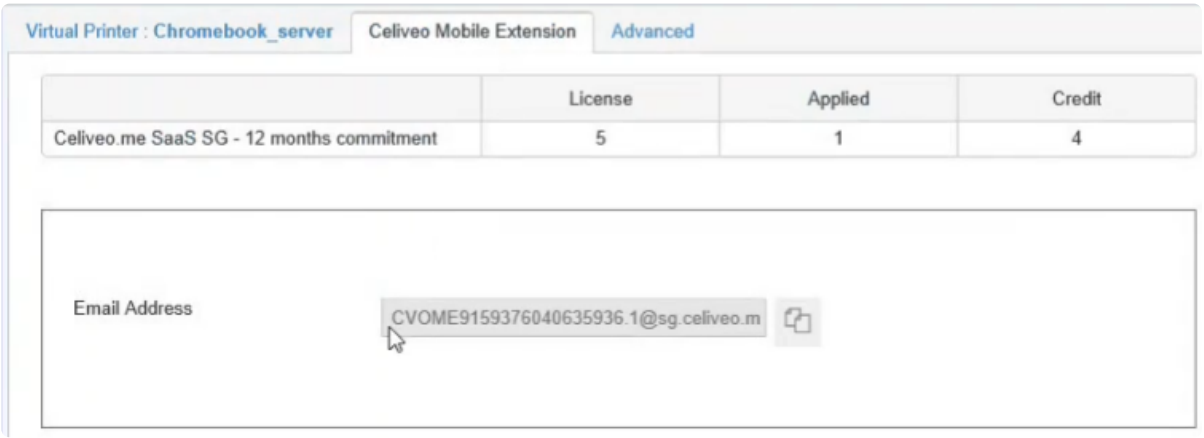
Mobile printing is the ability for anyone in the company to send documents to be printed on a corporate printer.

1. The user has a PDF file on his phone to print
2. He opens his corporate email and sends the file to an email address reserved for printing
3. He goes toward any printer in the company and connects with his credentials (or pin code/card)
4. He locates his job and prints them

Any type of document is supported.

Set up mobile printing

When the print administrator set up the Celiveo.me CSVP, an email address was displayed during the creation. If not saved, this email is available in the Web Admin CSVP settings:



This email address is the place in the Celiveo cloud services where the jobs are stored while waiting for the Celiveo.me CSVP to retrieve them.
Any job sent to this address will be retrieved by the CSVP. Because of the complexity of this email format, it is recommended to set up a corporate email that will redirect all emails to the celiveo.me address.
This way, rules can be applied to restrict the types of documents that can be printed and which email addresses can send print jobs… (according to corporate rules).
To set up those rules, you can follow this article as an example.

Last modified: 29 September 2022

15.4.1. Office 365 Email Rules

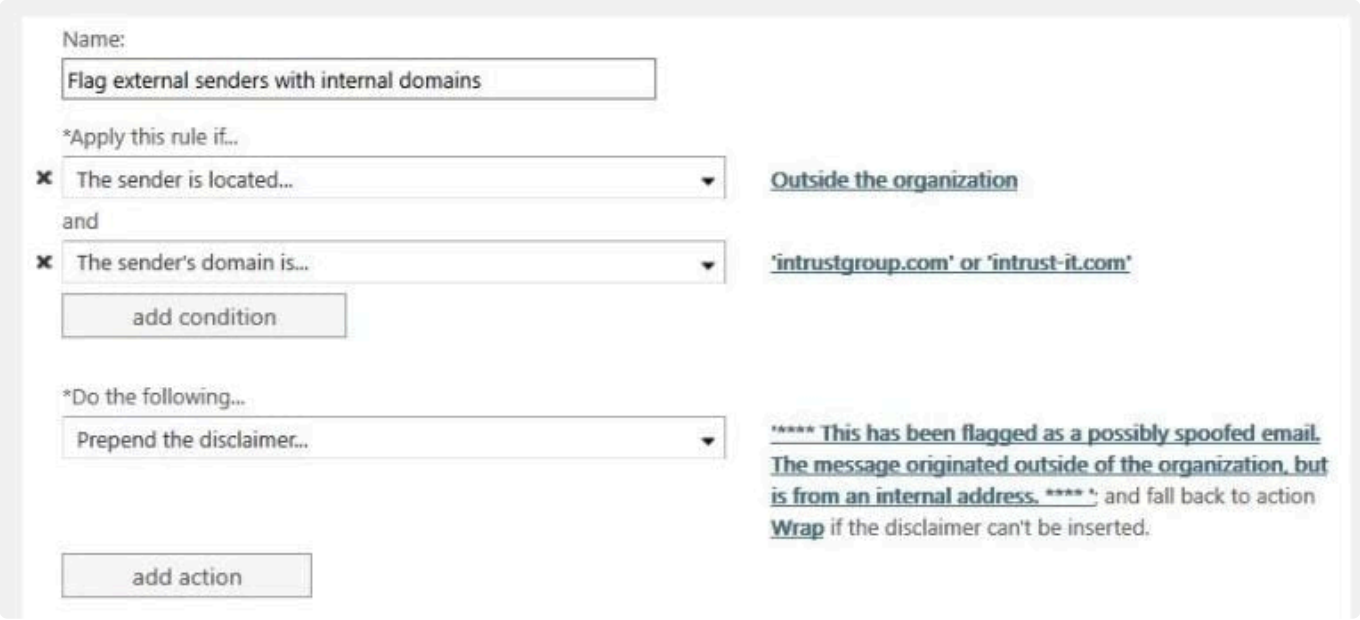
What are Office 365 Email Rules?

Email Rules are an important part of the configuration process as it allow the customer to enforce corporate email rules and other rules that are important to guarantee security flow between the Office 365 and celiveo.me.

Configuring Office 365 Email Rules

Anti-Spoofing

1. Log into the **Office 365 management portal**.
2. Open **Exchange Admin Center**.
3. Go to **Mail Flow** > **Rules**.
4. Create a new rule if the sender is outside the organization and if the sender's domain is one of your internal domains. Set the condition to Prepend the disclaimer and write a disclaimer explaining why the email is flagged as a spoofed email. See example below.



This Office 365 Anti-Spoofing Rule may add the disclaimer to emails from devices such as scanners and third-party services like Constant Contact. To set up your rule to not add the disclaimer to these:

1. Click the **add exception** button in the rule.
2. Specify the **sender**.

External Email Forwarding

1. Log into the **Office 365 management portal**.
2. Open **Exchange Admin Center**.
3. Go to **Recipients** > **Mailboxes**.
4. In the list of user mailboxes, click the mailbox that you want to configure mail forwarding for. A display pane is shown for the selected user mailbox.
5. Under **Mailbox settings** > **Mail flow settings**, click the **Manage mail flow settings** link.
6. In the Manage mail flow settings display pane, you will see the **Email forwarding option**. Click the *Edit *button next to this option to view or change the setting for forwarding email messages.
7. The Manage email forwarding display pane is shown. By default the Forward all emails sent to this mailbox setting is OFF. Turn it ON.
8. Under Forwarding address text box, enter the forwarding email address. The text box allows a search option for searching email addresses by partially entering the keyword.
9. You can turn ON the Keep a copy of forwarded email in this mailbox option if you wish to keep a copy of the forwarded email.
10. Click **Save** to save your changes. Click **Close** to exit from the Manage mail flow settings display pane.

Last modified: 29 September 2022

16. Celiveo Print-Web

Celiveo® Print-Web comes as an option of Celiveo Enterprise and offers a mobile print software solution that installs in minutes, inside the customers private network, and lets users print from any smartphone, tablet, or mobile computer with extreme ease.

Last modified: 29 September 2022

16.1. Celiveo Print-Web Installation Guide

Celiveo Print-Web Installation Guide

Last modified: 29 September 2022

16.2. Celiveo Print-Web Mobile Gateway Installation Guide

Celiveo Print-Web Mobile Gateway Installation Guide

Last modified: 29 September 2022

17. Technical Information

This topic details advanced technical information useful to get the best out of your Celiveo solution.

Quick and Easy Solution to Disable SSL/ Early TLS Protocols and Enforce TLS 1.2
Managing 32 bit and 64 bit Architectures
Environmental Impacts of Printing – Formulae used in TGS 10 reports
Pushing Print Jobs to Network Attached Storage
Celiveo WebAdmin Tools and API
Open Source codes used in Celiveo 8
Migration Support to Celiveo 8 Versions

Last modified: 29 September 2022

17.1. Celiveo Smart Appliance

Celiveo adds its intelligence to the printers other than HP FutureSmart and Ricoh SOP through a tiny Celiveo Smart Appliance connected to the network port behind the printer.

Celiveo provides the following services on those printers:

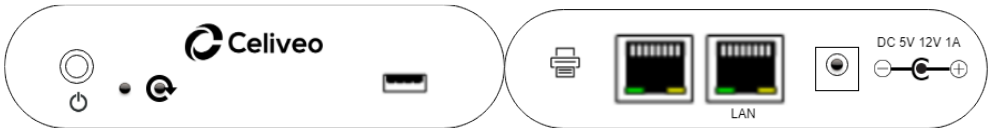
- User authentication for pull printing
- Pull printing with instant print jobs release upon badge or PIN authentication
- Tracking and reporting of pull print jobs

Celiveo Smart Appliance
Setup Celiveo Authentication Hardware
How to upgrade the Celiveo Version on CSA and Embedded Agents
Understanding CSA LED Flashing Behaviors

Last modified: 29 September 2022

17.1.1. Celiveo Smart Appliance (CSA)

Connectors



Connector		Description
Power switch		Power ON/OFF. **Needs to be pressed continuously until the CSA switches On or Off.**
USB port		(Optional) Connect a Celiveo authentication hardware such as a card reader to the USB port.
Reset Button (Pinhole)		Re-initialize the CSA
Printer port		Connect the supplied network cable from the CSA to the printer.
Network port		Connect a network cable from the CSA to the local network.
Power supply		Connect the supplied USB power cable from the CSA to the USB port on the printer.

Specifications

MEASUREMENTS	
Size	25 mm x 77 mm x 118 mm / 0.98” × 3.03” × 3.98”

Weight	160g / 0.35lbs
Case	Aluminum
Color	Silver/Black
Power Source	DC Jack
Ethernet port	2 x RJ45
Power	5V / 9V / 12DC
Certification	CE, FCC, IC, EAC
Compliance	REACH, RoHS

Note: Electrostatic Discharges (ESD) will not damage the Celiveo Smart Appliance but may reboot in case of very high intensity.

> ! **Important**: To switch on/off the CSA, press the Power button until the CSA switches on/off.

Powering the CSA

Powered by the Printer USB Connector

- Short cable to power from Printer USB.
- 5v USB power is necessary.
- No need for external power supply.
- No extra wall plug required.
- CSA is OFF when printer is OFF.
- CSA needs up to 120s to boot.

Powered by an external power supply

- 5 to 12v 2A external power supply.
- C14 output, wall cable (supplied upon demand based on geography)
- CSA is not OFF when printer is OFF.
- Spare wall plug required.

Network Settings

By default, the CSA is set in DHCP mode. You can also opt for fixed IP network settings.

Configure DHCP IP network settings through USB

1. Create a configuration file with the entry below. Save the file as ***ipsetup.conf*** file.

```
Remove any spaces in the configuration entries or the configuration file w
```

```
ill not work.
```

DHCPIP Fixed IP
MASK=x.x.x.x Subnet Mask

2. Format the USB flash drive to FAT32.
3. Copy the ipsetup.conf file to the USB flash drive.
4. Switch off the Celiveo Smart Appliance (CSA).
5. Connect the USB flash drive with the ***ipsetup.conf*** file to the CSA.
6. Switch on the CSA. The configuration file is automatically installed on the CSA.
7. Once the configuration completes, the LED on the CSA changes to a steady green light.
8. Remove the USB flash drive.

Configure Fixed IP network settings through USB

The fixed IP network settings are configured by providing the details in the ipsetup.conf configuration file.

1. Create a configuration file with the entries below. Save the file as ***ipsetup.conf*** file.

```
Remove any spaces in the configuration entries or the configuration file w
ill not work.
```

FIP=x.x.x.x Fixed IP
MASK=x.x.x.x Subnet mask
GATEWAY=x.x.x.x Gateway
PRI_DNS=x.x.x.x Primary DNS server IP
SEC_DNS=x.x.x.x Secondary DNS server IP
NTP_SERVER=x.x.x.x IP or hostname
SEARCH_DOMAIN=< value >

2. Format the USB flash drive to FAT32.
3. Copy the ipsetup.conf file to the USB flash drive.
4. Switch off the Celiveo Smart Appliance (CSA).
5. Connect the USB flash drive with the ***ipsetup.conf*** file to the CSA.
6. Switch on the CSA. The configuration file is automatically installed on the CSA.
7. Once the configuration completes, the LED on the CSA changes to a steady green light.
8. Remove the USB flash drive.

Last modified: 29 September 2022

17.1.2. Setup Celiveo Authentication Hardware

Celiveo Authentication Hardware refers to the card readers that are used to authenticate users at the device.

These card readers are supported:

- Proximity card reader
- Smart card reader
- Swipe card reader

Note: For up-to-date information on supported devices, visit https://www.celiveo.com

Connecting Celiveo Authentication Hardware to the printer device

Celiveo Authentication Hardware, such as card readers, can be connected to the devices in two ways:

- Connect to the Celiveo Smart Appliance, or
- Connect directly to the device.

Connect to Celiveo Smart Appliance

1. Connect a crossover fast Ethernet cable from the Celiveo Smart Appliance to the device.
2. Connect a USB cable from the Celiveo Smart Appliance to the Celiveo Authentication Hardware (external card reader).

For installation of the Celiveo Smart Appliance, see the article How to install the Celiveo Hardware.

Connect to device

The Celiveo Authentication Hardware can be connected to a device as an external card reader using the USB port. If the device has only one USB port, a USB hub can be used to connect both the smart card and proximity card reader. Before you Switch on the device, make sure both the Celiveo Authentication Hardware and reader are connected to the device.

Connect the external Celiveo Authentication Hardware through USB

Connect the Celiveo Authentication Hardware (external) to a device using the following ways:

1. Attach the back of the Celiveo Authentication to the device with a double-sided adhesive label.

> **Note**: Make sure the adhesive label does not cover the barcode on the back of the Celiveo Authentication Hardware. This information is required for technical support.

2. Use the two supplied adhesive cable brackets to guide the reader's cable from the back of the device to the front.

To connect Celiveo Authentication Hardware

1. Switch off the device and disconnect the power cable.
2. Connect a USB cable from the Celiveo Authentication Hardware to the USB port on the device.
3. Connect the device to the power cable.
4. Switch on the device.

Connecting Celiveo Authentication Hardware (Embedded) using Hardware Integration Pocket (HIP)

HP devices, such as HP FutureSmart devices and Ricoh devices, such as Ricoh SOP G2.x Android printer devices support embedded authentication hardware. The Celiveo Embedded Authentication Hardware is connected to the device in the HIP (Hardware Integration Pocket).

To connect the Celiveo Embedded Authentication Hardware to HP FutureSmart devices:

1. Switch off the device, and detach its power cable.
2. Remove the HIP Cover.
3. Locate the mini-USB slot connector.
4. Attach the Celiveo Embedded Authentication Hardware (mini-USB reader) to the HIP cover.
5. Plug the mini-USB Reader into the mini-USB plug.
6. Mount the HIP cover with the mini-USB reader onto the device.
7. Plug in the device and switch it on.

Last modified: 29 September 2022

17.1.3. How to upgrade the Celiveo Version on CSA and Embedded Agents

The Celiveo Version refers to the Celiveo firmware that runs as embedded on certain printers such as HP FutureSmart or Ricoh Android SOP 2.x MFP or as deployed in Celiveo Smart Appliance (CSA). Typically, the CSA Agent comes pre-loaded with the correct firmware. For printers that run on Embedded Agents, you must explicitly upload the Celiveo Version.

The primary and recommended method of upgrading Celiveo Version is through the Web Admin.

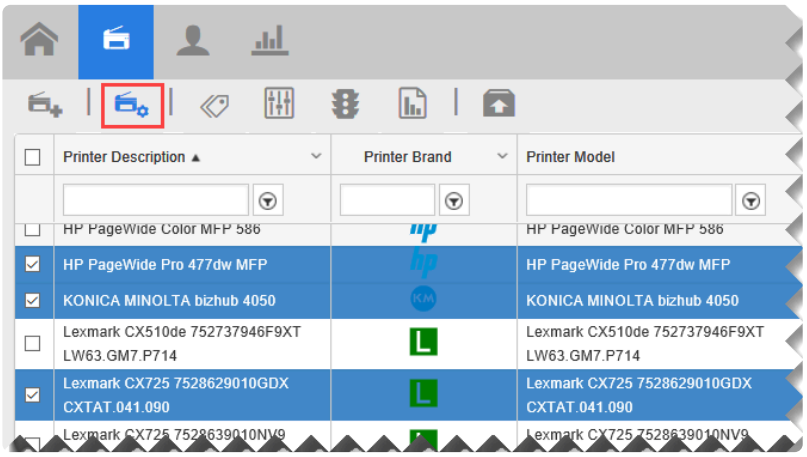
In case of CSA Agent, it can also be upgraded by flashing the firmware files directly to CSA Agent using USB memory stick.

Upgrade Celiveo Version through Web Admin

If you have a new version of the Celiveo firmware and you wish to upgrade it:

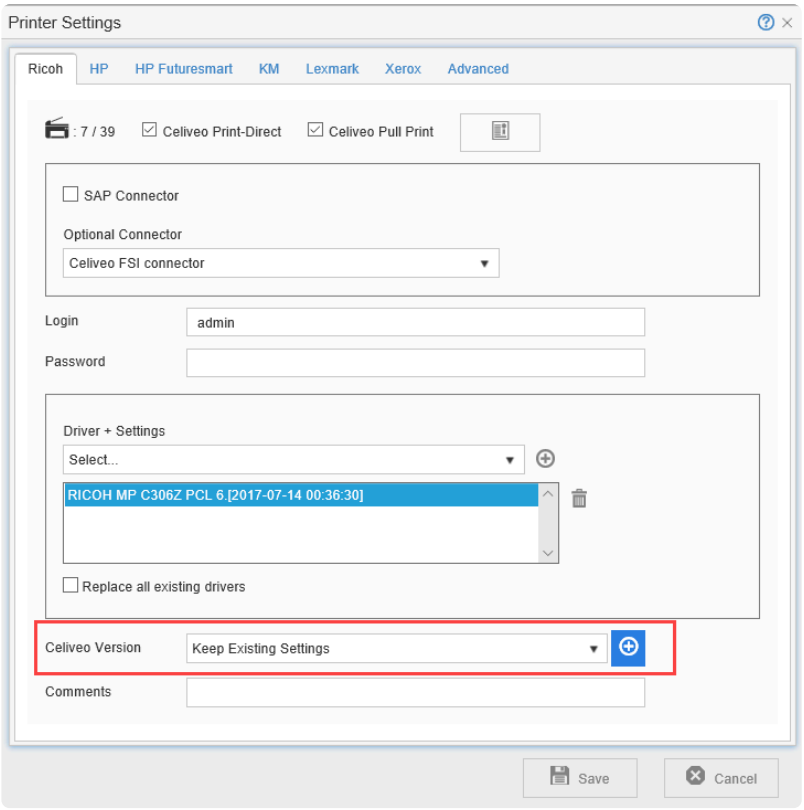
Step 1. Select the printer

1. At the Main menu in Web Admin, click .
2. Select the printer(s) for which you wish to upgrade the Celiveo Version. You may also select different printer types for this purpose.
3. At the Printer menu, click .



Step 2. Upload the Celiveo Version

A tabbed dialog box is displayed, where each printer type has a separate tab. Repeat the instructions below for each tab.



4. Click the **[+]** icon adjacent to the **[Celiveo Version]** drop-down. The Upload Embedded Solution File dialog displays.
5. Click **[Select Files]**.
6. Pick the *.mh/ *.mr/ *.mc/ *.bmc file provided for the printer.

You can download the latest Celiveo Version files from Downloads in the Celiveo Partner Portal.

> **Note**:
> For HP FutureSmart printers, choose the *.mh file.
> For Ricoh Android SOP G2.0 and G2.5 printers, choose the *.mr file.
> For other printers types, you can choose either *.mc or *.bmc file.

Step 3. Finalize

7. Once file is uploaded successfully, Click **[Save]**.
8. Synchronize the printer to upgrade the Celiveo Version on CSA.

> **Important: DO NOT** power off or disconnect the Celiveo Smart Appliance from power when its firmware is being upgraded.

Upgrade Celiveo Version through USB

> **Note**: This method is not applicable for HP FutureSmart printers and Ricoh Android SOP

2.x printers

There are two types of CSA firmware files. You need to flash in the order listed below:

1. OS Image (for example: 8.0.016.0329-SIA8.1_OSI.fw)
2. Celiveo Application file. (for example: 8.0.117.0919-SIA.fw)

To flash the CSA, copy the OSI.fw file to the USB Stick. This contains the OS Image and the Celiveo Application. However, if you only want to flash the Celiveo Application, please only copy the SIA.fw file to the USB Stick.
Follow the below steps for flashing:

1. Format the USB memory stick to FAT32.
2. Copy the firmware files to the root directory of the blank USB memory stick.
3. Switch off the CSA.
4. Insert that memory stick in the USB host port of the CSA.
5. Switch on the CSA. The update begins automatically.
6. LED will blink (around 15-20 minutes for OSI, 5 minutes for Firmware file).
7. Once the update is complete, the LED indicator on the CSA changes to a steady green light.
8. Remove the USB memory stick.

Last modified: 29 September 2022

17.1.4. Understanding CSA LED Flashing Behaviors

The table below describes the different CSA LED Flashing Behaviors to help you understand the meaning of the flashing and identify the potential errors.

Scenario	LED Behavior/Beep Activity
Normal Behavior	
Power on with network	Continous Green LED blinking followed by Red LED blinking and stable. Green LED once the network is established
Celiveo ready state	Steady Green LED
Error	
Power on without network or Network Failure	Continous Green LED blinking followed by Red LED blinking with Beeps
Celiveo Application boot up failure	Continous Green LED Blinking
Other Cases	
Factory Reset Response	Red LED flashing
Synchronization in progress	Green LED blinking followed by stable Green LED

https://player.vimeo.com/video/240127463

https://player.vimeo.com/video/274811409

https://player.vimeo.com/video/274810936

https://player.vimeo.com/video/274811008

https://player.vimeo.com/video/274810975

https://player.vimeo.com/video/240127463

https://player.vimeo.com/video/274811409

https://player.vimeo.com/video/274810936

https://player.vimeo.com/video/274811008

https://player.vimeo.com/video/274810975

https://player.vimeo.com/video/240127463

https://player.vimeo.com/video/274811409

https://player.vimeo.com/video/274810936

https://player.vimeo.com/video/274811008

https://player.vimeo.com/video/274810975

https://player.vimeo.com/video/240127463

https://player.vimeo.com/video/274811409

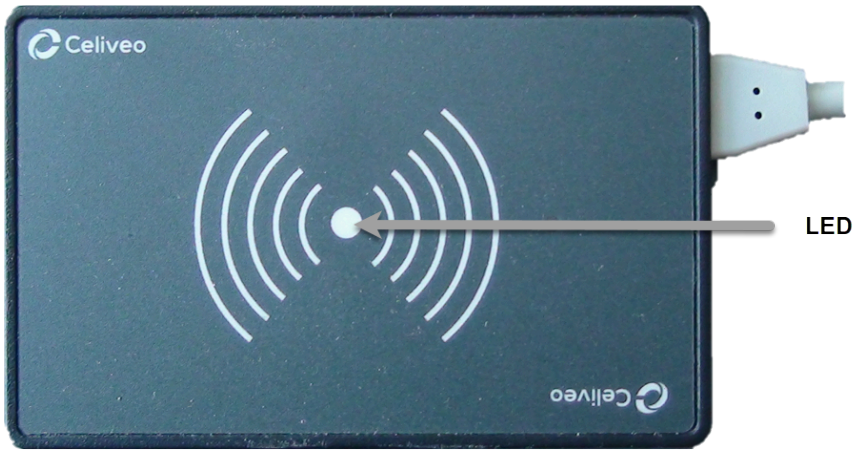
https://player.vimeo.com/video/274810936

https://player.vimeo.com/video/274811008

https://player.vimeo.com/video/274810975

Last modified: 29 September 2022

17.2. Multicard Reader – Specifications for Type A



LED Behavior

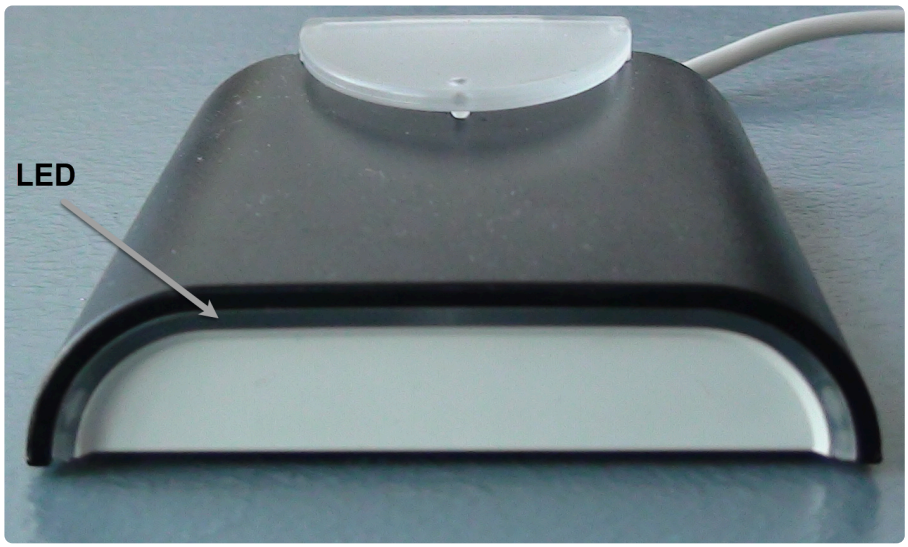
- LED Flashes 3 times: The user does not have any pending job.
- LED Flashes 6 Times: The user is not found\authenticated.

Card Type		
125 Khz	Casi Rusco, EM-Marin, HID Prox, HiTag, Indala, Keri, Nex Watch	
13.56Mhz	HID iCLASS, ISO1569, ISO14443A, Legic, Mifare DesFire	
General Specifications		
Supply Voltage	25ºC	
Recommended USB Operating Voltage	4.35-5.25 VDC	
Operating and Storage Environments		
Operating Temperature Range	-20ºC to +70ºC	
Storage Temperature Range	-30ºC to +80ºC	
Relative Humidity, non-condensing 25ºC:	95%	

Reader Interface Connection	USB Type-A standard / Type-A Mini	
USB Compliance	1.0, 1.0a, 1.1	
Interface		
Visual	Tri Color (LED) - Red, Green & Amber	
Audible	Frequency: 2800 Hz	
Mechanical		
Dimension	53mm x 83mm x 12mm / 2.09” × 3.27” × 0.47”	
Weight	120 grams / 0.265 lbs	
Color	Gray (RAL 7016)	
Electrical Specifications	Current Drain (mA @5VDC)	
	Typical Average	**Max**
Standby Current	1.5 mA	2.5 mA
Configured Current	45 mA	95 mA
Typical Read Height	25.4 mm Typical; Up to 76.2 mm Dependent on Proximity Card type and Environmental Conditions	
Certifications		
Australia & New Zealand	C-Tick	
Canada	ICES	
European Union	CE, RoHS	
USA	FCC	

Last modified: 29 September 2022

17.3. Multicard Reader – Specifications for Type B



LED Behavior

- LED Flashes 3 times: The user does not have any pending job.
- LED Flashes 6 Times: The user is not found\authenticated.

Card Type	
125 Khz	Casi Rusco, HID Prox, Indala Prox
13.56Mhz	HID iCLASS, ISO1569, ISO14443A, Legic, Mifare DesFire,
General Specifications	
Supply Voltage	25ºC
Recommended USB Operating Voltage	4.35 - 5.00 VDC
Operating and Storage Environments	
Operating Temperature Range	0° - 50° C (32° - 122° F)
Storage Temperature Range	20° - 65° C (-4° - 149° F)
Relative Humidity, non-condensing 25ºC:	10 - 90% Relative Humidity
Reader Interface Connection	USB Type-A standard

USB Compliance	1.1, 2.0
Interface	
Visual	Status indicators: Dual color LED Embedded: Green = Ready, Red = Busy External: White = Ready, Blue = Busy
Audible	Frequency: 2800 Hz
Mechanical	
Dimension	66 mm x 55 mm x 9 mm / 2.59” × 2.17” × 0.35”
Weight	14 grams / 0.03 lbs
Color	Black
Electrical Specifications	
Typical Read Height	25.4 mm Typical; Up to 76.2 mm Dependent on Proximity Card type and Environmental Conditions
Certifications	
Canada	ICES
European Union	CE, RoHS (REACH), WEEE
USA	FCC, UL

Last modified: 29 September 2022

17.4. [IMPORTANT] Quick and Easy Solution to Disable SSL/ Early TLS Protocols and Enforce TLS 1.2

IMPORTANT – THIS PROCESS IS MANDATORY TO SUPPORT TLS 1.2 WITHOUT IT CELIVEO WON'T WORK

Note: This is applicable for SecureJet (7.0.5 and higher) and Celiveo (8.0.0 and higher) products. Currently, Celiveo supports TLS 1.2 in HP FutureSmart printers.

According to PCI Security Standards Council, 30 June 2018 is the cutoff date for disabling SSL /early TLS protocols and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS 1.2 is strongly recommended) in order to meet the PCI Data Security Standard (PCI DSS) for secure communication.

Microsoft has released several patches both for Server side (SQL Server) and client side (Machine connecting to SQL Server) to enable TLS 1.2 support.

All the information can be found in the following link: https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server

Process for disabling SSL/ Early TLS protocols and re-configuring CSS/ SSS settings:

1. Update Windows OS:

Make sure that your Windows Server is up to date. Microsoft's latest update provides support for TLS System Default Versions. The Windows Update (mentioned below) enables the use of TLS v1.2 in .NET Framework 3.5 and its higher versions.

To download patch file for:

Windows Server 2012 R2: https://support.microsoft.com/en-us/help/3154520/support-for-tls-system-default-versions-included-in-the-net-framework

Windows Server 2012: https://support.microsoft.com/en-us/help/3154519/support-for-tls-system-default-versions-included-in-the-net-framework

Windows Server 2008 R2: https://support.microsoft.com/en-us/help/3154518/support-for-tls-system-default-versions-included-in-the-net-framework

Windows Server 2016: The following two Microsoft patches are mandatory for TLS 1.2 to be active on Windows Server 2016. The latest versions currently available are as of 2019-07.

- KB4509091 – Servicing Stack Update for Windows Server 2016 for x64-based Systems (SSU) – https://www.catalog.update.microsoft.com/Search.aspx?q=KB4509091
- KB4507460 – Cumulative Update for Windows Server 2016 for x64-based Systems – https://www.catalog.update.microsoft.com/Search.aspx?q=KB4507460

Notes:

- Make sure to restart the system, after installing the patch file.
- If your system is already up to date via Windows Update, then proceed to the next step.

2. Update SQL Server:

1. Refer to the table given in the link https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server to download the correct SQL Server patch.
2. Apply the SQL Server patch accordingly to your version **(Latest SQL Server might not require this step)**.

SQL Server release	First build that supports TLS 1.2	Download link for earlier builds	Additional information
SQL Server 2014 SP1	12.0.4439.1	Cumulative Update 5 for SQL Server 2014 SP1	KB 3052404 FIX: You cannot use the Transport Layer Security protocol version 1.2 to connect to a server that is running SQL Server 2014 or SQL Server 2012
SQL Server 2014 SP1 GDR	12.0.4219.0	SQL Server 2014 SP1 GDR TLS 1.2 Update	
SQL Server 2014 RTM	12.0.2564.0	Cumulative Update 12 for SQL Server 2014	KB 3052404 FIX: You cannot use the Transport Layer Security protocol version 1.2 to connect to a server that is running SQL Server 2014 or SQL Server 2012
SQL Server 2014 RTM GDR	12.0.2271.0	SQL Server 2014 RTM GDR TLS 1.2 Update	
SQL Server 2012 SP3 GDR	11.0.6216.27	SQL Server 2012 SP3 GDR TLS 1.2 Update	
SQL Server 2012 SP3	11.0.6518.0	Cumulative Update 1 for SQL Server 2012 SP3	KB 3052404 FIX: You cannot use the Transport Layer Security protocol version 1.2 to connect to a server that is running SQL Server 2014 or SQL Server 2012
SQL Server 2012 SP2 GDR	11.0.5352.0	SQL Server 2012 SP2 GDR TLS 1.2 Update	
SQL Server 2012 SP2	11.0.5644.2	Cumulative Update 10 for SQL Server 2012 SP2	KB 3052404 FIX: You cannot use the Transport Layer Security protocol version 1.2 to connect to a server that is running SQL Server 2014 or SQL Server 2012
SQL Server 2008 R2 SP3	10.50.6542.0	SQL Server 2008 R2 SP3 TLS 1.2 Update	
SQL Server 2008 R2 SP2 GDR (IA-64 only)	10.50.4047.0	SQL Server 2008 R2 SP2 GDR (IA-64) TLS 1.2 Update	
SQL Server 2008 R2 SP2 (IA-64 only)	10.50.4344.0	SQL Server 2008 R2 SP2 (IA-64) TLS 1.2 Update	
SQL Server 2008 SP4	10.0.6547.0	SQL Server 2008 SP4 TLS 1.2 Update	
SQL Server 2008 SP3 GDR (IA-64 only)	10.0.5545.0	SQL Server 2008 SP3 GDR (IA-64) TLS 1.2 Update	
SQL Server 2008 SP3 (IA-64 only)	10.0.5896.0	SQL Server 2008 SP3 (IA-64) TLS 1.2 Update	

3. Enable/Disable SSL/TLS protocols:

- You can manually disable SSL 1.0/2.0/3.0 and early TLS protocols and enable TLS 1.2 in the

Registry. Refer to the document available here on how to do this.

- Alternatively, you can download and run the TLS RegistryEdit script file to update the registry on application and database server.
- Make sure the registry keys are set as shown below:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:00000001
"DisabledByDefault"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
"Enabled"=dword:00000001
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
```

Disabled SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1

Enabled TLS 1.2

Set TLS 1.2 for .NET 3.5 application

Notes:

- At this point RDP to connect to the remote server might stop working in some cases because TLS 1.0 will be disabled. Make sure that you are using the latest RDP/windows update.
- Some of the settings on Registry (HKLMSYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols) may also change. So a registry backup or VM Snapshot is recommended.

4. On the Server Running CSS:

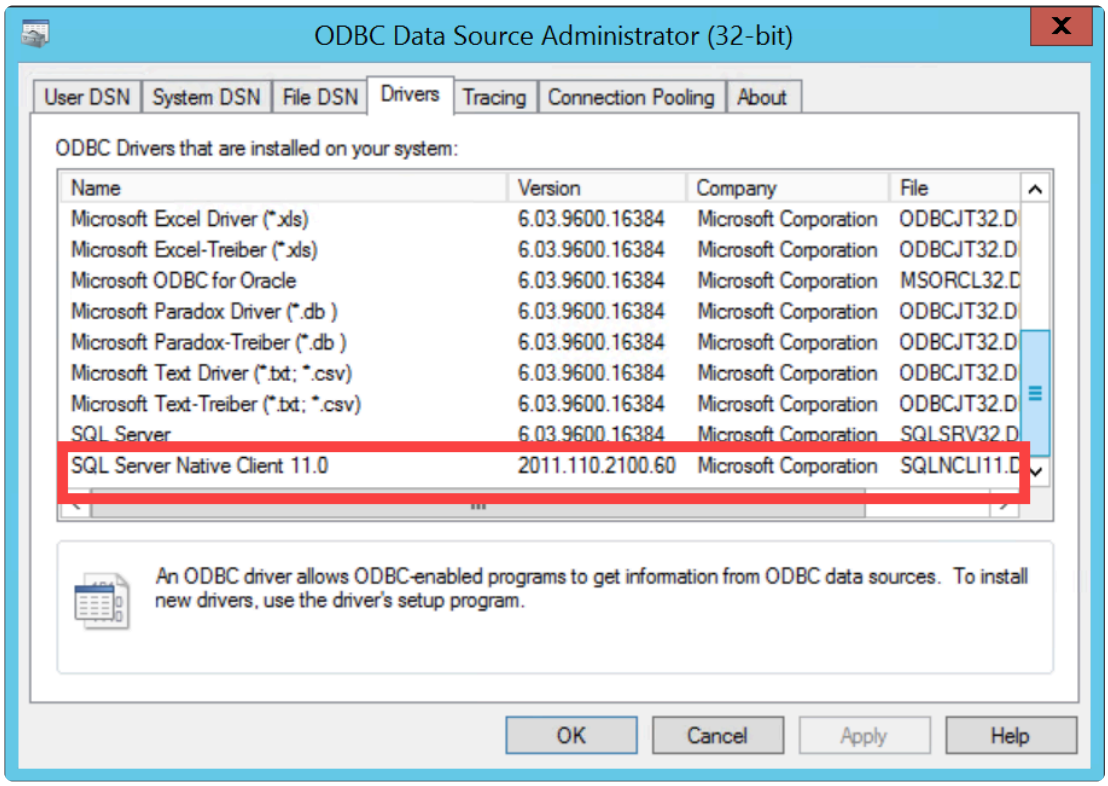
1. Apply the **SQL Server Native Client** patch corresponding to the SQL Server that it will connect to. You can download the patch from here: https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server

SQL Server Native Client (for SQL Server 2008 R2)	SQL Server Native Client (x86 and x64)
SQL Server Native Client (for SQL Server 2008 R2)	SQL Server 2008 R2 Native Client (IA-64)
SQL Server Native Client (for SQL Server 2008)	SQL Server 2008 Native Client (x86 and x64)
SQL Server Native Client (for SQL Server 2008)	SQL Server 2008 Native Client (IA-64)
SQL Server Native Client (for SQL Server 2012 and SQL Server 2014)	Microsoft SQL Server 2012 Native Client - QFE
Microsoft ODBC Driver for SQL Server	Microsoft ODBC Driver 11 for SQL Server - Windows
JDBC 6.0	Microsoft JDBC Drivers 6.0 (Preview), 4.2, 4.1, and 4.0 for SQL Server
JDBC 4.1 and JDBC 4.2	Microsoft JDBC Drivers 6.0 (Preview), 4.2, 4.1, and 4.0 for SQL Server

2. Verify that **SQL Server Native Client 10 or higher** is installed on the server or client machine running CSS/ SSS (Serverless/ Server-based).

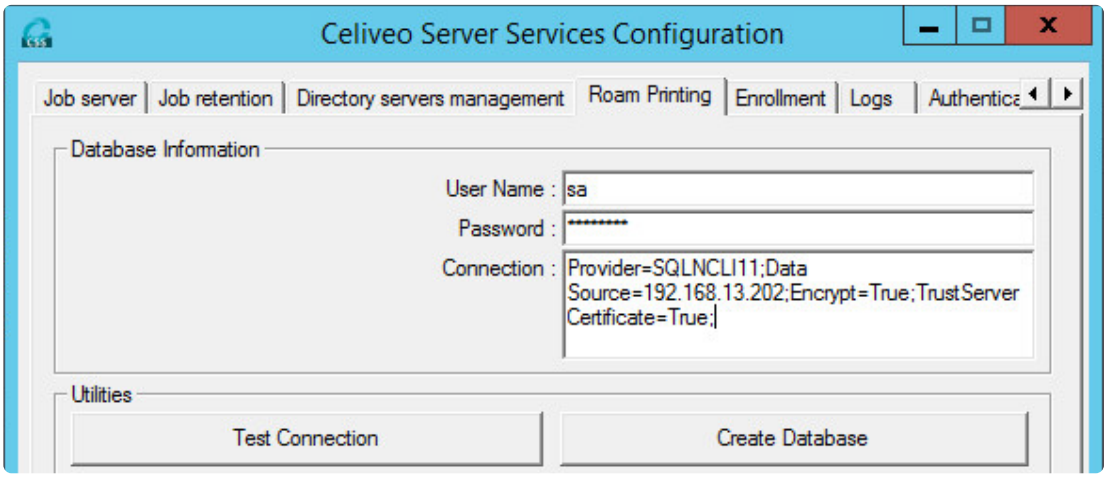
On the machine:

a. Press **Start**
b. Type **Run**
c. Type **%windir%\syswow64\odbcad32.exe** and press **OK**
d. Go to the **Drivers** tab and note the File name.



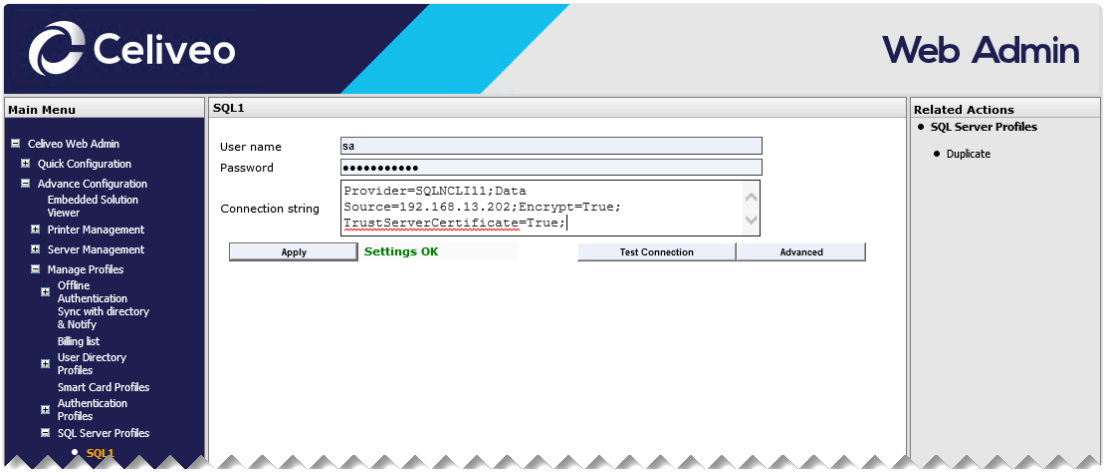
3. Now, Launch the **CSS/ SSS Configuration tool** as Administrator.
4. Go to the **Roam Printing** tab.
5. Change the **Connection** string in order to force the SQL native client provider instead of the OLEDB:

Provider=< Name of the file without the extension >;Data Source=< Server IP Address_or_Host name >;Encrypt=True;TrustServerCertificate=True;
For example: Provider=SQLNCLI11; Data Source=192.168.13.202; Encrypt=True; TrustServerCertificate=True;



6. Apply the same configuration on **Enrollment** tab.
7. Press **OK/Apply**.

Alternatively, the Connection string can also be configured via Celiveo Web Admin application.



Warning:

- Once the patch is applied on the SQL Server and TLS 1.1/1.2 is enforced, SQL Management studio won't be able to access the SQL DB as it also requires a patch or a newer version.
- RDP might require an update for Admins to login on the SQL Server since it normally operates on SSL.
- Other 3rd party software might not work as expected since SSL 1.0/2.0/3.0 and TLS 1.0 is forcibly disabled on the SQL Server machine.

Last modified: 29 September 2022

17.5. Managing 32 bit and 64 bit Architectures

How to add x86 (32 bit) Print Drivers on a x64 (64 bit) Windows Print Server

> **Note**: Both x86 and x64 drivers MUST have the same name. If they have the same name, they will appear automatically in Additional drivers for both architectures in the Printer's sharing properties.

Create and share a print queue on x64 Windows Print Server

1. Login to the Windows Print Server with Administrator account (Domain/ Local).
2. Click on **Start > Control Panel > Hardware**.
3. Click on **Add a Printer** and follow the steps to install the printer.
4. Download the 32 bit version of the printer driver, from the Printer manufacturer's driver site.
5. Next, right-click the Printer name and choose **Printer Properties**.
6. Click the **Sharing** tab.
7. Click on **Additional Drivers**.
8. Select **x86 Type 3 – User Mode**.
9. When prompted, provide the location of the 32 bit printer driver that was downloaded.

How to add x64 (64 bit) Print Drivers on a x86 (32 bit) Windows Print Server

Create and share a print queue on x86 Windows Print Server

1. Login to the Windows Print Server with Administrator account (Domain/ Local).
2. Click on **Start > Control Panel > Hardware**.
3. Click on **Add a Printer** and follow the steps to install the printer.
4. Download the 64 bit version of the printer driver, from the Printer manufacturer's driver site.
5. Next, right-click the Printer name and choose **Printer Properties**.
6. Click the **Sharing** tab.
7. Click on **Additional Drivers**.
8. Select **x64 Type 3 – User Mode**.
9. When prompted, provide the location of the 32 bit printer driver that was downloaded.

Last modified: 29 September 2022

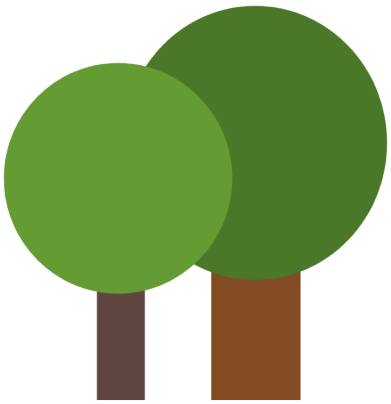
17.6. Environmental Impacts of Printing – Formulae used in TGS 10 reports

Formulae used in calculating the environmental impact due to loss of trees in paper production and the greenhouse gas mainly carbon dioxide (CO2) released during the process.

Some paper facts and assumptions:

- Here we consider the paper used for printing are 100% virgin copier paper of A4 size and not recycled.per Facts:
  - 1 A4 size sheet weighs 0.009 pounds (0,004 g) (see: https://www.papersizes.org/paper-weights.htm)
  - 1 carton = 10 reams = 5000 sheets
  - 1 tree makes 16.67 reams of copy paper or 8,333 sheets
  - 1 ream (500 sheets) uses 6% of a tree, i.e. 0.6 trees (see: http://conservatree.org/learn/EnviroIssues/TreeStats.shtml)
- Carbon absorption by trees (Carbon sequestration)
  - The amount of carbon absorbed vary for trees of different species and ages. Here, a 25 year old pine tree is taken as a standard for calculation.
  - An average pine tree of 25 year old absorbs 14.667 [1] pounds (6,350 kg) of CO2 per year.

Calculating the impact of cutting down trees



This value represents the number of tree(s) that has gone into the making of paper,
Calculation: **Total number of sheets of paper / 5000 sheets (per carton) * 0.6 trees For example**: A company uses printing paper on an average of 245,902 (non-recycled) A4 sheets per year. Calculating the loss of trees due to this print paper usage would be:
245,902 sheet of paper per year / 5000 sheets = 49.18 cartons of paper
49.18 cartons * 0.6 trees = 29.50824 trees are cut down per year

Calculating the total carbon dioxide emitted

The carbon dioxide emission is calculated in two parts:

- **Carbon sequestration**

  This denotes the quantity of carbon that would have been absorbed had the tree been alive. According to the assumption: An average pine tree of 25 year old absorbs 14.667 pounds (6,350 kg) of CO2 per year.

  Calculating the CO2 sequestration for each sheet of paper : **(Number of trees * 14.667 pounds**

(6,350 kg) of CO2) / Number of sheets

For the above example, if 29.50824 trees are cut down per year, then **29.50824 trees cut down * 14.667 pound of CO2 = 432.80 pounds (195,95 kg) of CO2** is no longer absorbed due to loss of trees.

Thus, each sheet of paper is worth **432.80/245,902 = 0.00176 pounds (0,00080 kg) of CO2**

- **Carbon dioxide produced during paper production**

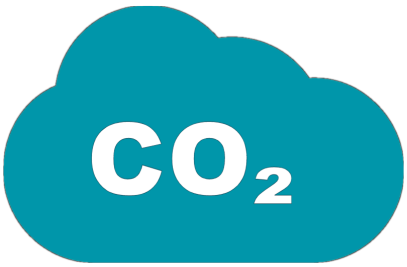
According to EPA%(color-red)*% 1 pound of paper produces 4.36%(color-red)[2]% pounds of CO2 during production.

Calculating the CO2 produced by each sheet of paper: **(Total weight of paper in pounds * 4.36 pounds of CO2) / Number of sheets**

For the above example, **245,902 sheets of paper * 0.009 pounds per paper = 2,213.12 pounds (1003,7 kg) of paper**

2,213.12 pounds of paper * 4.36 pounds of CO2 = 9469.19 pounds (4295,06 kg) of CO2 is produced during paper production

Thus, each sheet of paper produces **9469.19 pounds / 245902 sheets of paper = 0.03924 pounds (0,01783 KG) of CO2** during production

	The CO2 emission is calculated as a sum total of carbon dioxide not absorbed due to tree loss + carbon dioxide released during paper production Calculation: **(Number of trees * 14.667 pounds of CO2) / Number of sheets + (Total weight of paper in pounds * 4.36 pounds of CO2) / Number of sheets** For the above example: (0.00176 + 0.03924) * 245902 = 10,081.99 pounds (4572,66 kg) of CO2 is released per year.

You may also read :https://www.celiveo.com/smart-printing-blog/green-it-environmental-facts-about-printing

[1] [2] The values are derived from Study Report: Save Paper submitted by Daniel in MIT, and U.S EPA, 2006. Solid Waste Management and Greenhouse Gases: A Life-Cycle Assessment of Emissions and Sinks, EPA530-R-06-004

* U.S. Environmental Protection Agency, publishes guidelines for minimum recycled product content, for use by federal agencies for purchasing standards. EPA also advocates source reduction practices, as well as other aspects of environmentally sound products, such as reduced toxins, energy savings, and biomass projects. In addition to providing guidance on environmental products, EPA regulates many aspects of paper industry production, including emissions (air, water, land) and solid waste management.

Last modified: 29 September 2022

17.7. Pushing Print Jobs to Network Attached Storage (NAS)

Contents

- What is NAS?
- How does NAS work for virtual printers?
- How to push print jobs to NAS?
- How to configure NAS path while creating CVP deployment package?
- Support for NAS during CVP manual installation

What is NAS?

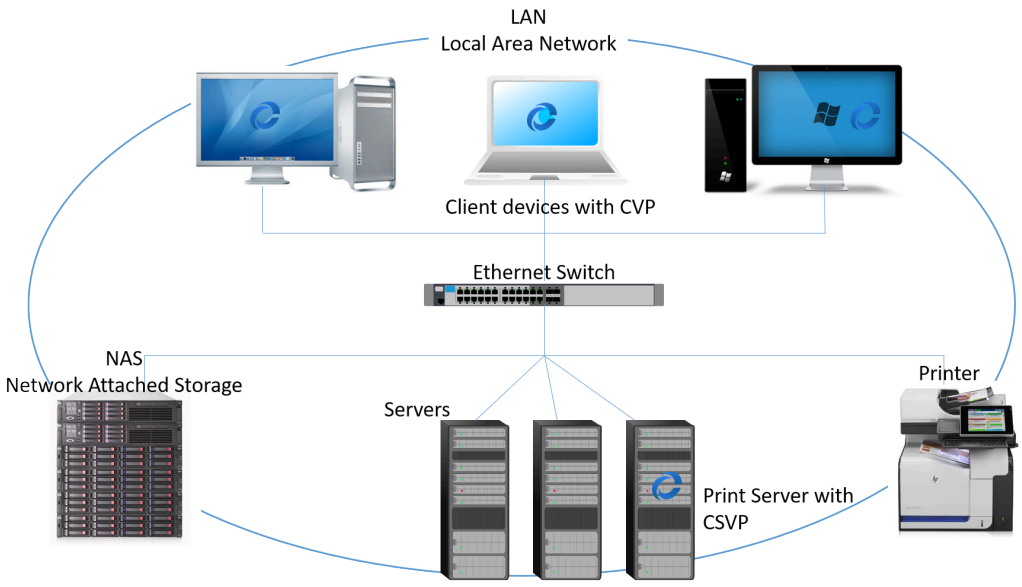
Network Attached Storage or NAS is a typical storage unit (single purpose computer server unit) attached to the network that provides file based data storage access to varied group of client systems. The purpose of **NAS** is to provide centralized and shared storage for digital files. For this reason there can be multiple hard drives in a single NAS unit.

- NAS units generally do not have a keyboard or a display unit. They are accessed through browsers.
- The NAS unit connected to a network, can be accessed by any number of PCs as long as they are also on the same network.

Some benefits of NAS include:

- Additional storage space
- Data protection with fail-over configurability
- Easy to setup

NAS connected to a network:



How does NAS work for Celiveo Virtual Printers?

NAS works as a temporary storage location (remote storage location) for print job files, in the case when Print Server (CSVP) is unreachable to store print job information.

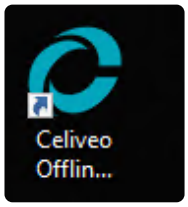
Celiveo has now enabled support for pushing print job files to NAS unit for easier access to print jobs details. In the event, when the Print Server is not reachable (Celiveo Server Services in CSVP are offline) when trying to send print jobs from a user workstation using Celiveo Virtual Printer, the print jobs are re-routed to be stored in NAS unit temporarily. Once the Print Server is accessible, all the print jobs stored in NAS are moved to local storage of the Print Server. Thus NAS unit acts as a temporary location for storing print job data generated across all CVP workstations in the network.

How print job data are pushed to NAS?

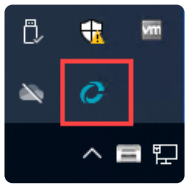
Print Job data can be pushed to NAS by two methods:

- **Shutdown to NAS**: This feature is configured while creating the Celiveo Virtual Printer (CVP) deployment package. CVP can push the print files to a temporary storage (NAS unit) which is connected in the same domain network during shutdown of workstation. You should add the domain network details (User name/ Password/ Domain name) and NAS path while configuring the CVP package.

- **Push printing** (manual): In this method, a CVP user can either:
  - Choose to move the print job data to the NAS unit using the **Celiveo Offline Printing** icon available on the desktop. This icon is made available upon CVP installation.

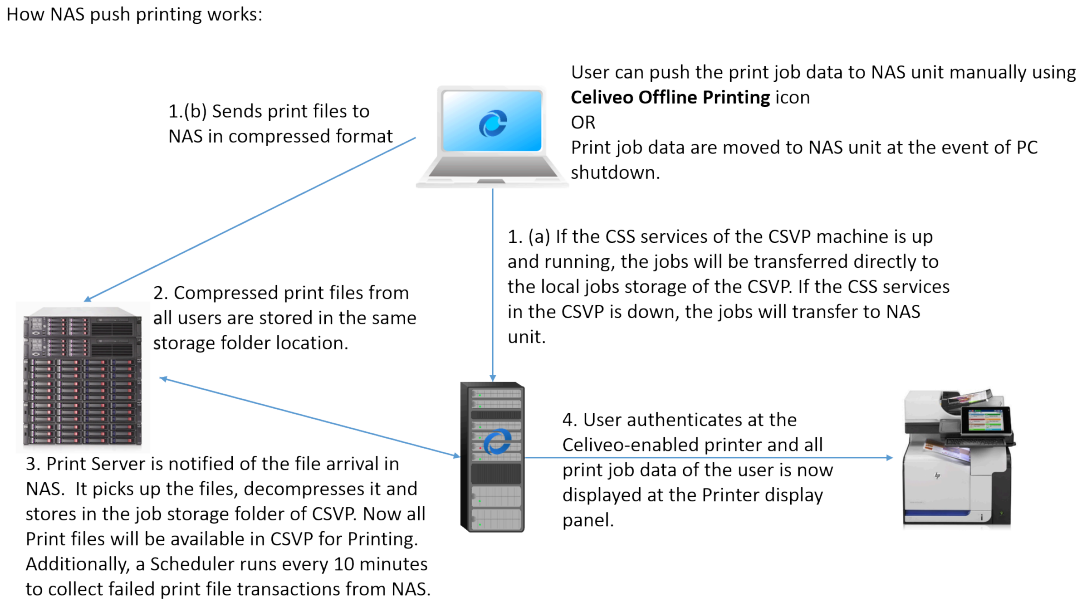
    

  - Right-click the Celiveo icon available on the Windows system tray and choose **Offline Printing**.

When user sends a print job to NAS, the CVP initially checks if the Print Server is accessible.

- IF Print Server is accessible (CSS services is online) : all print files are pushed directly to the Print Server, where it is stored in the default jobs storage folder.
- IF Print Server is not accessible (CSS services is offline): all print files are pushed to NAS (temporary storage). While pushing to NAS, all print files are **compressed** and stored at a single location (destination folder) in the NAS unit. This reduces the storage space used in NAS instead of allocating a definite amount of space to an individual user's print job information.



How does Print Server pick up print job files from NAS?

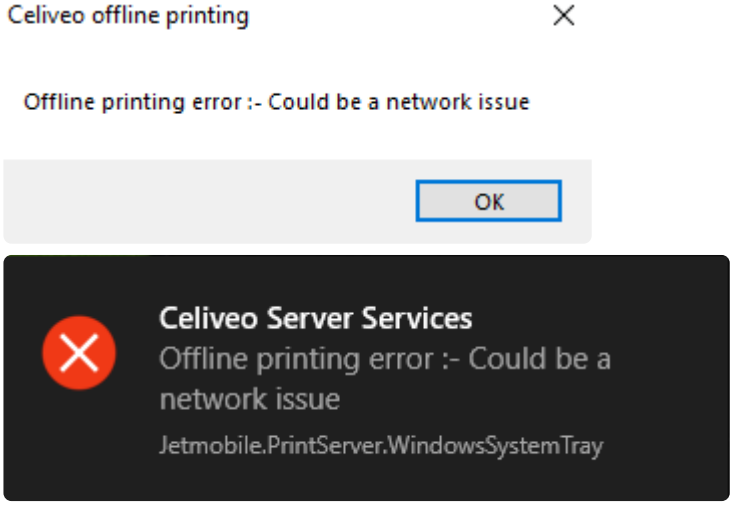
As and when the print jobs get transferred to NAS, the Print Server is notified of this event, and when it the compressed print files are picked from NAS unit, decompressed and stored in the jobs storage folder of Print Server. Now all those print files will be available at the Print Server.

In addition to this, a scheduler runs every 10 minutes to check for any failed print job transactions in NAS. For each scheduler event, all the remnant print job files available in the NAS folder are picked, decompressed and stored in the jobs storage folder of the CSVP.

No copy of these print files are retained in the NAS folder.

What happens when NAS is not available?

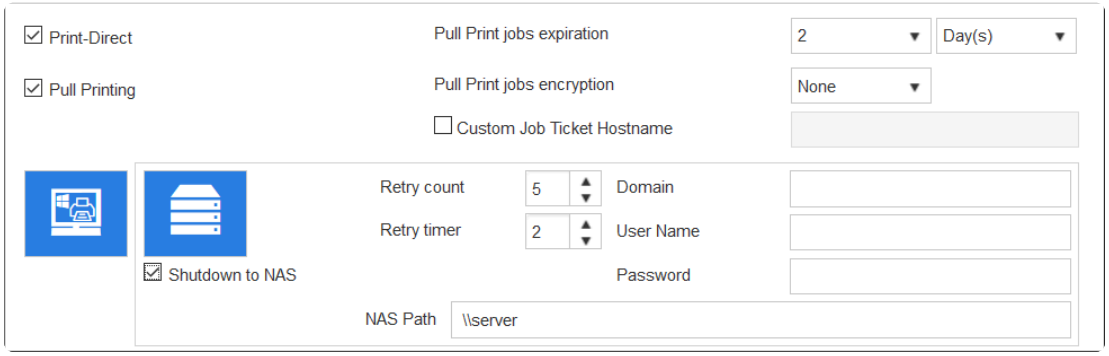
- When the NAS is not available while doing a **manual push print** using the desktop icon or Windows system tray icon, appropriate error messages are displayed notifying the user.



- When the NAS is not reachable **upon Shutdown** of client workstation, the print jobs are retained on client machine's default jobs location.

How to configure NAS while creating Celiveo Virtual Printer?

While configuring the CVP deployment package, you have the option to choose **Remote** server to store the print jobs.



1. Select the **[Shutdown to NAS]** option. This allows the print jobs information to be transferred to the NAS unit when user initiates shutdown of the workstation.
2. Enter **[User Name]**, **[Password]**, **[Domain]** and **[NAS Path]**.
3. At **[Retry Count]**, enter the number of attempts to reach the NAS to store the jobs.
4. At **[Retry timer]**, enter the time interval (Seconds) between each attempt to reach the NAS.
5. Once all settings are complete, proceed with creating the deployment package.

Support for NAS during CVP manual installation

You can install Celiveo Virtual Printer using silent installation with an option to push print job data to a Network Attached Storage (NAS). This increases accessibility to the print jobs when CVP is offline (user workstation is shutdown).

To enable this feature during installation, run the following command: **installer.exe -ccp -s**

Note: -s prevents display of any popup notifications to the user during silent installation.

Last modified: 29 September 2022

17.8. Celiveo WebAdmin Tools and API

NOTE: The Celiveo WebAdmin command line API tool is available from WA 8.6.19.808 and newer versions.

This Celiveo WebAdmin command line API tool allows admin to import printers in bulk using CSV file, synchronize a printer and get its synchronization status. This command-line tool can also be invoked by third-party systems, by passing the right parameters. It responds using the correct return code at the standard output – stdout.

```
C:\Program Files\Celiveo\Celiveo 8\API Tools>cvocli.exe
Celiveo WebAdmin Tool and API c Celiveo Pte Ltd 2011-2022
Version: 8.9.32.2
Usage:
cvocli import <csvPath>
cvocli sync <printerIp/serial/MAC>
cvocli getstatus <printerIp/Serial/MAC>
cvocli delete <printerIp/Serial/MAC> [-f]
cvocli update colorAndPageSize
```

Location

The latest version of the Celiveo Web Admin Command Line API tool is available in the Web Admin installation directory, usually under *C:\Program Files\Celiveo\Celiveo 8\API Tools*

Call:

Calls to this API tool is performed from the Windows command-line interface (cmd.exe) or using Start-Process in Powershell or Process.Start() in C# or any other language's method which spawns a process on Windows OS.

Always run the command-line tool in administrator mode.

The API returns value zero when the call is successful with a response on stdout or non-zero when the call fails, with description on stdout.

Security:

This tool supports TLS 1.2 encryption or any protocol that is configured for the CeliveoDB SQL Server database access (defined in SQL Server).

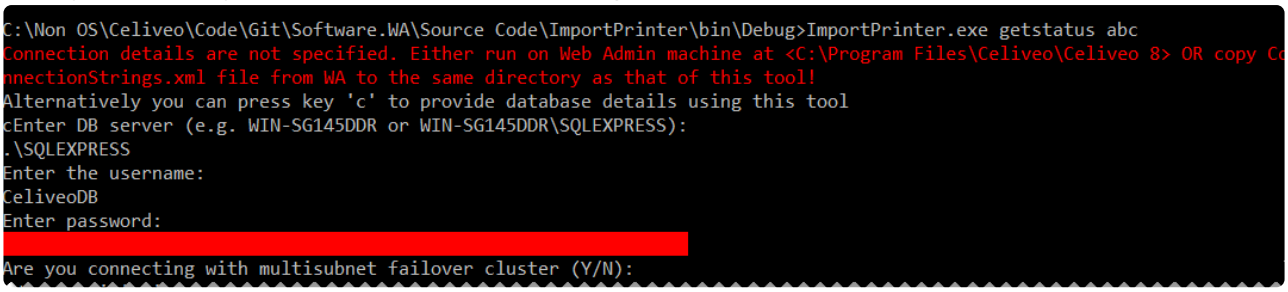
It uses that protocol to encrypt communication to the SQL Server database.

Before you begin:

This tool needs the connection details to access the Web Admin database (CeliveoDB).

You can provide database information in one of the following two ways:

- Copy ConnectionString.xml from Web Admin Server's "C:\Program Files\Celiveo\Celiveo 8\Web Admin" to the directory where the command line API tool is installed and run. Ensure that the access to the directory containing the tool is secured to prevent unauthorized usage.
  The login information is read from that encrypted file and used to access the CeliveoDB database
  OR
- Run the tool on the server where Web Admin is installed at "C:\Program Files\ Celiveo\Celiveo 8"
  Launch the command line tool with the syntax "cvocli.exe getstatus abc".
  This is a one-time operation that asks for all Celiveo DB database details, they will be stored locally in an encrypted file and not requested again.



API to Import Printers into Celiveo WebAdmin

Purpose: This call initiates the import of printers from a CSV file into the Celiveo Web Admin software. The information about the printer is obtained from the values provided in the CSV file.
You must have created and tested some master printers in the Celiveo WebAdmin software (Master Printers), that the imported printers will clone when being added through the API.

Example of process:

- Create and configure a master printer in the Celiveo WebAdmin portal, its MAC Address is 00:8A:75:42:FE:1F.

  Important: That printer to clone shall be of the exact same type as the injected printers that will clone it.
  Examples:
  If you want to inject HP Futuresmart 3 or 4 printers, you must have defined an HP Futuresmart 3 or 4 master printer.
  If you want to inject Ricoh SOP 2.x printers, you must have defined a Ricoh SOP 2.x master printer.
  If you want to inject Lexmark Android-capable printers, you must have defined a Lexmark Android-capable master printer.
  etc…

- Build a CSV file where each line represents a printer to import into the Celiveo WebAdmin, and contains the MAC address of the printer to clone.

The column content of the printer definition overrides those properties cloned from the master printer (ie: tags, name, description…)

- run the import utility
- synchronize the printer(s) using the Celiveo WebAdmin or the command-line tool

List of printers to import with master printer(s) cloning:

The CSV file needs to be created with one line per printer to inject, and each line data in the following format:

Column 1	IPv4 MAC Address of MP2C Format: 12:34:56:78:90:AB or 123456789AB
Column 2	HostName of P2I (string, max length= 250 chars)
Column 3	IPv4 Address of P2I Format: xxx.xxx.xxx.xxx
Column 4	IPv4 MAC Address of P2I Format: 12:34:56:78:90:AB or 123456789AB
Column 5	Serial number of P2I (string, max length = 50 chars)
Column 6	Printer model of P2I (string, max length = 250 chars) The printer model must be solution-compatible with the MP2C printer model.
Column 7	Printer Brand of P2I (string, LEXMARK HP RICOH KM XEROX CANON TOSHIBA FUJI-XEROX KYOCERA etc… The brand must be the exact same as the MP2C printer brand.
Column 8	Printer Description of P2I (string, max length = 250 chars)
Column 9	Printer Type for P2I (“MFP” or “SFP”) The printer Type must be the exact same as the MP2C printer Type.
Column 10	Tag1 value of P2I (string, max length = 150 chars)
Column 11	Tag2 value of P2I (string, max length = 150 chars)
Column 12	Tag3 value of P2I (string, max length = 150 chars)
Column 13	Tag4 value of P2I (string, max length = 150 chars)
Column 14	Tag5 value of P2I (string, max length = 150 chars)

Where, MP2C = Master Printer to clone and P2I = Printer to Inject

Syntax	**cvocli.exe import < CSVPath >**, where CSVPath is the full path to the CSV.
Example	cvocli.exe import C:\Users\Documents\Printers\Printers.csv
Response Status	Returns printer added or updated description, if successful:
Error	Returns Error status and description if the printer is not able to be added. 0: Success -1000: Invalid number of command-line parameters 1000: error connecting to CeliveoDB SQL database 1004: Invalid command

API to Synchronize a Printer

Purpose: This call synchronizes a printer present in the Celiveo Web Admin database, to load the printer agent and settings, as appropriate.
It is the same as syncing the printer from the Celiveo WebAdmin UI.

Note: The printer should have been created interactively in the Celiveo WebAdmin UI or through the “cvocli.exe import” call documented above.

Syntax	– **For CSA-Based printers: cvocli.exe sync < filepath or IP Address > —csa** Filepath —> For multiple printers, path to the file – One IP per line. IP Address —> IPv4 address for a single printer. - **For non-CSA based printers: cvocli.exe sync < filepath or IP Address >** Filepath —> For multiple printers, path to the file – One IP per line. IP Address —> IPv4 address for a single printer.
Example	cvocli.exe sync 192.168.4.45 -csa cvocli.exe sync 192.168.4.45
Response	No text output on stdout upon success or failure.
Return Code	Returns Non-Zero code in case the printer does not exist in Web admin or for any other error. 0: Success -1000: Invalid number of command-line parameters 1000: error connecting to CeliveoDB SQL database 1003: Printer to be synced does not exist in Web Admin database 1004: Invalid command

API to Get Synchronization Status of Printer present in Celiveo WebAdmin

Purpose: This call gets the status of printer present in Celiveo Web Admin.
The status of the printer is returned, that’s the value displayed in the Celiveo Web Admin UI.

Syntax	**cvocli.exe getstatus < filepath or IP Address >** Filepath —> For multiple printers, path to the file – One IP per line. IP Address —> IPv4 address for a single printer.
Example	cvocli.exe getstatus 192.168.4.145
Response	Returns status of the printer if the call is successful: Error Configuration in progress Synchronized Sync failed: Could not connect to database Sync failed: Unable to execute SQL procedure Sync failed: No data Sync failed: Unable to retrieve SQL configuration from Web Admin. Sync failed: Internal error Sync failed: Unknown error Synchronized (Cost profile not set) Synchronized (Print rules not set) Synchronized (Cost profile and print rules not set) Sync failed: No authentication configuration Printer configuration in progress Sync failed: upgrade Celiveo Sync failed: Invalid printer credentials Sync failed: Invalid AD/LDAP credentials All embedded code packages loaded Downloading Celiveo embedded solution Sync failed: Unable to download Celiveo embedded solution Sync failed: Unable to install Celiveo embedded solution Configuring Celiveo embedded solution Sync failed: Unable to configure Celiveo embedded solution Installing Celiveo embedded solution Sync failed: Printer is offline. Not synchronized Sync request sent N/A Ready for synchronization Printer is unreachable Sync failed Sync failed: no answer from CSA Ready for license synchronization License update failed License validation failed
Return code	Returns Error status and description if the printer is not able to be added. 0: Success -1000: Invalid number of command-line parameters 1000: error connecting to CeliveoDB SQL database 1004: Invalid command

	Returns “Printer not found” on stderr for any other error.

API to delete a printer

Purpose: This call deletes a printer present in Celiveo Web Admin.

Syntax	**cvocli.exe delete < PrinterIP >**, where PrinterIP is the IP address of the printer to delete.
Example	cvocli.exe delete 192.168.4.45
Response Status	Returns printer deleted, if successful:
Error	Returns Error status and description if the printer is not able to be added. 0: Success -1000: Invalid number of command-line parameters 1000: error connecting to CeliveoDB SQL database 1004: Invalid command

Last modified: 29 September 2022

17.9. Open Source codes used in Celiveo 8 (Latest version)

GNU GENERAL PUBLIC LICENSE	Matrix Version	License/Source Location	Component
NETPLUGD – 1.2.9.2	1.2.9.2	https://github.com/vyos/netplug/releases	
LINUX KERNEL – 3.2.0	3.2.0-SIA-1.16	https://www.kernel.org/	
GNU LESSER GENERAL PUBLIC LICENSE	**Matrix Version**	**License/Source Location**	**Component**
OPENSC – 0.13.0	0.13.0	http://www.gnu.org/licenses/gpl2.html	FIRMWARE
LIBUSB – 1.0.19	1.0.9	http://libusb.info/	FIRMWARE
GEMALTO .NET PKCS11 – 2.2.0.9	2.2.0.9		
CCID – 1.4.19	1.4.19	https://alioth-archive.debian.org/releases/pcsclite/ccid/1.4.19/	
LIBRARY	**Matrix Version**	**License/Source Location**	**Component**
OpenLdap	2.4.33	http://www.openldap.org/software/download/OpenLDAP/openldap-release/LICENSE	FIRMWARE
ASM	4.2	http://asm.ow2.org/license.html	
Dropbear	2012.55	https://secure.ucc.asn.au/hg/dropbear/raw-file/tip/LICENSE	
FLTK	1.3.2	http://www.fltk.org/COPYING.php	FIRMWARE
IPTables	1.4.15	http://www.netfilter.org/licensing.html	
Kerberos	1.11	http://web.mit.edu/kerberos/krb5-devel/doc/mitK5license.html	
Libxml2	2.9.1	http://opensource.org/licenses/mit-license.html	FIRMWARE
MiniZip	1.1	https://github.com/nmoinvaz/minizip/blob/master/LICENSE	FIRMWARE
NET-SNMP	5.7.1	http://www.net-snmp.org/about/license.html	
NTP	4.2.6p5	http://opensource.org/licenses/NTP	
CyrusSasl	2.1.26	https://cyrusimap.org/imap/download/installation.html#licensing	FIRMWARE
SQLite	3.8.3.1	http://www.sqlite.org/copyright.html	FIRMWARE

TinyXml	2.6.2	https://sourceforge.net/projects/tinyxml/files/tinyxml/2.6.2/	FIRMWARE
Zlib	1.2.5	http://www.zlib.net/zlib_license.html	FIRMWARE
	1.0.2.o		FIRMWARE
Openssl	0.9.8	http://www.openssl.org/source/license.html	CSS
OpenSc	0.13.0	http://www.gnu.org/licenses/gpl2.html	FIRMWARE
pcsc	1.8.14	https://alioth-archive.debian.org/releases/pcsclite/pcsclite/1.8.14/	FIRMWARE
ossp-uuid	1.6.2	http://www.ossp.org/pkg/lib/uuid/	FIRMWARE
ProtoBuf	2.5.0	https://github.com/protocolbuffers/protobuf/blob/master/LICENSE	CSS
Celib2	1.0	https://github.com/coldnew/celib/tree/master/LICENSE	
arp-scan	1.9	https://github.com/royhills/arp-scan/blob/master/COPYING	
Cronie	1.4.8	https://github.com/cronie-crond/cronie/blob/master/COPYING	
Fping	3.5	https://github.com/schweikert/fping/blob/develop/COPYING	
Libcrafter	0.3	https://github.com/pellegre/libcrafter/blob/master/libcrafter/LICENSE	FIRMWARE
Arping	2.13	https://github.com/ThomasHabets/arping/blob/arping-2.x/LICENSE	
FreeTDS	5.1.0	https://github.com/FreeTDS/freetds/blob/master/COPYING.txt	FIRMWARE
Apache Tomcat	9.0.1	http://www.apache.org/licenses/LICENSE-2.0	
NLog	4.6.5	https://github.com/NLog/NLog/blob/master/LICENSE.txt	Web Admin/ CVP
Newtonsoft.Json	12.0.2	https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md	Web Admin/ CVP
SevenZipSharp	LGPL v3.0	https://archive.codeplex.com/?p=sevenzipsharp	Web Admin/ CVP
gsoap	2.8.16	https://www.cs.fsu.edu/~engelen/license.html	FIRMWARE
jsoncpp	0.5.0	https://github.com/open-source-parsers/jsoncpp/blob/master/LICENSE	FIRMWARE
unixodbc	2.3.5	https://sourceforge.net/directory/os:windows/	FIRMWARE

		license:lgpl/	
jtds	1.3.0	http://jtds.sourceforge.net/license.html	BUSINESS EMBEDDED
log4j	1.2.17	https://github.com/usnistgov/jsip/blob/master/licenses/LOG4J-LICENSE.txt	BUSINESS EMBEDDED
org.sqldroid	1.0.3	https://github.com/SQLDroid/SQLDroid/blob/master/LICENSE	BUSINESS EMBEDDED
com.unboundid	4.0.4	https://docs.ldap.com/ldap-sdk/docs/LICENSE-UnboundID-LDAPSDK.txt	BUSINESS EMBEDDED
DiffieHellman	0.0.0.0	https://github.com/dscape/diffie-hellman/blob/master/LICENSE	CSS
Ionic.Zip	1.9.1.8	https://github.com/litdev1/LitDev/blob/master/Ionic.Zip.License.txt	CSS
Ionic.Zlib	1.9.1.8	https://github.com/jstedfast/Ionic.Zlib/blob/master/License.zlib.txt	CSS
Novell.Directory.Ldap	2.0.0.0	https://github.com/dsbenghe/Novell.Directory.Ldap.NETStandard/blob/master/LICENSE	CSS
Starksoft.Net.Ftp	1.0.158.0	https://github.com/bentonstark/starksoft-aspen	CSS
Starksoft.Net.Proxy	1.0.131.0	https://github.com/bentonstark/starksoft-aspen	CSS
Tamir.SharpSSH	1.1.1.13	https://github.com/kthompson/SharpSSH	CSS
Org.mentalis.Security.dll	1.0.13.715	http://www.mentalis.org/site/license.qpx	CSS
Cryptopp (Cryptlib.lib)		https://www.cryptopp.com/License.txt	CSS
7zip-1801	19.0	https://sourceforge.net/projects/sevenzip/	CSS

Last modified: 29 September 2022

17.10. Upgrade to Celiveo 8

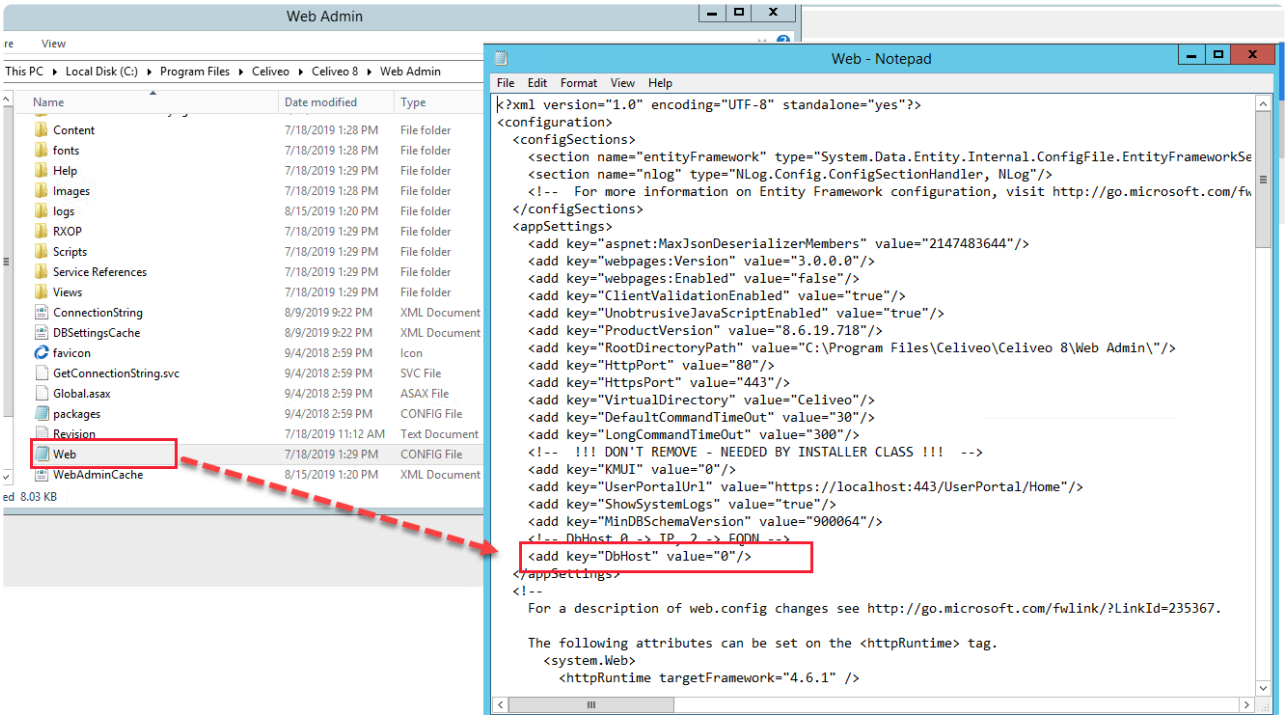
Celiveo Web Admin Installer

This Celiveo 8 installer comprises of Web Admin, Celiveo Virtual Printer (CVP) and Discovery Agent (DA). This product installer is 64-bit compatible and should only be installed on Windows Server systems running on 64-bit OS. It is not recommended to install WA on Windows Client systems, except for demonstrative purposes. For more information, refer to System requirements for Celiveo 8.
Celiveo Virtual Printer installer is compatible for both 32-bit and 64-bit operating systems. The appropriate version will be automatically deployed based on the OS running on the client/ server systems.

Before you begin…

If you have an existing Celiveo 8 solution from a previous release, **it is necessary to uninstall the old version before installing the new version**.
Ensure to take note of the following attributes in the Web configuration file before uninstalling the solution. If the attribute values are modified, you will have to update those values in the Web configuration file of the new version.

1. Go to “C:\Program Files\Celiveo\Celiveo 8\Web Admin”
2. Open Web configuration file.
3. Search for attribute key “DbHost”.
4. Take note of the value if it has been changed. The default value is zero.
   “DbHost” values can be the following:
   0: The Web Admin will use the Database IP in the CVP configuration file and to send Database details to printers.
   Or
   2: The Web Admin will use the Database Hostname or FQDN (depending on the DNS resolution) in the CVP config file and to send to printers.
5. Similarly, note the value for the attribute “KMUI” if it has been changed. The default value is zero. (This is optional)

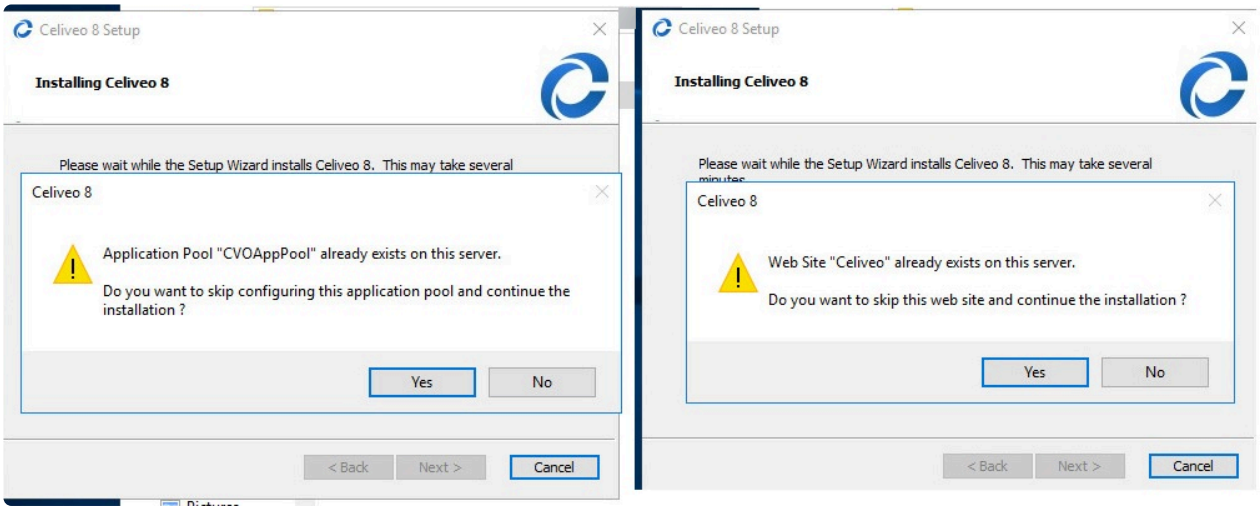


Uninstall the existing Celiveo 8 solution

1. Go to **Control Panel > Programs and Features**.
2. Choose Celiveo 8 and click **Uninstall**.
3. Click **OK** on the confirmation dialog to uninstall.

Install the new Celiveo 8 solution

1. Download the latest Celiveo 8 solution from here.
2. Follow the steps here to install the Celiveo Web Admin.
3. During the installation, confirmation prompts will be displayed to skip the configuration of the Celiveo Application Pool and Website.
4. Click **Yes** to use the existing Application pool and Website.



5. Complete the installation and update the Web configuration file, if required.

Celiveo Virtual Printer

To upgrade the Celiveo Virtual Printer installed on a user's work station:

1. Follow the instructions given here to upload the new Celiveo Virtual Printer deployment package on Web Admin.
2. Follow the instructions given here to download and install the new Celiveo Virtual Printer Deployment package on a user's workstation.

Celiveo Smart Appliance/ Embedded Agents

To upgrade the agents (Celiveo Smart Appliance/ Embedded Agent for HP FutureSmart and Ricoh Android printers), follow the instructions given here to upgrade the Celiveo Version on CSA Agent/ Embedded Agents.

Migrating from SecureJet 7.0.x / Celiveo 8.0.x to Celiveo 8

Follow the instructions given here to upgrade to the latest Celiveo 8 version.

Last modified: 29 September 2022

17.11. Migration Support to Celiveo 8 Versions

This section explains how to smoothly transition to Celiveo 8 by installing a new environment that operates in tandem with the existing one in order to avoid production disruption. Once the migration is complete and validated that it is operating correctly the old one can be uninstalled.

For ease of understanding, let's term the Windows Server installed with the existing solution as Legacy Server.

> ! **IMPORTANT NOTE**: Tracking data migration from the legacy application is not available.

Why migrating from SecureJet 7.0.x or Celiveo 8.0.x to Celiveo 8?

- The first SecureJet 7 version has been released in 2010, and most of the software is based on early .Net technology from Microsoft, plus SQL drivers from that time.
- All that technology has evolved and Microsoft has discontinued some of them.
- One example is SQL Compact Edition used by Celiveo Web Admin, its support ends the 13th of July 2021, there will be no more vulnerability check or fixes from Microsoft.
- Celiveo is evolving to Zero Trust Architecture and public/private Cloud support and that's not compatible with the old SecureJet and Celiveo 8.0.x architecture.
- Celiveo 8R is based on all the latest and most secure technology required at a time high security is mandatory.
- Celiveo 8R is adds compatibility to Konica-Minolta, Ricoh SOP, Lexmark
- Celiveo 8R supports HP Modern devices that were introduced in 2021

Before you begin…

While upgrading from SecureJet 7.0.5, 7.0.6 and Celiveo 8.0.1, 8.0.2 to Celiveo 8 versions:

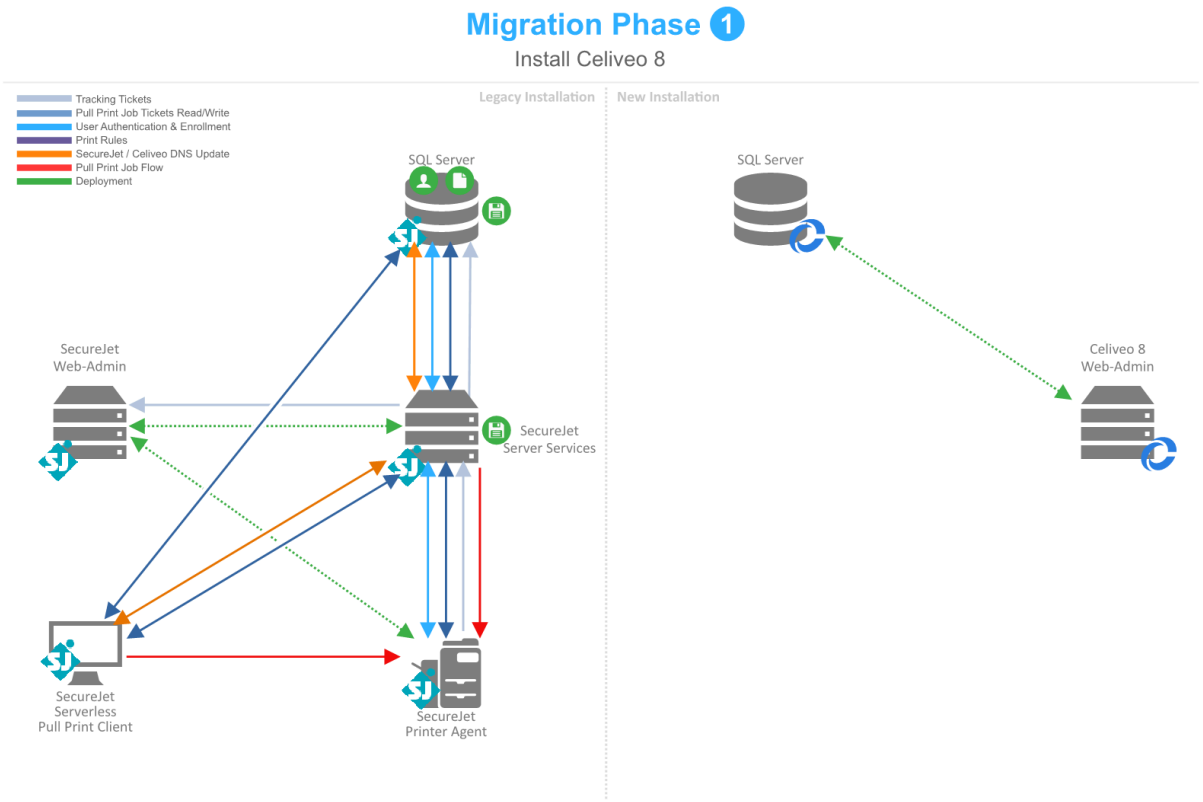
- Ensure the minimum system requirements for installing Celiveo 8 solution are fulfilled. Refer to the System Requirements for Celiveo 8 for further details.
- Ensure that the Legacy Server containing the SecureJet or Celiveo solution is up to date. Ensure the printers are synchronized successfully in SecureJet 7.0.5, 7.0.6, or Celiveo 8.0.1, 8.0.2 Web-Admin and you are able to successfully release a pull print job.
- Ensure you have the latest version of Celiveo 8, ready to be installed in the new Server. You can get the latest version from the Downloads section.
- Ensure that HP FutureSmart printers are upgraded to the latest firmware version.
- **IMPORTANT**: If the customer has users enrolled in SQL instead of AD then a custom SQL script needs to be executed at phase 4 on the Legacy Server SQL Server in order to migrate the SJPS Enrollment Table to the new Celiveo 8 SQL Server DB. Ensure you obtain a copy of the SQL script before you start the migration process. Contact Support with SSS/CSS version so the custom

script can be generated and delivered.

- **IMPORTANT**: Ensure to back up the Master SecureJet Server Services Server and SQL databases mainly SJPS and TGS (PrintManager80 / PrintManager90) before you initiate phase 2.
- **IMPORTANT**: If you have an SAP connector and are planning to migrate, read this section.

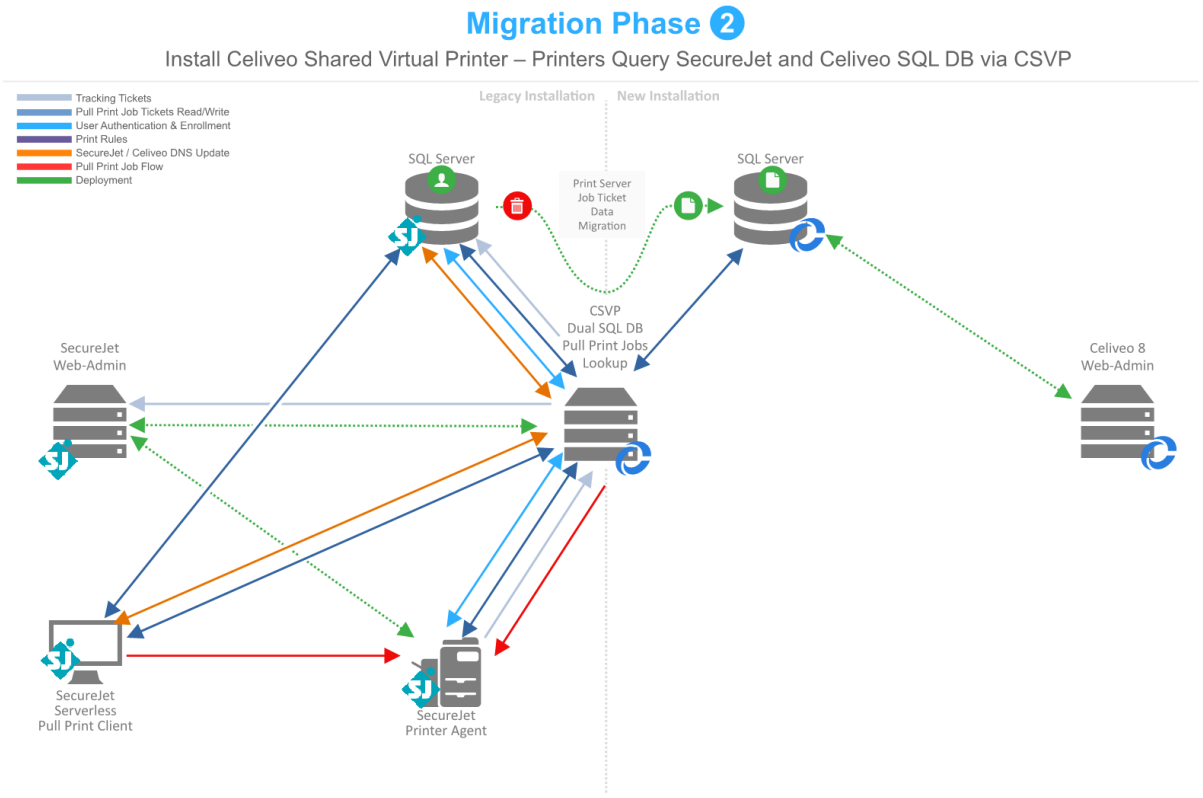
Phase 1

1. This phase can be executed without any production disruption in the deployed environment and should be done upfront. During this stage, it is recommended to execute a pilot during phase 1 before initiating phase 2.
2. Provision a new SQL Server to host the new Celiveo DB data and a Windows Server to host the new Celiveo 8 Web-Admin.
3. Install Celiveo 8 in the Windows Server and point to the newly provisioned SQL Server DB Instance.
4. In the Celiveo Web-Admin Celiveo 8 create, configure and export a CSVP. This will replace the legacy master SecureJet Server Services and is necessary for phase 2.
5. In the Celiveo Web-Admin Celiveo 8 create, configure and export a CVP. This will replace the legacy SecureJet Server Serverless Pull Printing Client and is necessary for phase 3.
6. In the Celiveo Web-Admin Celiveo 8 create an Access & Rules Control > Acess Control Rule profile that points to Active Directory or LDAP. Make sure that the Access Control Rule is created as it will be required on phase 4.
7. Just before starting Phase 2 make sure to do a backup or take a snapshot of the server that is hosting the master SecureJet Server Services / Celiveo Server Services and Celiveo SQL Server DB.



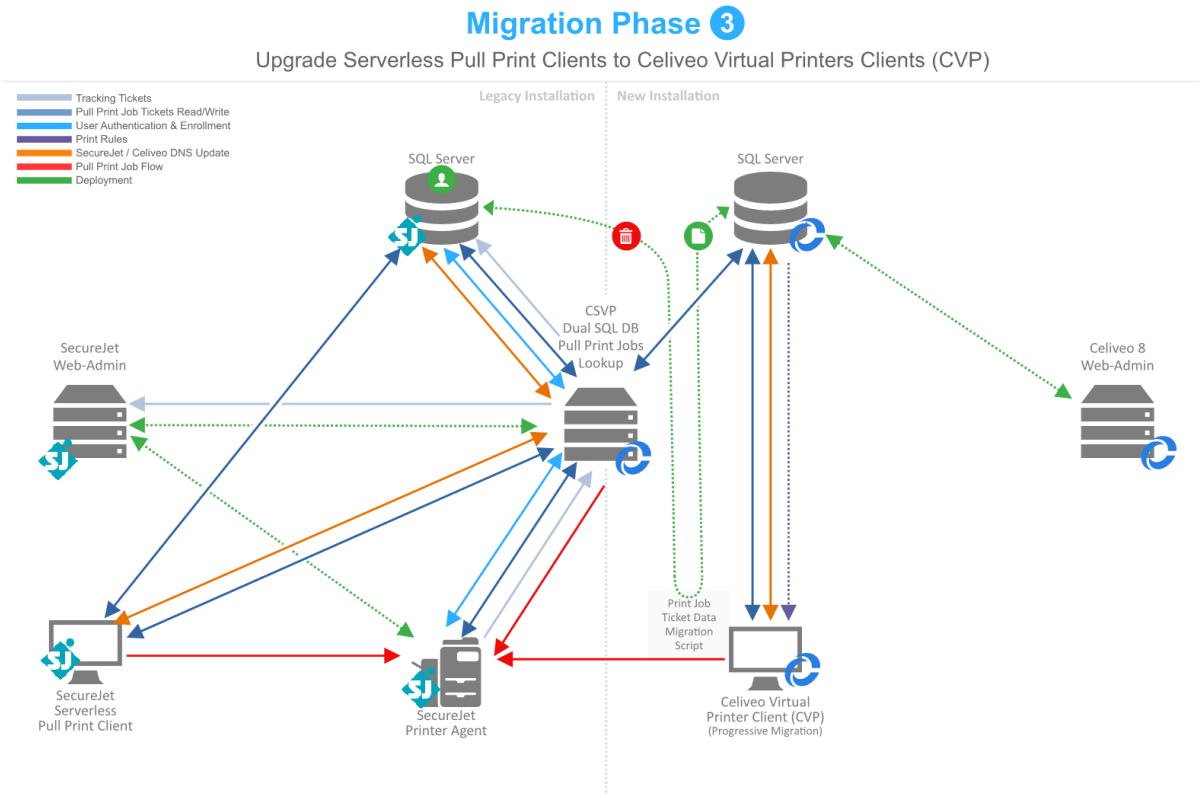
Phase 2

1. (Operation in the Server) Run the MigrationCVP.exe – This process will remove the SecureJet Server Services / Celiveo Server Services Job tickets for the target Server from the legacy SecureJet SQL DB and move them to the Celiveo 8 SQL DB.
2. Install the CSVP that was exported in phase 1.
3. Make sure that the CSVP is configured with Dual SQL DB lookup that will point to both legacy SecureJet SQL DB and new Celiveo 8 DB.
4. The CSVP is now prepared to query both SQL DB.



Phase 3

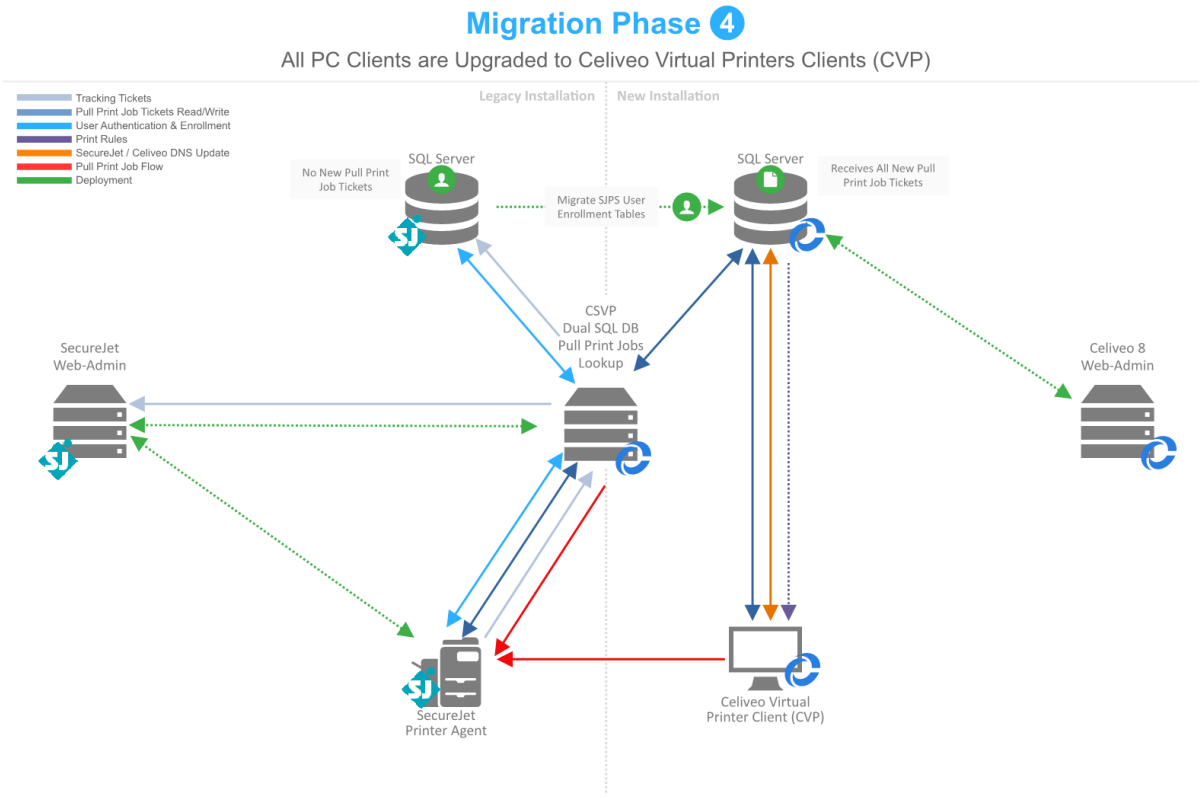
1. (Operation in the Workstations/Laptops) Run the MigrationCVP.exe – This process will remove the Job tickets for the target workstation from the legacy SecureJet SQL DB and move them to the Celiveo 8 SQL DB.
2. Install the CVP that was exported in phase 1.
3. This process will continue until all workstations are fully upgraded to Celiveo 8 CVP.
4. Note: Migrated Print Jobs that are manually deleted or expired will contain incorrect tracking paper size and currency data.



After migrating to a CSVP/CVP the tracking data of deleted or expired print jobs will be sent exclusively to the Celiveo 8 DB.

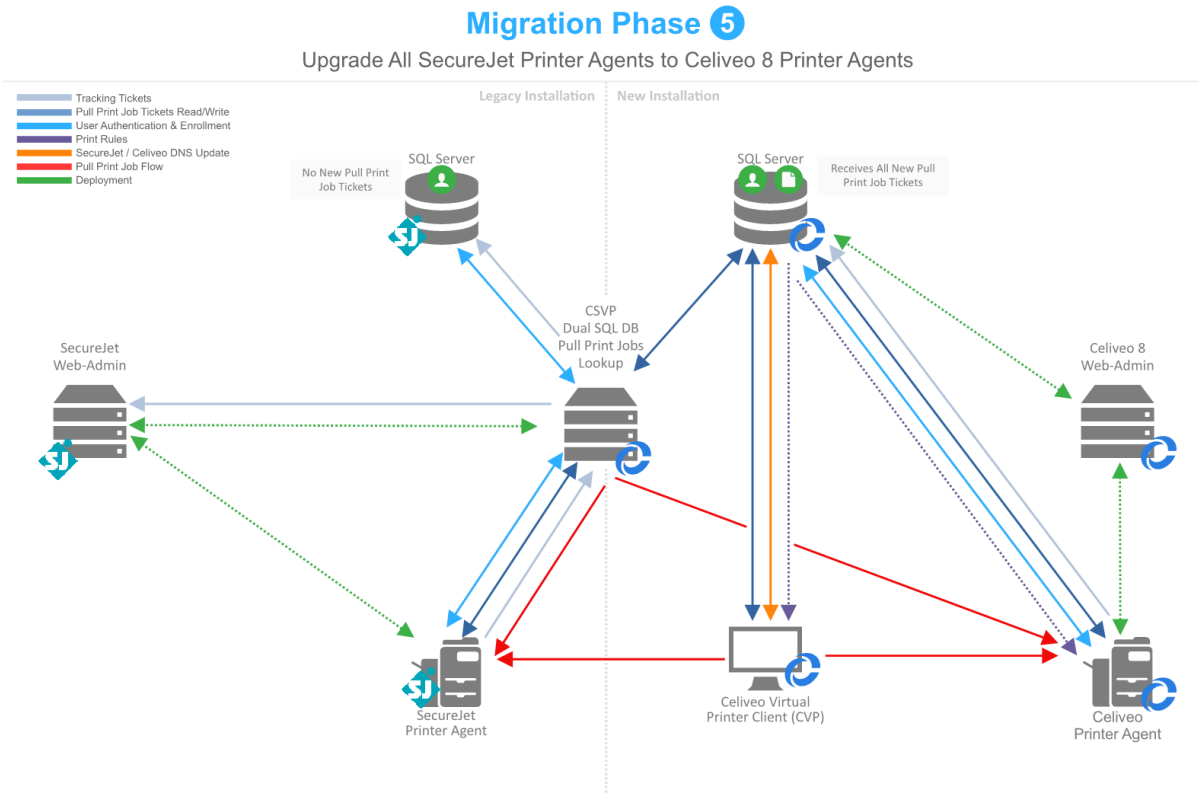
Phase 4

1. Once all workstations are fully upgraded to Celiveo 8 CVP a script needs to be ran on the legacy SecureJet SQL DB to migrate the SJPS Enrollment Tables to the Celiveo SQL DB.
2. At this point the legacy SecureJet DB won't receive Pull Print Job Tickets anymore as they'll all be submitted to the Celiveo 8 SQL DB.
3. The SecureJet SQL DB will still be used for Authentication and Tracking as long as there're SecureJet Printer Agents.



Phase 5

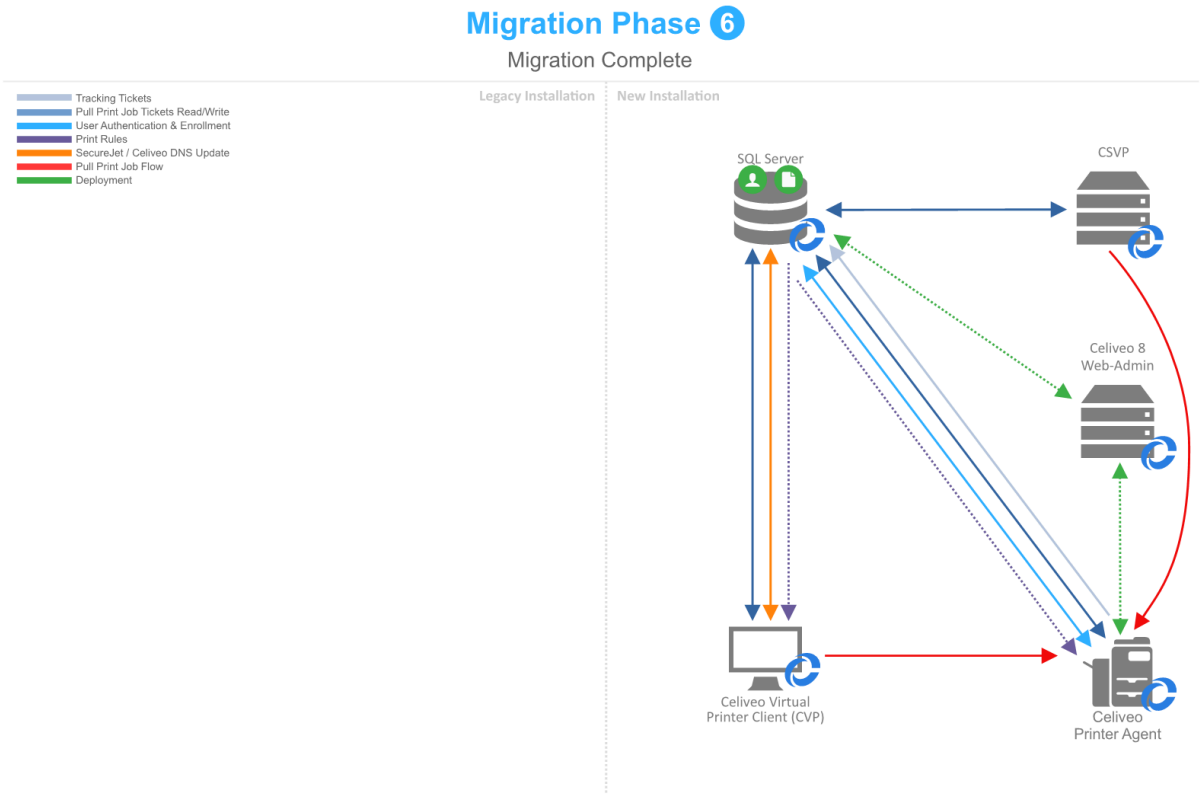
1. Progressively start migrating them SecureJet Printer Agents to Celiveo 8 Printer Agents. To achieve that add the printers to the Celiveo 8 Web-Admin, this process can be done manually, CSV list, or Celiveo CLI to automate the process.
2. Notes: SecureJet Printer Agents report tracking data to the SecureJet SQL DB and Celiveo Printer Agents report tracking to the Celiveo SQL DB.



> ! The SAP connector needs to be configured and installed on Phase 5 but can only fully operate once SecureJet / Celiveo is migrated to Celiveo 8 (Phase 6) because it requires Celiveo 8 Printer Agents. This also means that a printer with SecureJet/Celiveo Printer Agent should be kept until the very last moment to maintain the legacy system with SAP operability and then upgrade the printer.

Phase 6

1. Once all Printer Agents have been fully migrated to Celiveo 8 the migration process is complete.
2. At this point all Legacy Servers can be decommissioned. Note that if legacy tracking data is important then the legacy SQL DB (PrintManager80 / PrinterManager90) and respective TGS 7 / TGS 8 need to be kept.



[Migrate from SecureJet 7.0]

[Migrate from Celiveo 8.0.x]

Last modified: 29 September 2022

17.11.1. Migrate from SecureJet 7.0.x

Phase 1

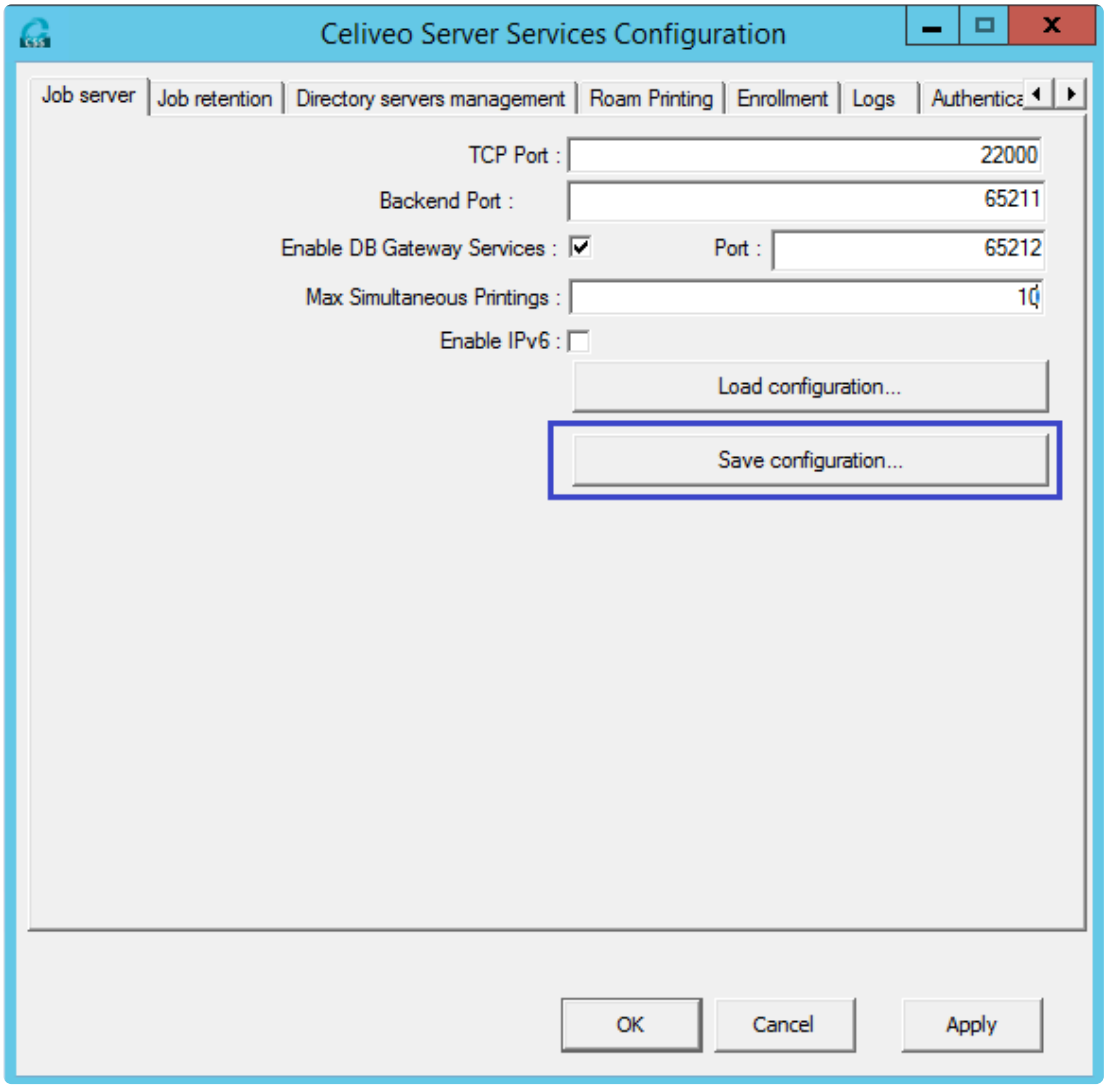
Before starting the migration validate that Phase 1 of the process described in the previous chapter is done.

Phase 2 – Replace SecureJet Server Services 7.0.x with CSVP

1. Open the Celiveo 8 Web Admin and create a CSVP. This CSVP should be created with an AD access profile.
2. Download the CSVP package and copy it to the SecureJet Server Services 7.0.x.
3. Back up the SecureJet Server Services 7.0.x configuration on the Celiveo 8 server:

> **Note:** a backup of the SecureJet Server Services 7.0.x configurations is recommended. If there is no backup, then the configurations need to be done manually to match the previous configurations after migrating SecureJet Server Services 7.0.x configuration to Celiveo 8 CSS that is part of the CSVP.

- Navigate to **C:\Program Files\Jetmobile\Celiveo Server Services**.
- Run **SJ Print-PS Configuration** as administrator.
- Click **Save Configuration…**

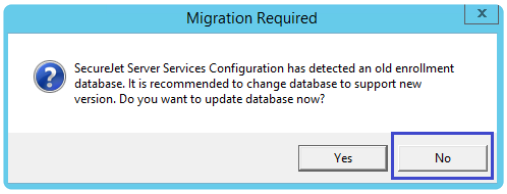


5. Execute the MigrationCVP.exe console application as Administrator on the SecureJet 7.0.x server. Once the MigrationCVP.exe console application is successfully run, unzip the CSVP package and install the CSVP as administrator.

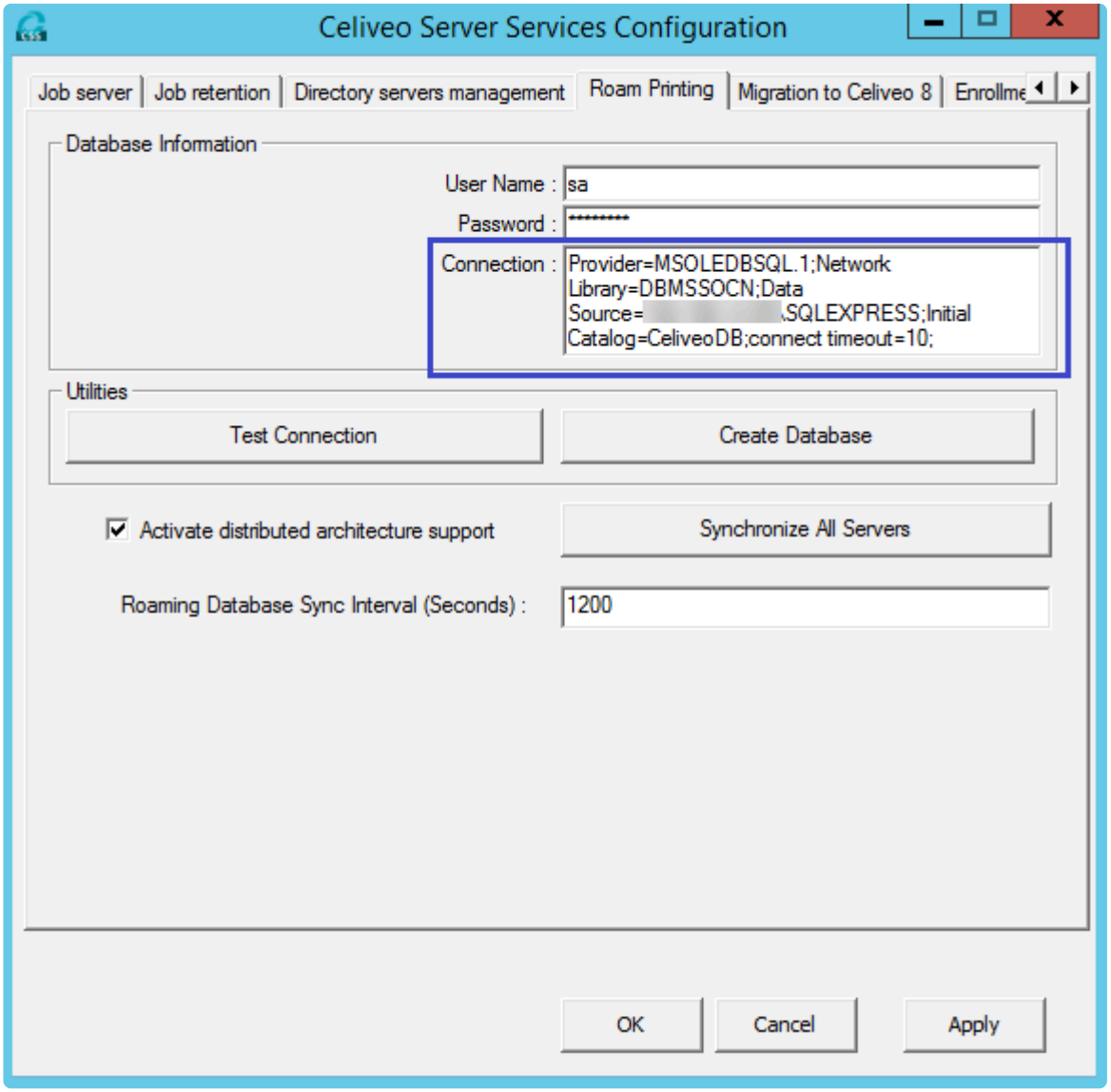
Notes:

- If the backup is made following the method given in step #4, the CSVP can be installed by simply running **installer.exe** on the CSVP package as an administrator. The default TCP Port on the CSS configurations will be '22000'.
- If the CSS backup is not performed on step #4 and if a different TCP port needs to be defined, please use the following method to install the CSVP on the Celiveo 8.0.x server:
    1. Open the command prompt as administrator.
    2. Go to the unzipped CSVP package folder using the command prompt.
    3. Type **installer.exe -p< PORT_NUMBER >** Ex: installer.exe -p2000

6. Once the CSVP installation is complete, navigate to **C:\Program Files\Celiveo\Celiveo Server Services** and open **SJ Print-PS Configuration** as administrator. If it prompts to upgrade the enrollment database, click 'No'.

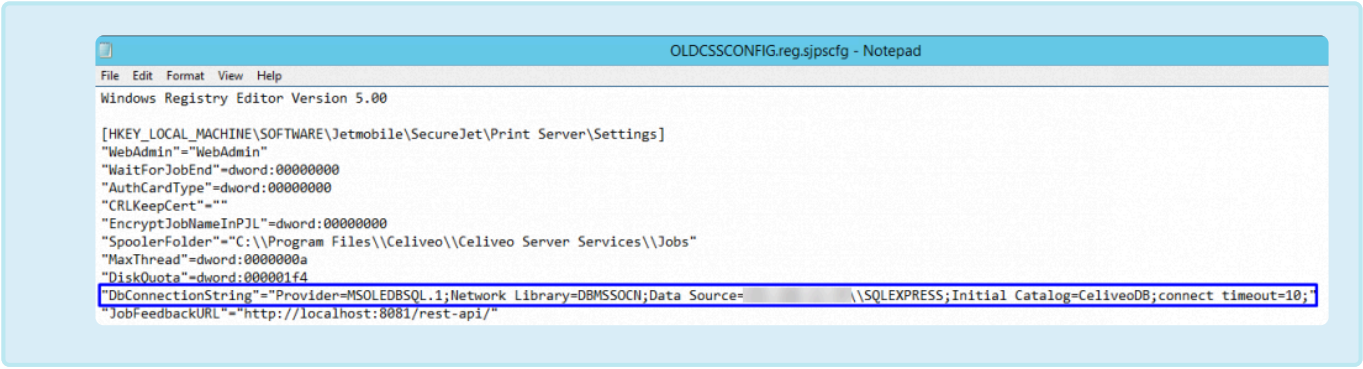


7. Navigate to the **Roam Printing** tab and copy the connection string.

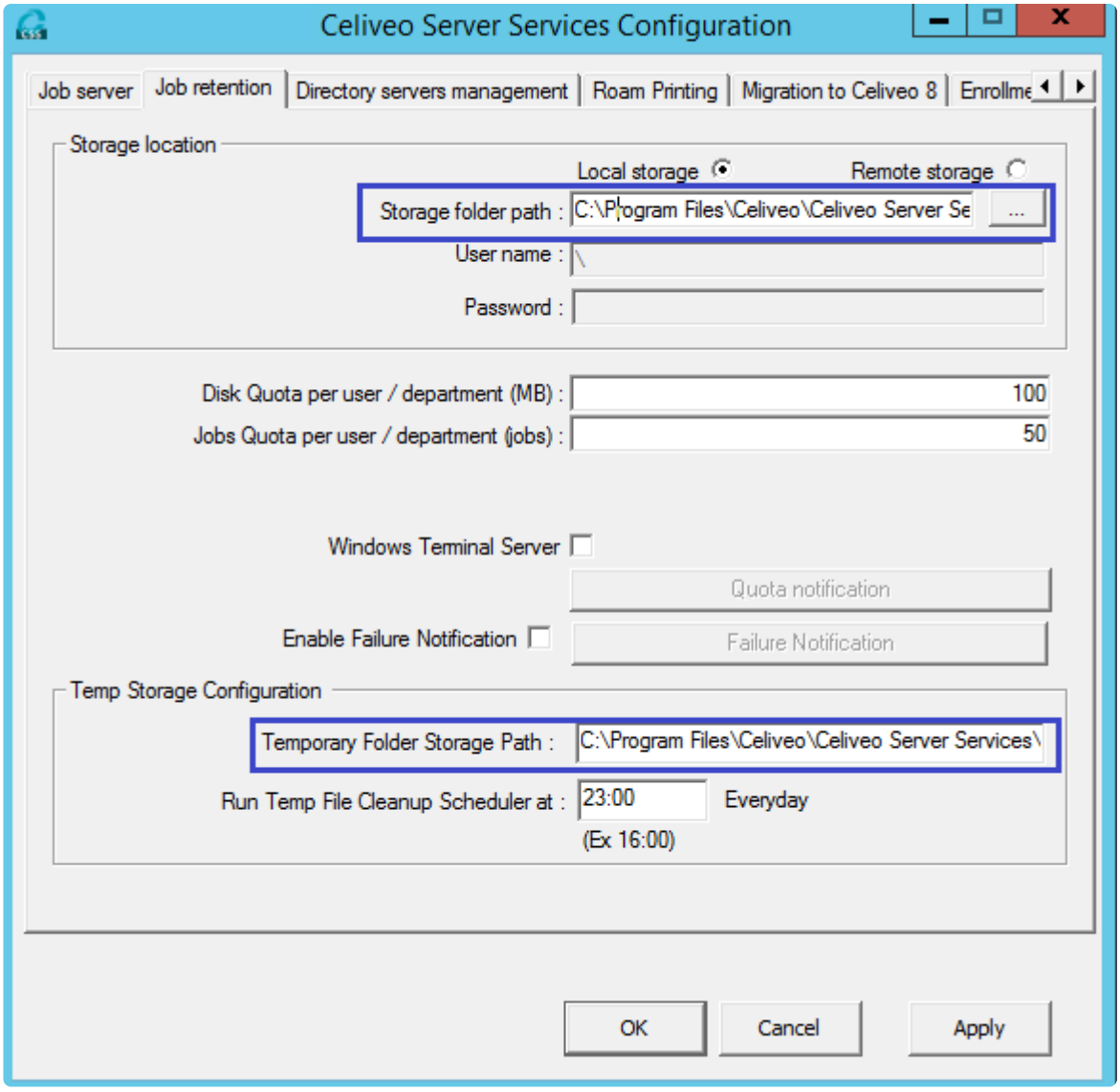


Open the saved SSS configuration file and replace the SJ 7.0.x DBConnectionString with the Celiveo 8 DBConnectionString.
"DbConnectionString"="Provider=MSOLEDBSQL.1;Network Library=DBMSSOCN;Data Source=\\;Initial Catalog=CeliveoDB;connect timeout=10;"

> Note: Make sure to replace any slash (\) on the connection string with double slashes (\\)

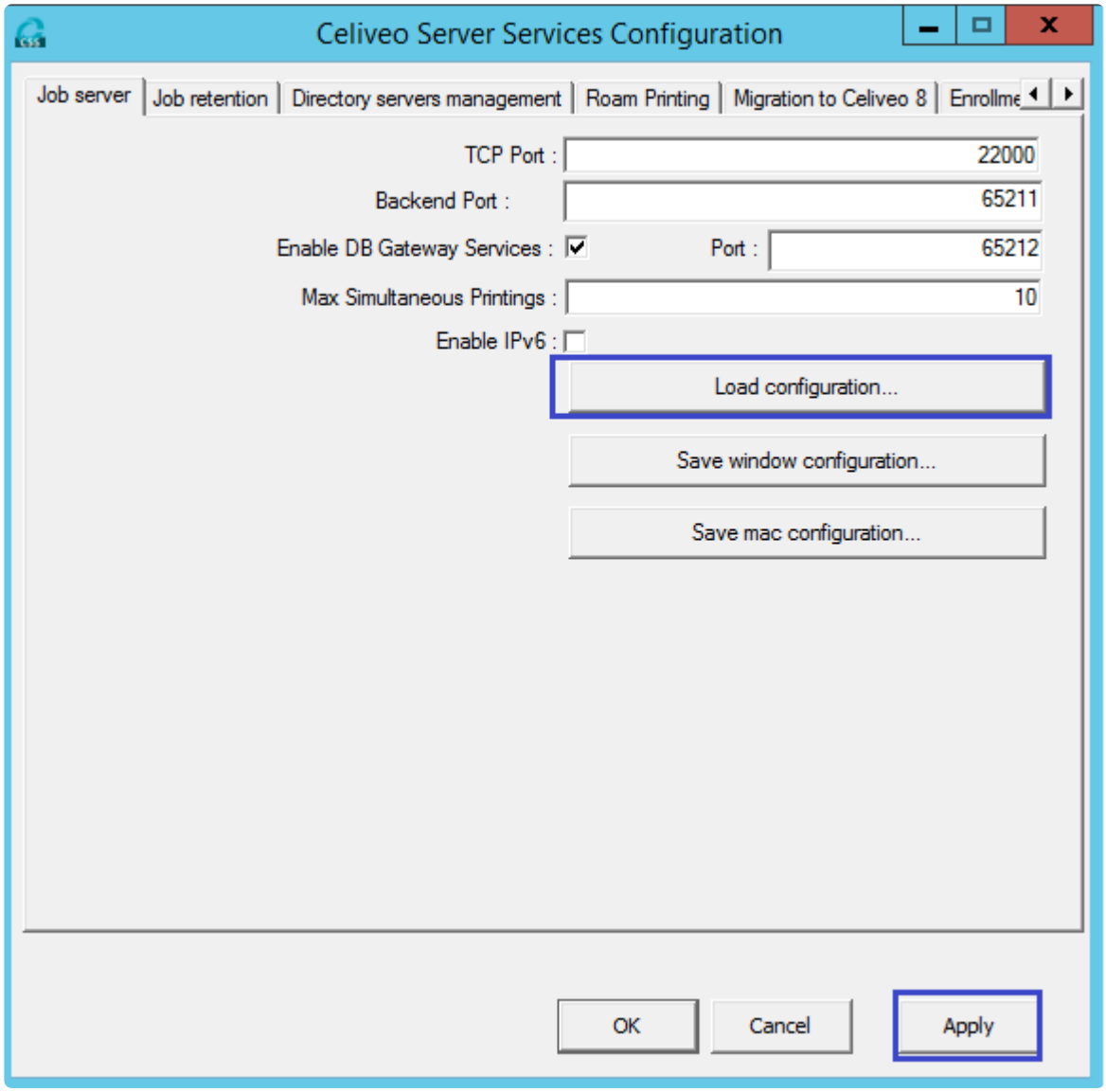


8. If the old SSS configurations are not saved, all tabs need to be manually configured to match the existing configurations on the previous SSS except for the **Job retention** tab.
9. Storage folder path and Temporary Folder Storage Path on the Job retention tab should always point to Celiveo Server Services as indicated below:
   Storage folder path = C:\Program Files\Celiveo\Celiveo Server Services\Jobs
   Temporary Folder Storage Path = C:\Program Files\Celiveo\Celiveo Server Services\Temp

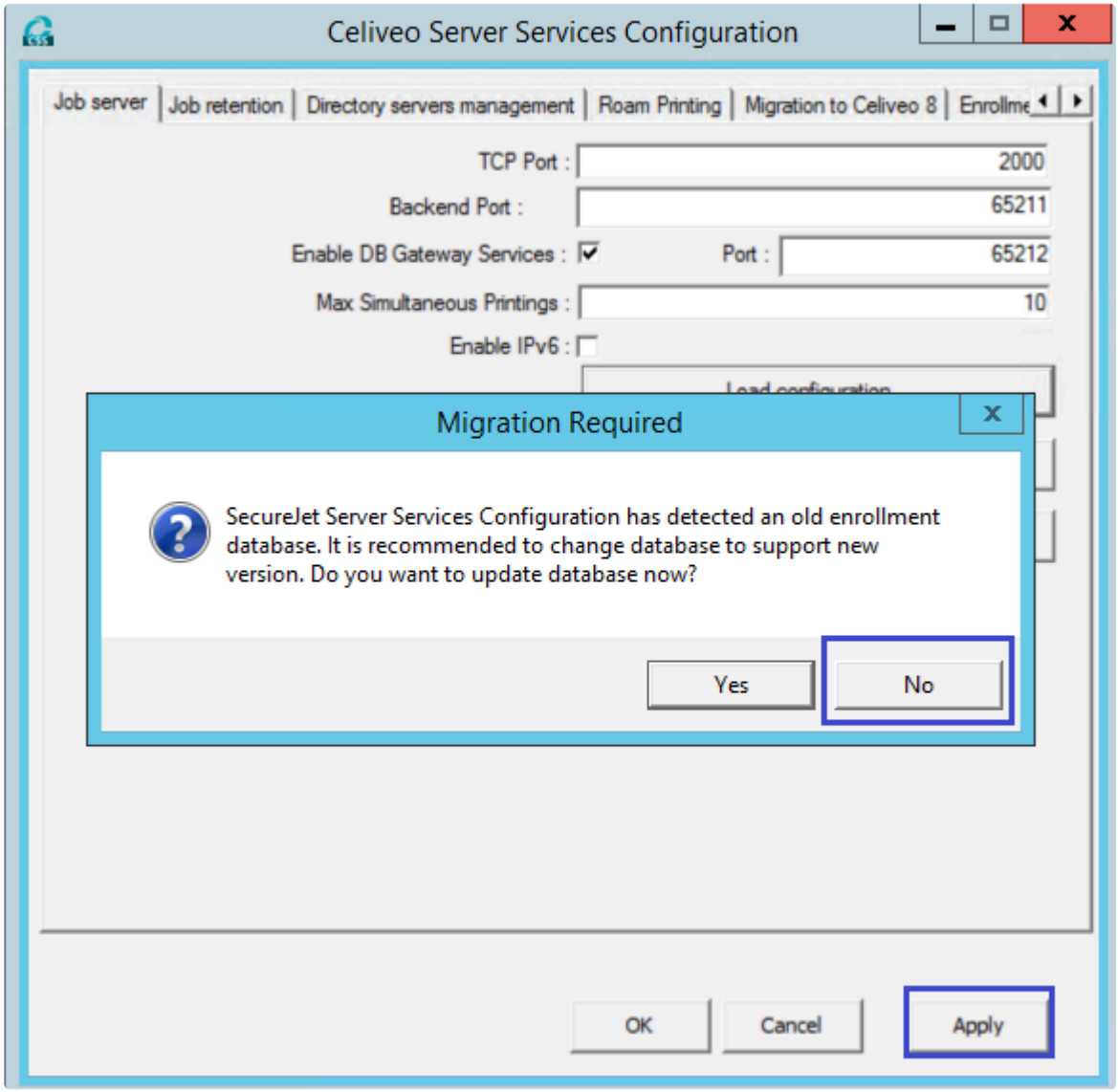


If the old SSS configurations are saved, proceed to the following steps:

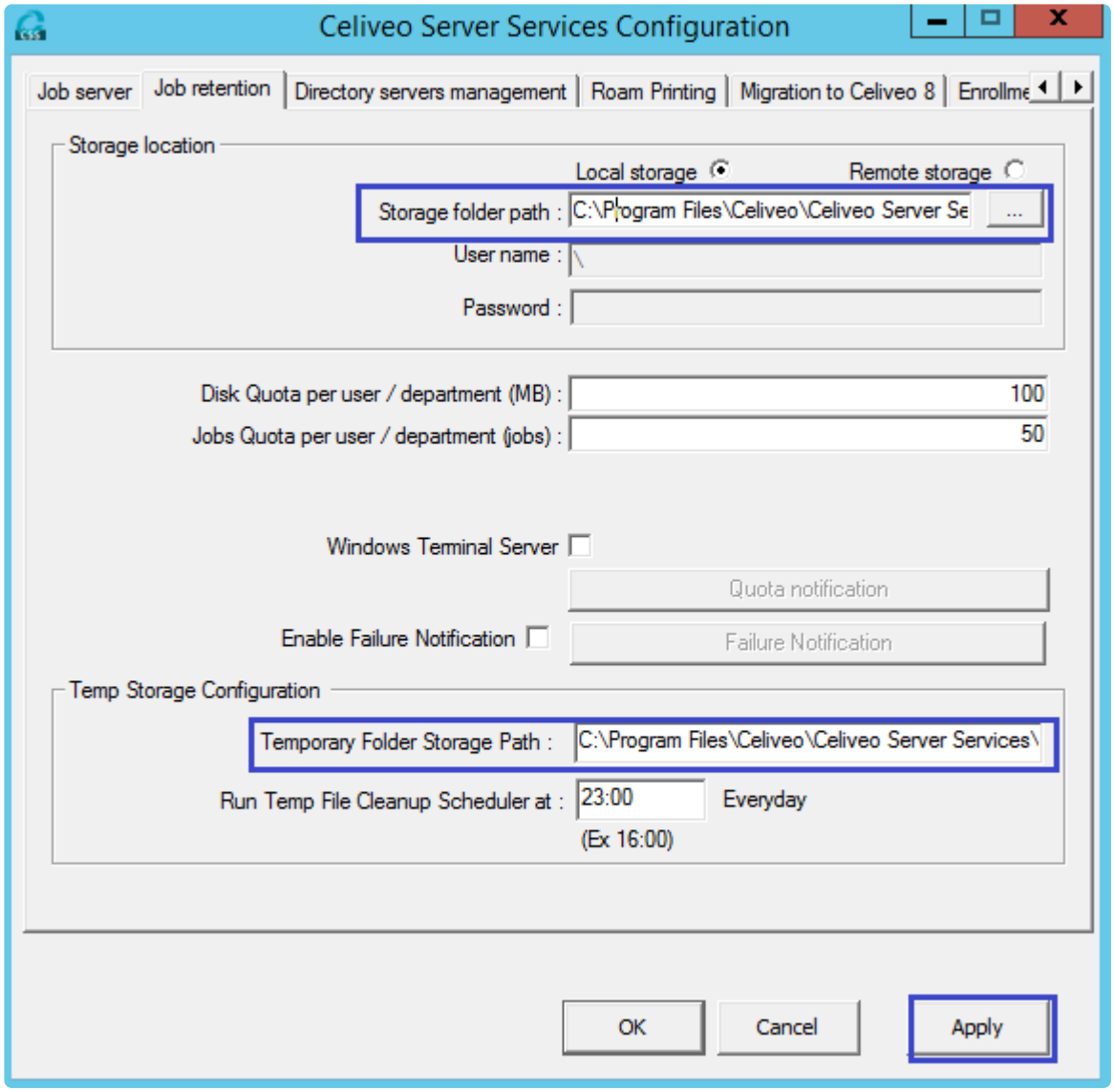
a. Navigate to the **Job Server** tab and click **Load configuration…** to load the SSS configurations saved on step #4. Once the configuration is loaded, click **Apply**.



Once the old configurations are loaded, if it prompts to upgrade the enrollment database, click **No** and **Apply the changes**.

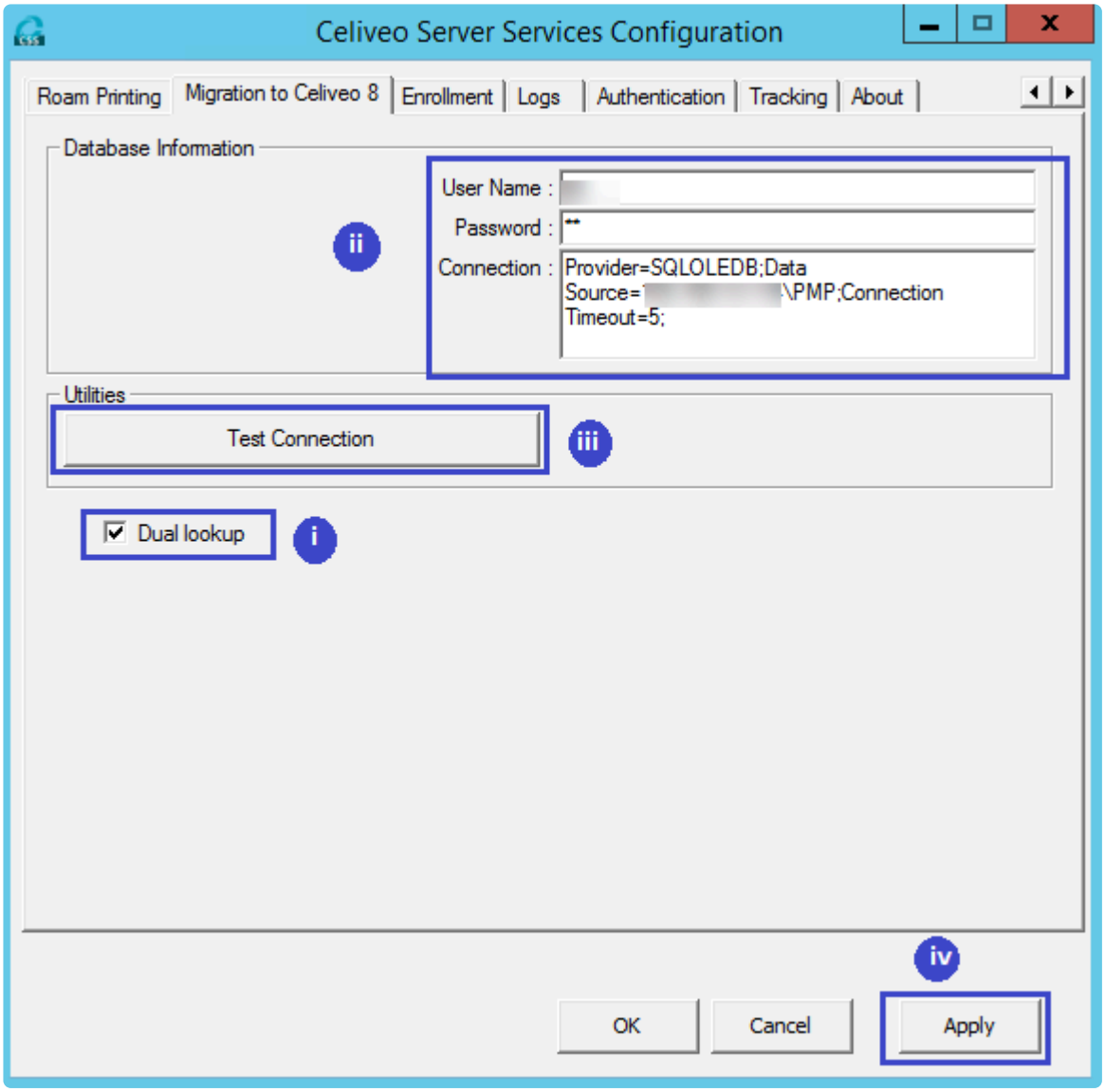


b. Navigate to the **Job retention** tab and edit the **Storage folder path** and **Temporary Folder Storage** fields as indicated below and click **Apply**.
_Storage folder path = C:\Program Files\Celiveo\Celiveo Server Services\Jobs
Temporary Folder Storage Path = C:\Program Files\Celiveo\Celiveo Server Services\Temp_



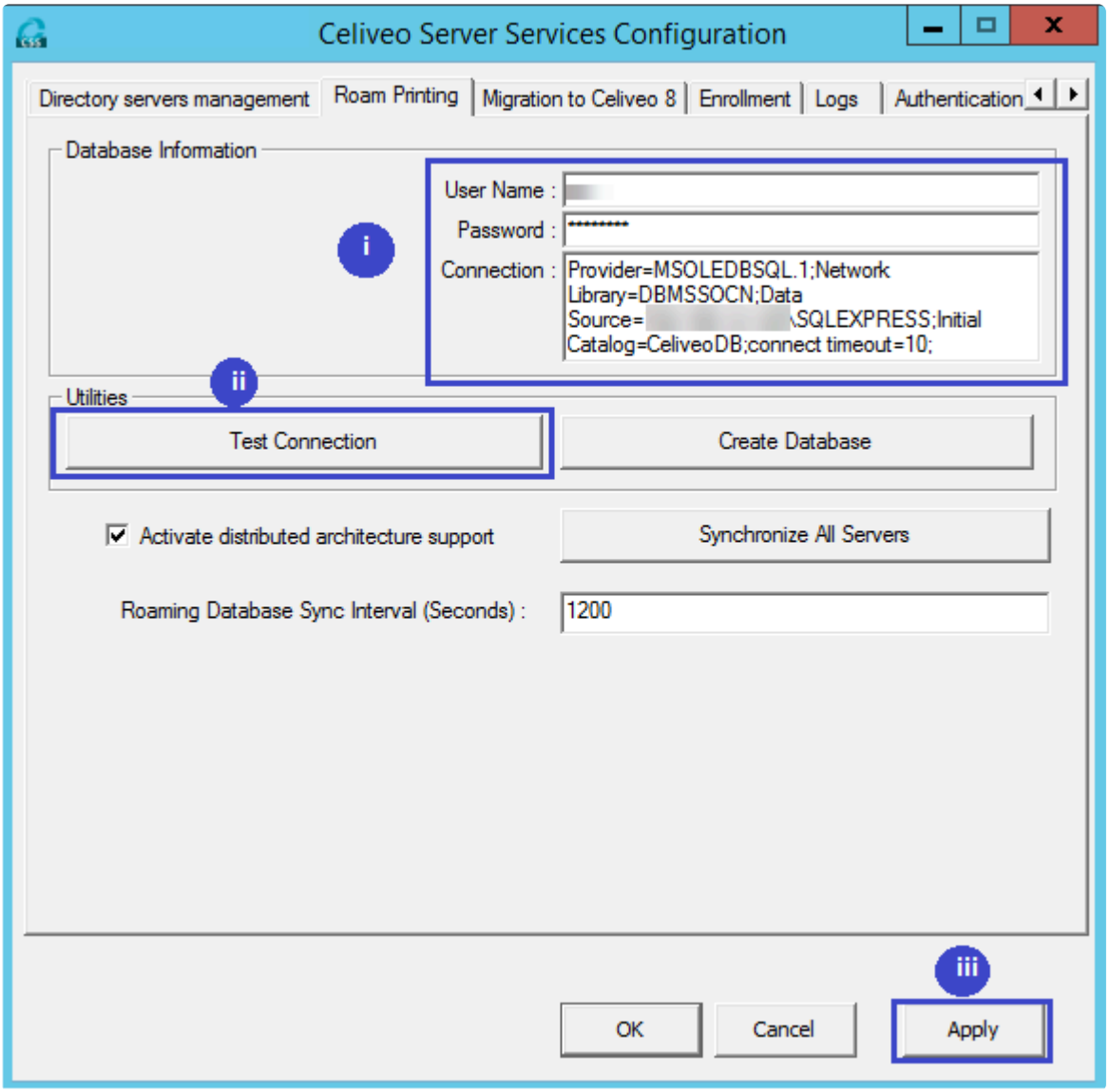
- Navigate to the **Migration to Celiveo 8** tab and perform the following steps:

i. Enable the **Dual lookup** checkbox.
ii. Enter the SJ7.0.x connection string.
iii. Test the connection.
iv. Once the connection is successful, click **Apply**.

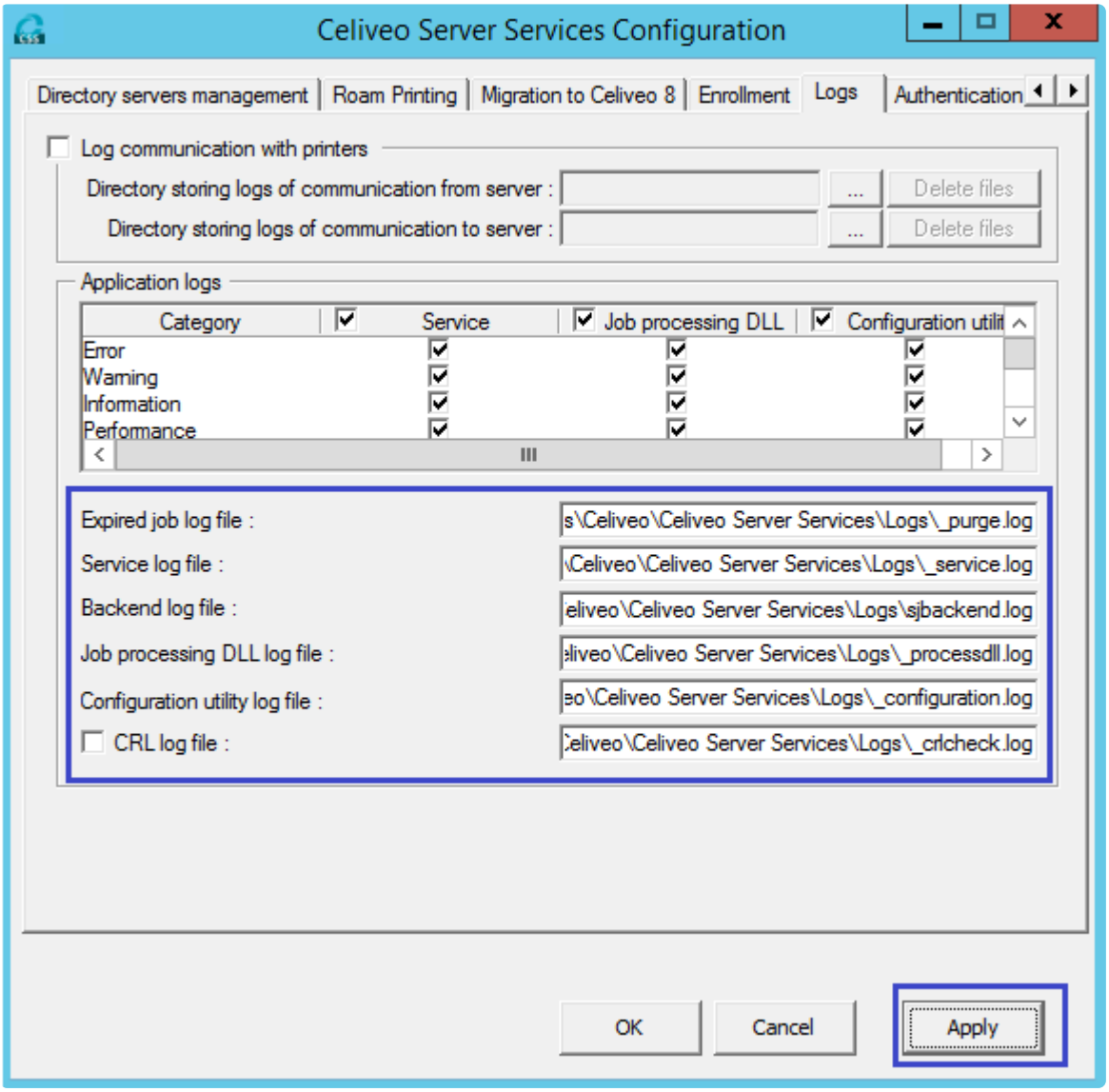


- Navigate to the **Roam Printing** tab and perform the following steps:

i. Make sure that the database connection string is pointing to the Celiveo 8 database.
Note: To avoid any error, install the MSOLEDBSQL driver on the SecureJet Server Services 7.0.x.
ii. Test the connection.
iii. Once the connection is successful, click **Apply**.



e. Navigate to the **Logs** tab and replace the existing log paths which point to SecureJet Server Services with Celiveo Server Services as indicated below
_Expired job log file = C:\Program Files\Celiveo\Celiveo Server Services\Logs_purge.log
Service log file = C:\Program Files\Celiveo\Celiveo Server Services\Logs_service.log
Backend log file = C:\Program Files\Celiveo\Celiveo Server Services\Logs\sjbackend.log
Job processing DLL log file = C:\Program Files\Celiveo\Celiveo Server Services\Logs_processdll.log
Configuration utility log file = C:\Program Files\Celiveo\Celiveo Server Services\Logs_configuration.log
CRL log file = C:\Program Files\Celiveo\Celiveo Server Services\Logs_crlcheck.log_



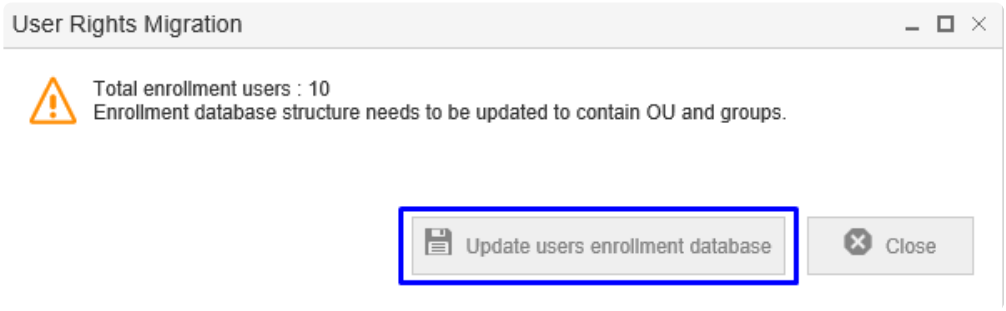
Phase 3 – Migrate SecureJet Serverless Pull Print Clients to Celiveo 8 CVP

1. Create a CVP from the Celiveo 8 Web Admin.
2. Download the CVP package and install it on the SecureJet 7.0.x SPP client.
3. Execute the MigrationCVP.exe console application as an administrator on the SJ7.0.x SPP client.
4. Once the MigrationCVP.exe console application is successfully run, unzip the CVP package and install the CVP as administrator.
5. Once the CVP installation is complete, perform a sign-out/sign-in on the client PC.

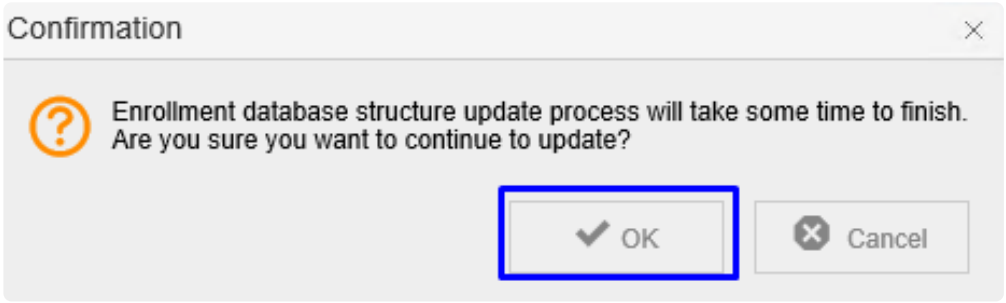
Phase 4 – Migrate the SJPS User Enrollment Table to the new SQL DB

1. In SecureJet 7.0.x database, right-click on **SJPS > Task > Generate Script > Next**
2. Select **Select specific database table > select dbo.T_Enrollment > Next**
3. Provide a name and a path for the file.
4. Click **Advanced**.

5. Select **Data only** in the *Types of data to script *
6. Click **OK** then **Next**.
7. Copy the script to the Celiveo 8 database.
8. Execute the script on the Celiveo 8 database. **Note**: Make sure to log out and close all the opened Celiveo 8 Web Admin windows.
9. Since the Celiveo 8 Web Admin has been opened before at least once, delete all records in the table dbo.MigrationStatus from the database.
10. Open the Celiveo 8 Web Admin and Log in.
11. Select **Update users enrollment database**.

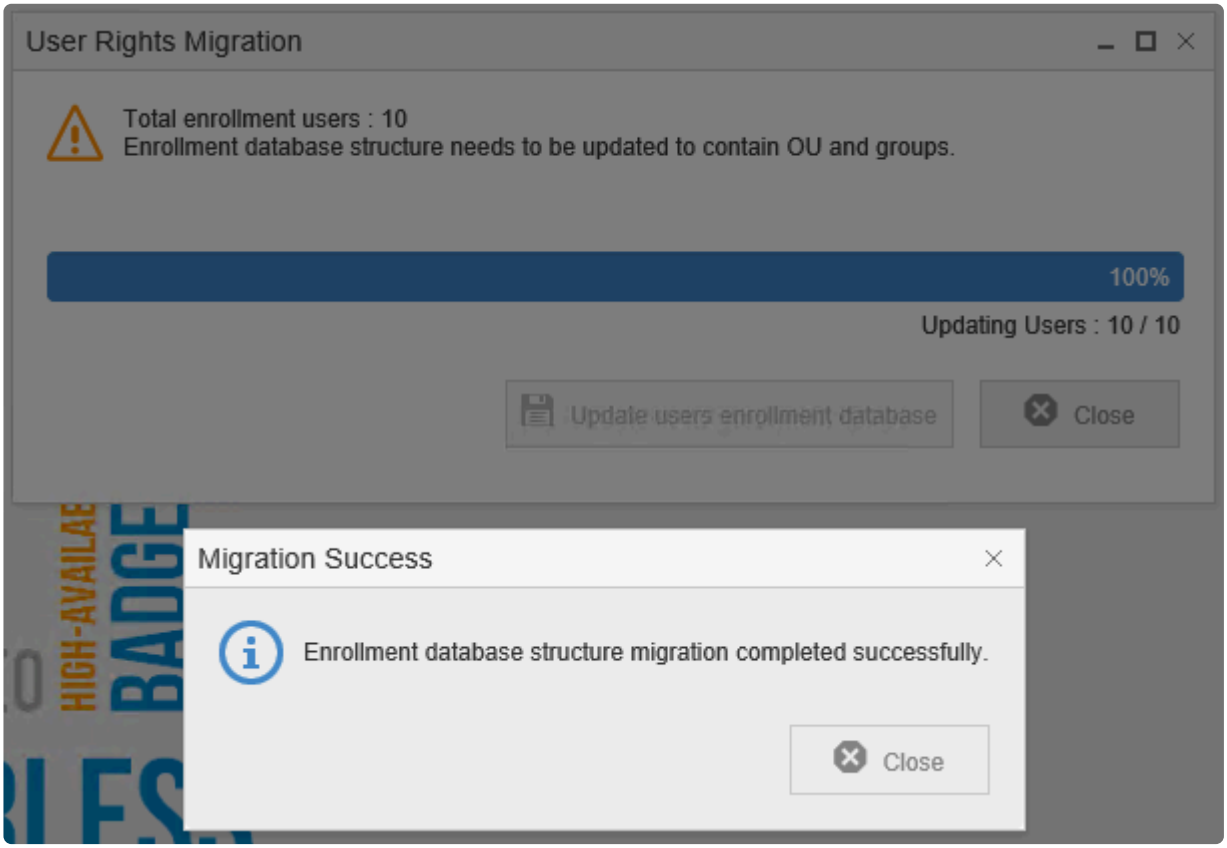


12. Click **OK** to confirm.

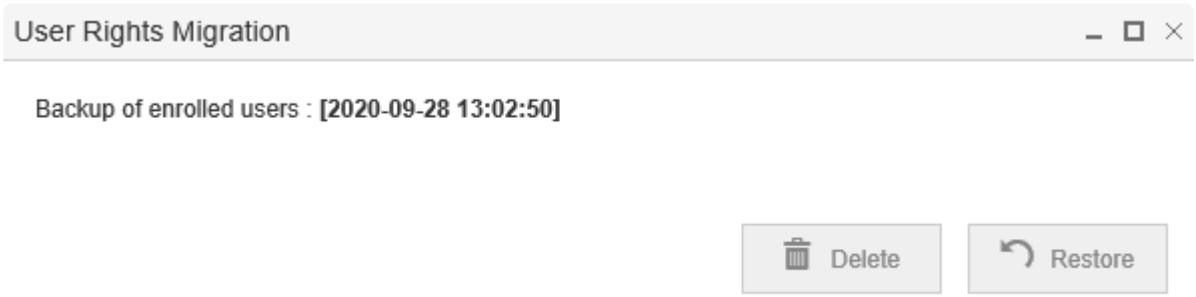


The migration starts.

13. Once the migration is successful, a confirmation message displays.



14. Close the backup popup.



Limitations

- A user cannot have a mix of SecureJet 7.0.x Serverless Pull Print Clients and Celiveo 8 CVP client workstations. If a user has multiple SecureJet 7.0.x Serverless Pull Print Clients, all of them need to be upgraded to Celiveo 8 CVP clients in order to use the Celiveo functionalities.
- Once the enrollment table is migrated, the users should not enroll using SecureJet 7.0.x printers.
- If there is any job left with the SecureJet 7.0.x Serverless Pull Print Client, the jobs will be migrated to the new Celiveo 8 database upon the migration of the SPP client to the Celiveo 8 CVP client. However, the tracking details listed below will not appear on the reports for the expired and deleted migrated jobs.
  For deleted jobs:
  [PrinterFormatterNumber] = NULL
  [Language] = Blank
  [UserGroups] = NULL
  [UserOUs] = NULL
  For Expired jobs:
  [Language] = Blank
  [UserGroups] = NULL
  [UserOUs] = NULL
- If there is any job left with the SecureJet 7.0.x Serverless Pull Print Client, the jobs will be migrated to the new Celiveo 8 database upon the migration of the SecureJet 7.0.x Serverless Pull Print Client to the Celiveo 8 CVP client. However, the tracking information for the migrated jobs will not be displayed under FQDN and the currency will be based on the client machine's local system account settings.
- Printer details for deleted jobs will not be available in the Celiveo 8 database after migrating the SJ7.0.x server SSS to Celiveo 8 CSS. Printer details will be populated only if that particular printer is available on the Celiveo 8 DB.
- Jobs generated from a SJ7.0.x SPP client will not be retrieved from a Celiveo 8 printer until the SJ7.0.x SPP client is upgraded to Celiveo 8 CVP client.

Last modified: 29 September 2022

17.11.2. Migrate from Celiveo 8.0.x

Phase 1

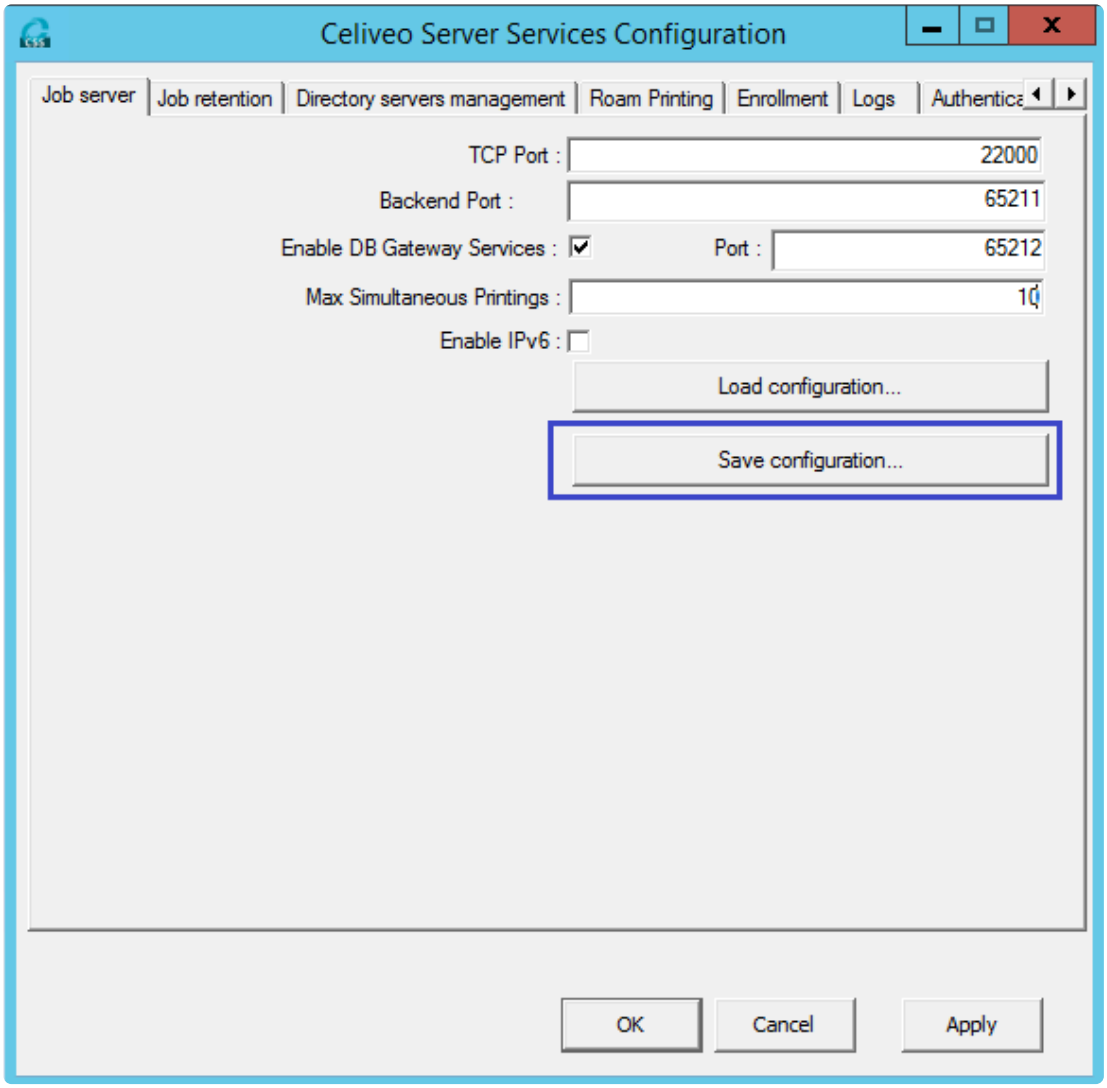
Before starting the migration validate that Phase 1 of the process described in the previous chapter is done.

Phase 2 – Replace Celiveo Server Services 8.0.x with CSVP

1. Install the Celiveo 8 Web Admin on a separate server.
2. Open the Celiveo 8 Web Admin and create a CSVP. This CSVP should be created with an AD access profile.
3. Download the CSVP package and copy it to the Celiveo 8.0.x server.
4. Back up the Celiveo Server Services configuration on the Celiveo 8.0.x server:

> **Note:** a backup of the Celiveo 8.0.x server CSS configurations is recommended. If there is no backup, then the configurations need to be done manually to match the previous configurations after migrating Celiveo 8.0.x CSS to Celiveo 8 CSS.

- Navigate to **C:\Program Files\Jetmobile\Celiveo Server Services**.
- Run **SJ Print-PS Configuration** as administrator.
- Click **Save Configuration…**

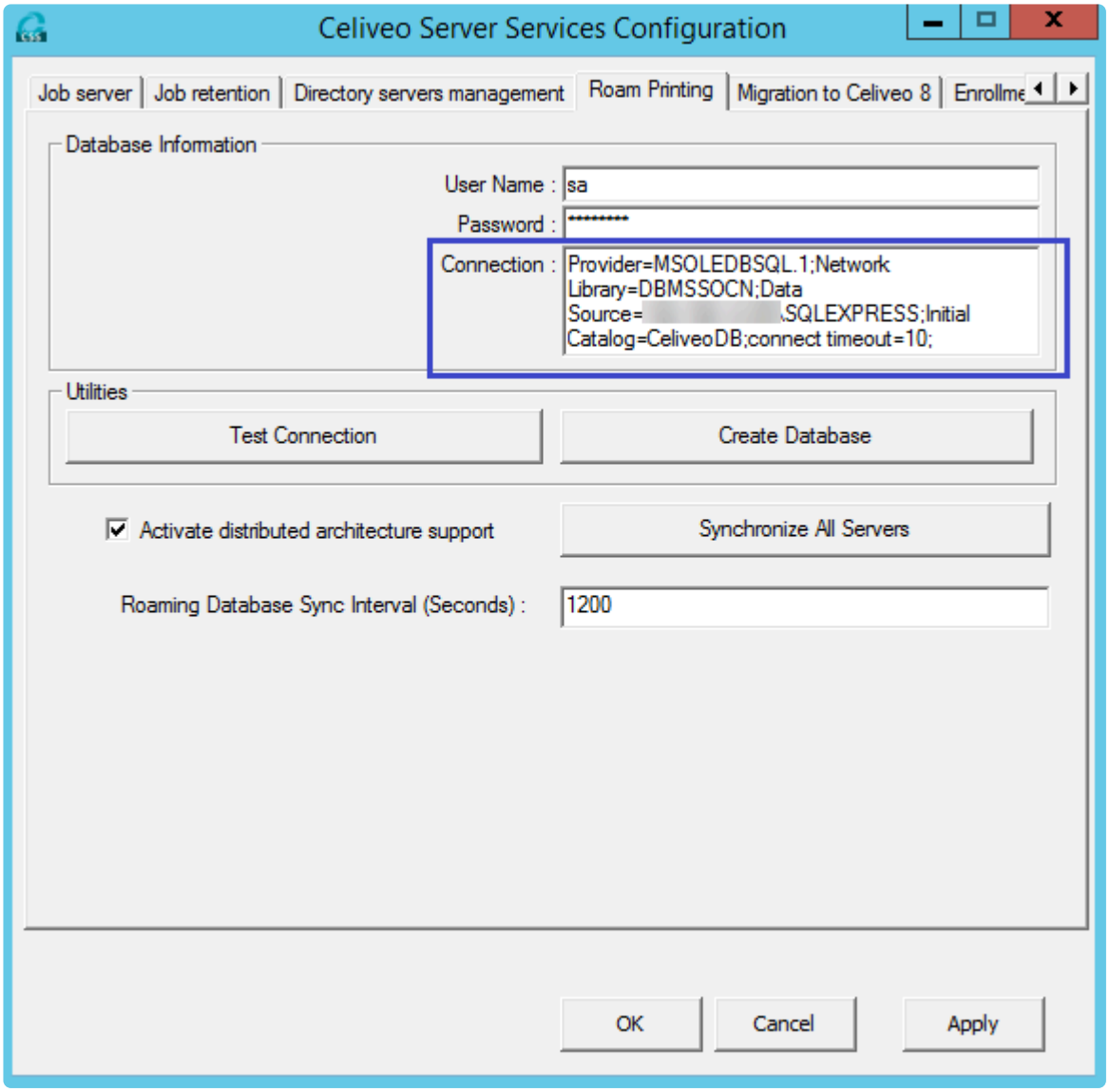


5. Execute the MigrationCVP.exe console application as Administrator on the Celiveo 8.0.x server.
Once the MigrationCVP.exe console application is successfully run, unzip the CSVP package and install the CSVP as administrator.

Notes:

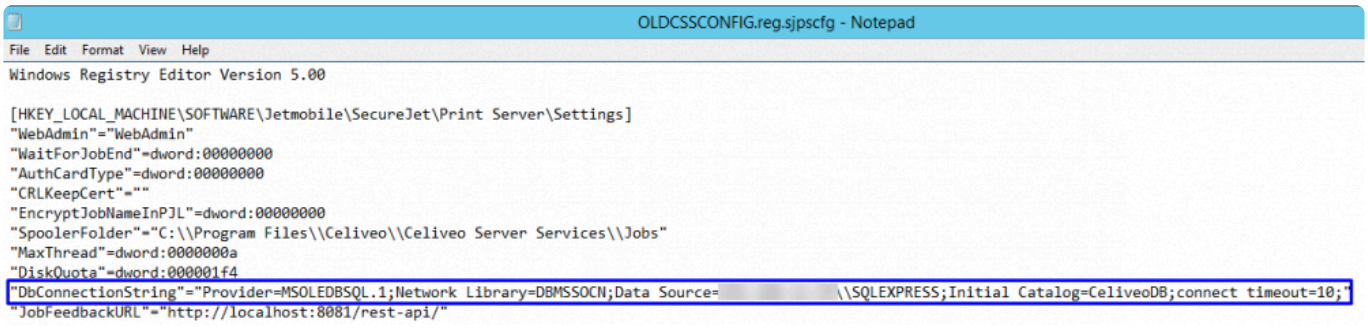
- If the backup is made following the method given in step #4, the CSVP can be installed by simply running **installer.exe** on the CSVP package as administrator. The default TCP Port on the CSS configurations will be '22000'.
- If the CSS backup is not performed on step #4 and if a different TCP port needs to be defined, please use the following method to install the CSVP on the Celiveo 8.0.x server:
    1. Open the command prompt as administrator.
    2. Go to the unzipped CSVP package folder using the command prompt.
    3. Type **installer.exe -p< PORT_NUMBER >** Ex: installer.exe -p2000

6. Once the CSVP installation is complete, navigate to **C:\Program Files\Celiveo\Celiveo Server Services** and open **SJ Print-PS Configuration** as administrator.
7. Navigate to the **Roam Printing** tab and copy the connection string.



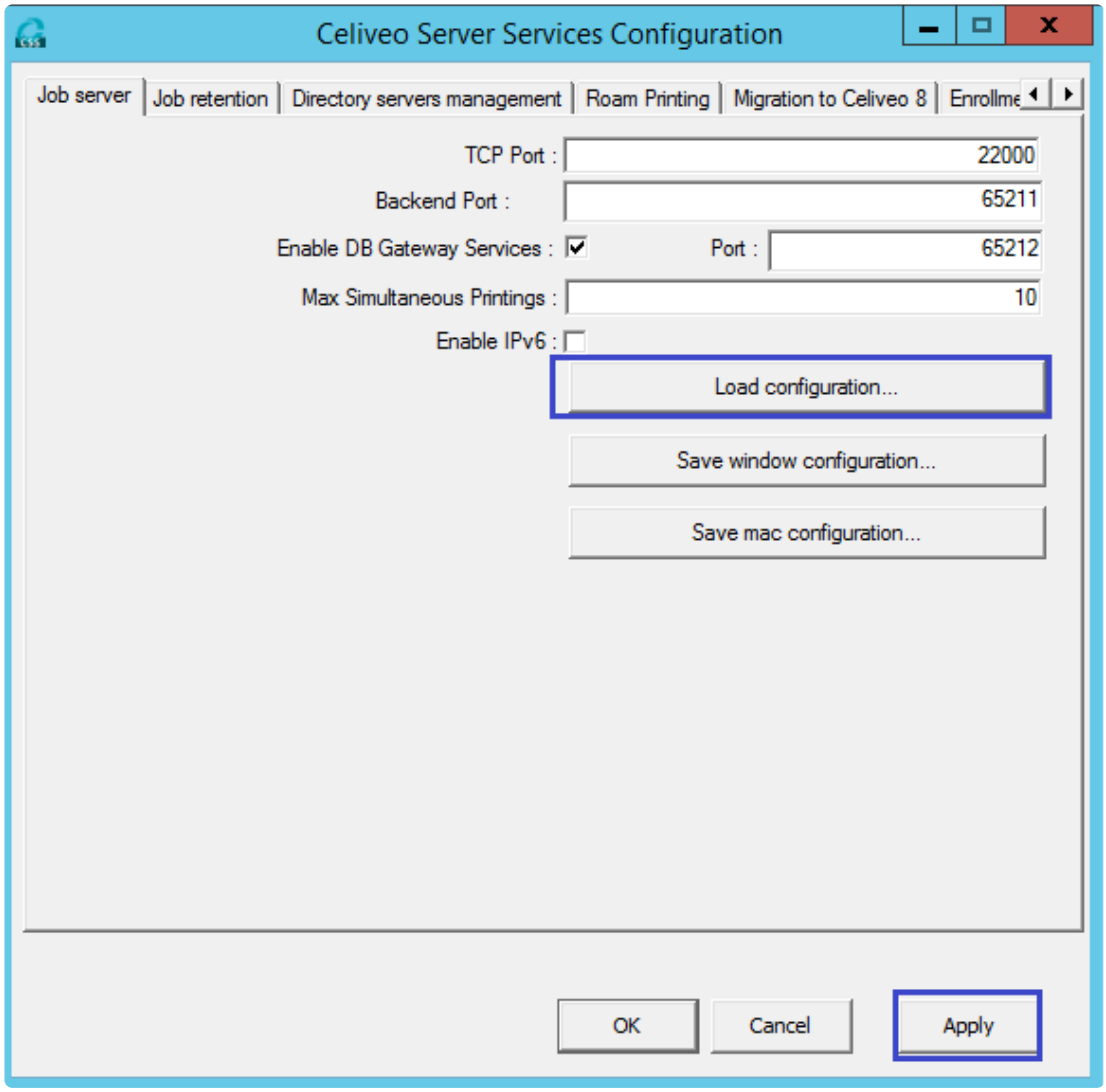
Open the saved CSS configuration file and replace the Celiveo8.0.x DBConnectionString with the Celiveo 8 DBConnectionString.
"DbConnectionString"="Provider=MSOLEDBSQL.1;Network Library=DBMSSOCN;Data Source=\\;Initial Catalog=CeliveoDB;connect timeout=10;"

Note: Make sure to replace any slash (\) on the connection string with double slashes (\\)



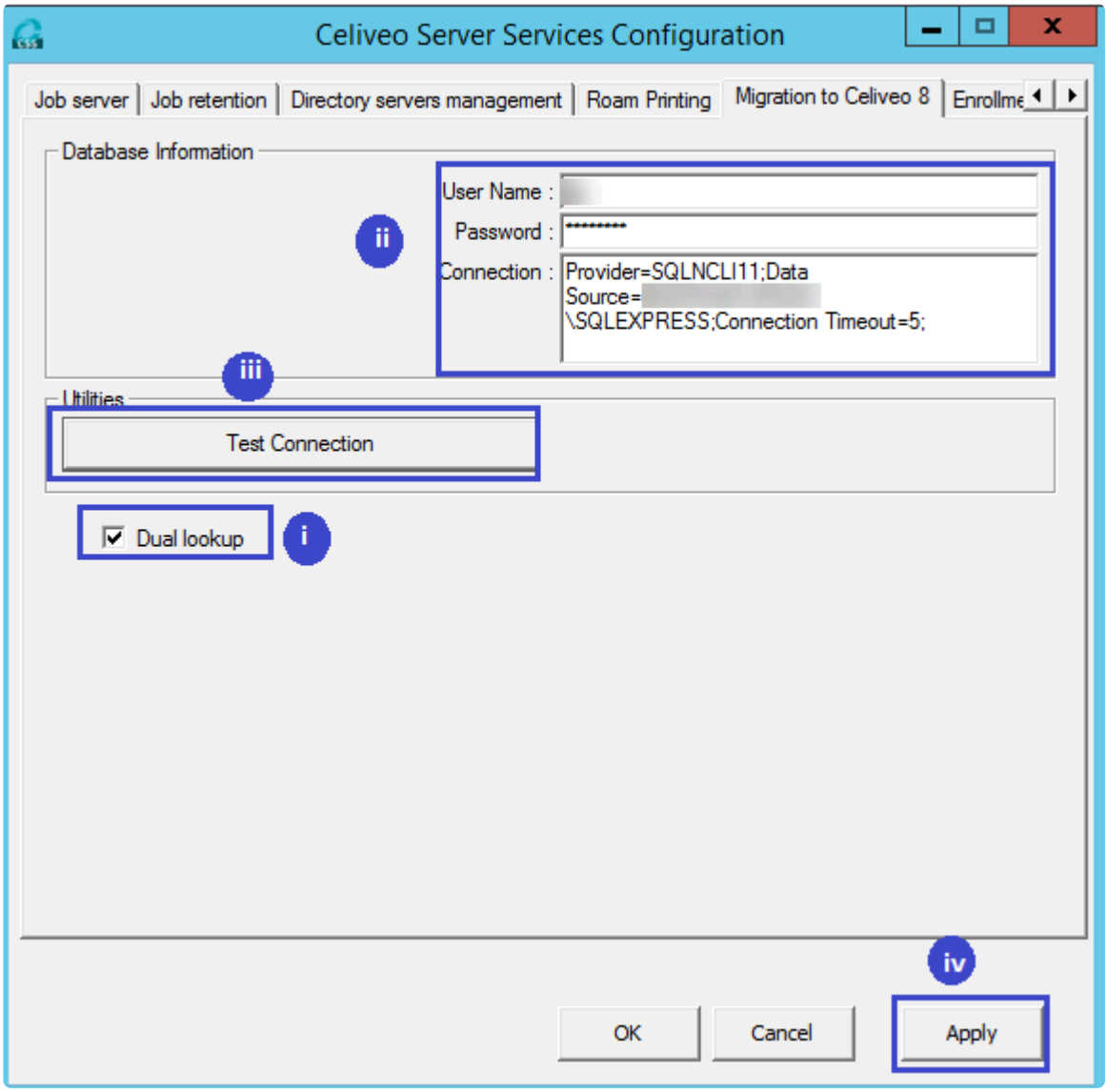
- If the old CSS configurations are not saved, all tabs need to be manually configured to match the existing configurations on the previous CSS.
- If the old CSS configurations are saved, follow the steps below:

1. Navigate to the **Job Server** tab and click **Load configuration**… to load the SSS configurations saved on step #4. Once the configuration is loaded, click **Apply**.



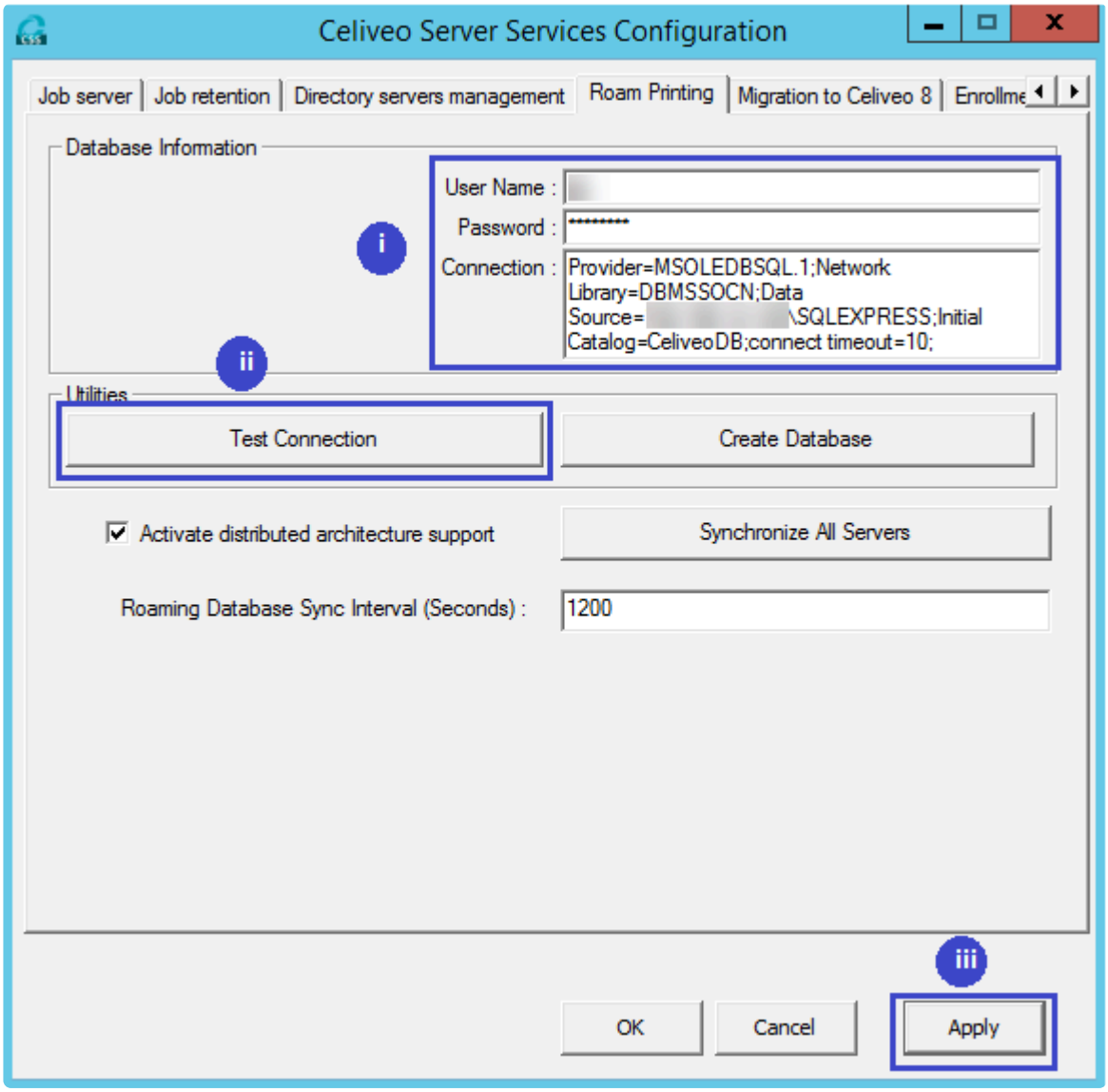
2. Navigate to the **Migration to Celiveo 8** tab and perform the following steps:

i. Enable the **Dual lookup** checkbox.
ii. Enter the Celiveo 8.0.x connection string.
iii. Test the connection.
iv. Once the connection is successful, click **Apply**.

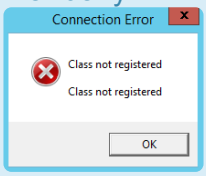


3. Navigate to the **Roam Printing** tab and perform the following steps:

i. Enter the Celiveo 8 connection string.
ii. Test the connection.
iii. Once the connection is successful, click **Apply**.



Note: If you encounter the error below, you need to install the MSOLEDB driver manually.

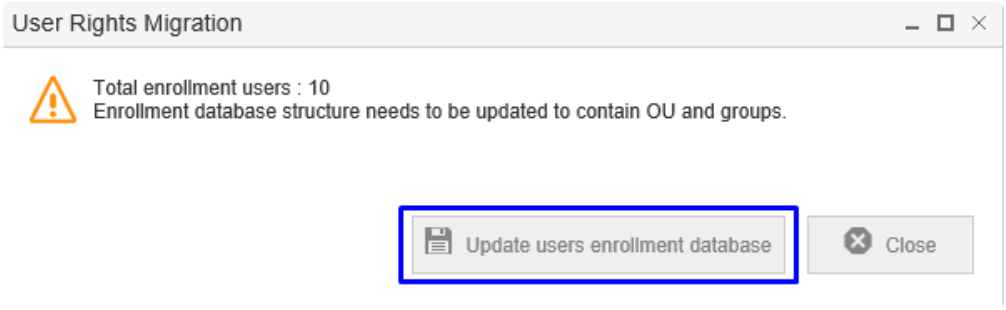


Phase 3 – Migrate Celiveo 8.0.x Serverless Pull Print Clients to Celiveo CVP

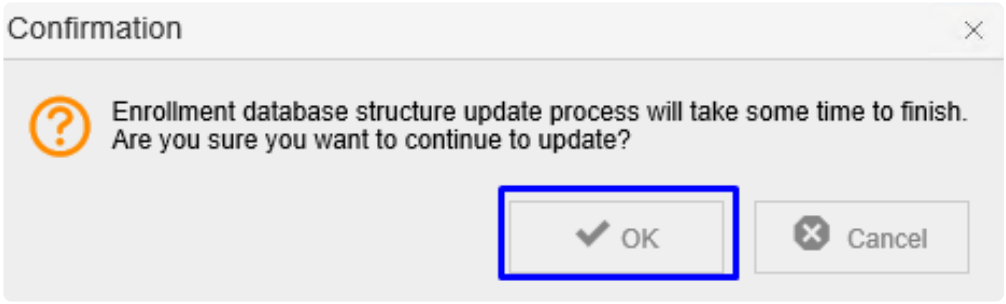
1. Create a CVP from the Celiveo 8 Web Admin.
2. Download the CVP package and copy it to the Celiveo 8.0.x SPP client.
3. Execute the MigrationCVP.exe console application as Administrator on the Celiveo 8.0.x client.
4. Once the MigrationCVP.exe console application is successfully run, unzip the CVP package and install the CVP as administrator.
5. Once the CVP installation is complete, perform a sign-out/sign-in on the client PC.

Phase 4- Migrate the SJPS User Enrollment Table to the new SQL DB

1. In Celiveo 8.0.x database, right-click on **SJPS > Task > Generate Script > Next**
2. Select **Select specific database table > select dbo.T_Enrollment > Next**
3. Provide a name and a path for the file.
4. Click **Advanced**.
5. Select **Data only** in the *Types of data to script *
6. Click **OK** then **Next**.
7. Copy the script to the Celiveo 8 database.
8. Execute the script on the Celiveo 8 database. **Note**: Make sure to log out and close all the opened Celiveo 8 Web Admin windows.
9. Since the Celiveo 8 Web Admin has been opened before at least once, delete all records in the table dbo.MigrationStatus from the database.
10. Open the Celiveo 8 Web Admin and Log in.
11. Select **Update users enrollment database**.

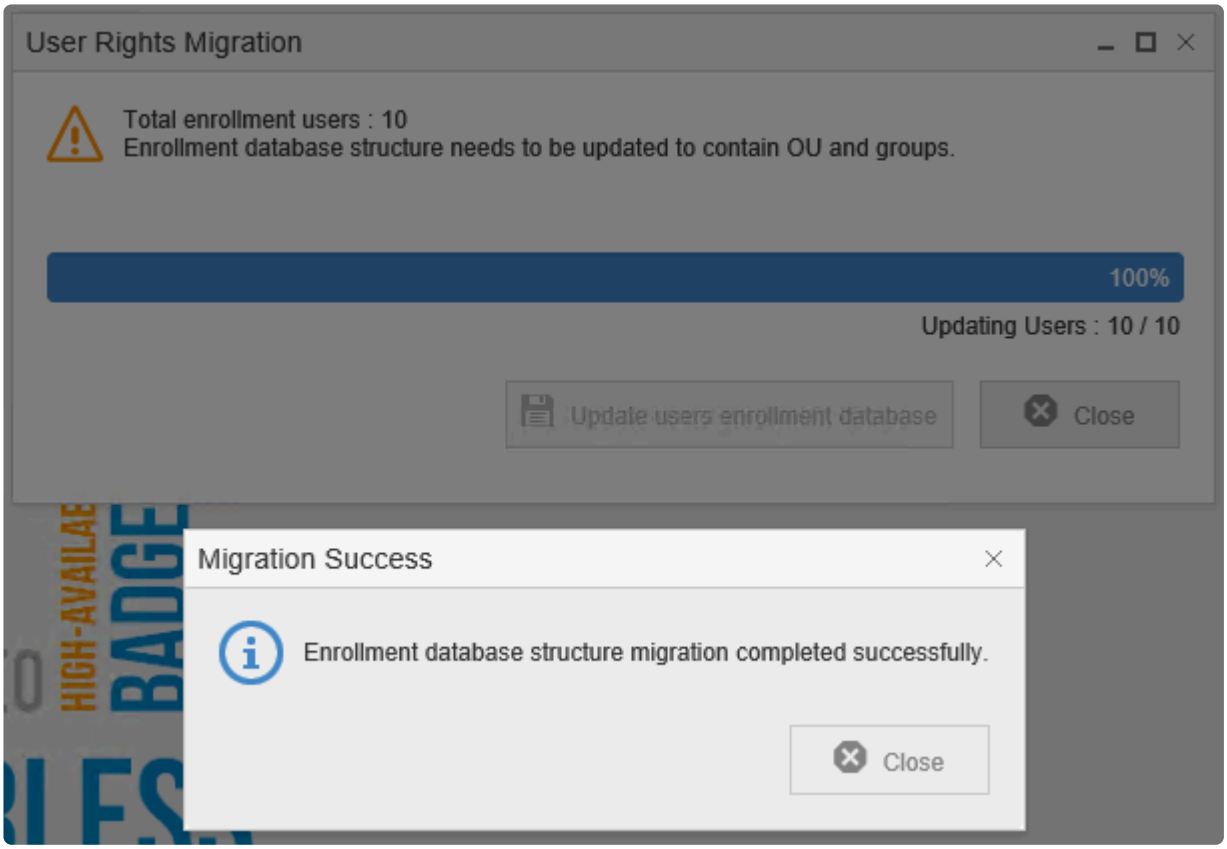


12. Click **OK** to confirm.

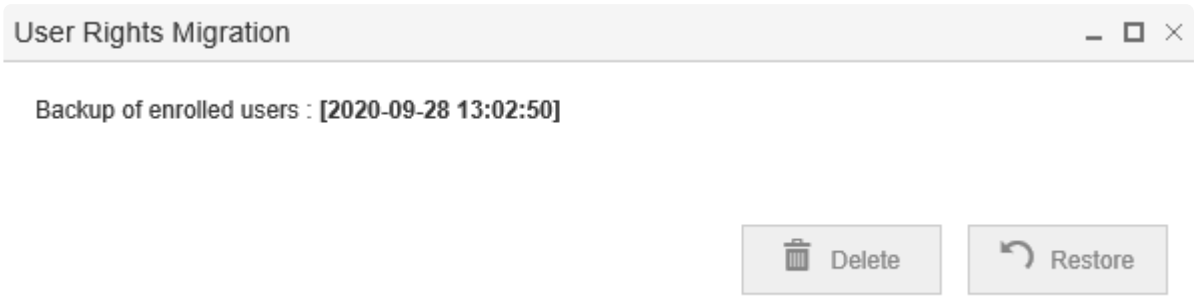


The migration starts.

13. Once the migration is successful, a confirmation message displays.



14. Close the backup popup.



Limitations

- A user cannot have a mix of Celiveo 8.0.x SPP clients and Celiveo 8 CVP client workstations. If a user has multiple Celiveo 8.0.x SPP workstations, all of them need to be upgraded to Celiveo 8 CVP clients in order to use the Celiveo functionalities.
- Once the enrollment table is migrated, the users should not enroll using Celiveo 8.0.x printers.
- If there is any job left with the Celiveo 8.0.x SPP client, the jobs will be migrated to the new Celiveo 8 database upon migration of the SPP client to the Celiveo 8 CVP client. However, the tracking details listed below will not appear on the reports for the expired and deleted migrated jobs.
  For deleted jobs:
  [PrinterFormatterNumber] = NULL
  [Language] = Blank
  [UserGroups] = NULL
  [UserOUs] = NULL
  For Expired jobs:
  [Language] = Blank

[UserGroups] = NULL
[UserOUs] = NULL

- If there is any job left with the SecureJet 7.0.x Serverless Pull Print Client, the jobs will be migrated to the new Celiveo 8 database upon the migration of the SecureJet 7.0.x Serverless Pull Print Client to the Celiveo 8 CVP client. However, the tracking information for the migrated jobs will not be displayed under FQDN and the currency will be based on the client machine's local system account settings.
- Printer details for deleted jobs will not be available in the Celiveo 8 database after migrating the SJ7.0.x server SSS to Celiveo 8 CSS. Printer details will be populated only if that particular printer is available on the Celiveo 8 DB.
- Jobs generated from a SJ7.0.x SPP client will not be retrieved from a Celiveo 8 printer until the SJ7.0.x SPP client is upgraded to Celiveo 8 CVP client.

Last modified: 29 September 2022

17.11.3. SAP Connector Migration

Pre-requisites/Limitations/Known Issues

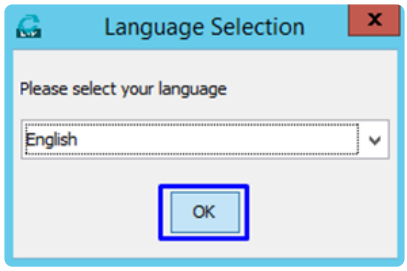
1. CSS Server needs to be up to date to properly support TLS 1.2 for .NET 3.5.
2. Once Celiveo 8 is configured for SAP, SAP jobs cannot be printed using the printers with legacy embedded. Therefore, make sure that there are no jobs left to be printed before the SAP migration.
3. The maximum character limit which can be used for the SAP print queue is 44 characters. This includes the CSVP name + Driver name.
4. Only the following special characters are supported for the print queue: ~ ! @ # % ^ _ ( ) + ` – = { } [ ] ; .
5. If SQL Enrollment is involved, the Enrollment table migration needs to be done at the beginning of the process.
6. MachineName in tracking data for SAP jobs will be the SAP System ID.
7. SAP profiles need to be reconfigured in the SAP utility after each connector installation.
8. The ‘Celiveo Print-ERP Communication Server’ service needs to be restarted after each CSS restart, new CSVP installation, or print queue generation via the CVP context menu.
9. If the ‘Add’ button is disabled upon creating an SAP profile with an empty field in the SAP utility, refresh the browser in order to enable it back.

Steps to follow

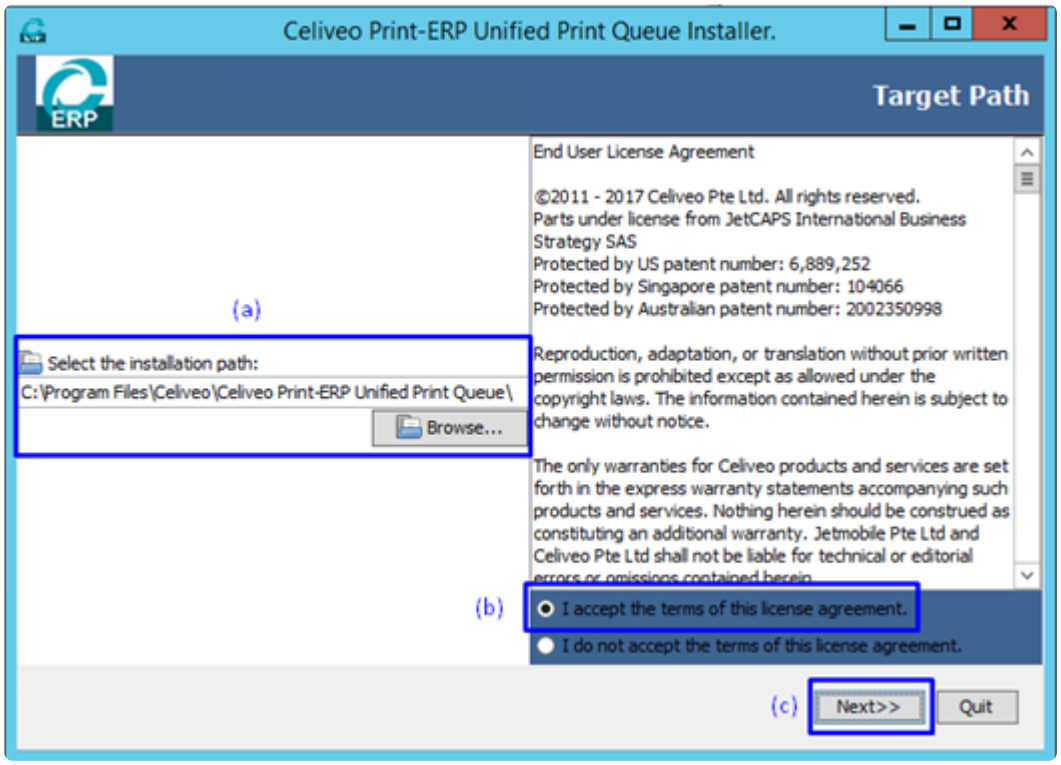
1. Install Celiveo 8 on a new server.
2. Install Celiveo Track GreenSaver on the same server.
3. Create a CSVP from the Celiveo 8 Web Admin and download the CSVP package.
4. Unzip and install the CSVP package on the server which is going to be the CSS server.
5. Install Celiveo Print ERP for SAP Unified Print Queue connector on the above CSS server as indicated here.
6. Configure the **sapconfig-ui** utility as indicated here.
7. Configure the Celiveo BC_XOM Connector (Client Connector) to point to Celiveo 8 server as indicated here.
8. Configure and Download ROMS/Output Devices as indicated here.
9. Upload downloaded ROMS/Output Devices to SAP logon.
10. Sync SAP printers with Celiveo 8 Web Admin using the SAP connector.

Install Celiveo Print ERP for SAP Unified Queue Connector

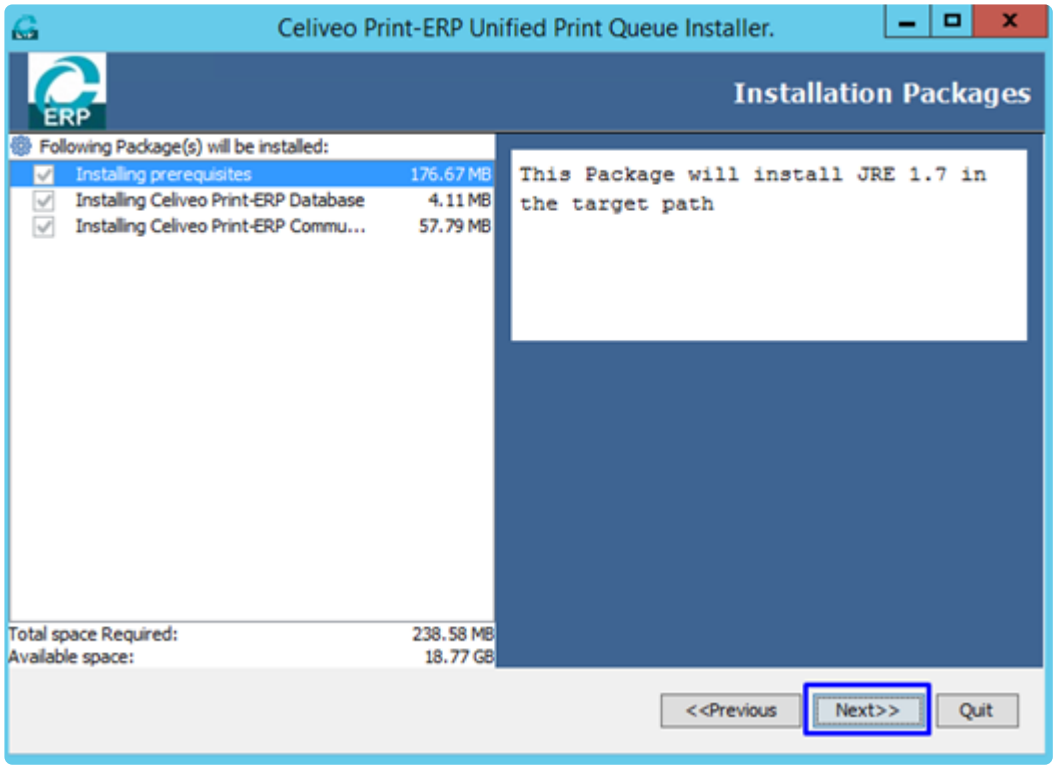
The Celiveo Print-ERP Unified Print Queue Connector needs to be installed on the CSS server. If the environment does not have TLS1.2, follow the steps in section 5.1.
1. Right-click the **Celiveo_Print_ERP_for_SAP_Unified_Print_Queue.exe** installer and select **Run as administrator**.
2. Once the extraction is done, select the language and click **OK** to start the installation wizard.



3. The installation wizard will open with the target path details and license agreement details.
a. Select the path to be installed. The default installation path will be *C:\Program Files\Celiveo\Celiveo Print-ERP Unified Print Queue*.
b. Accept the terms of the license agreement
c. Click **Next** to proceed with the installation wizard.

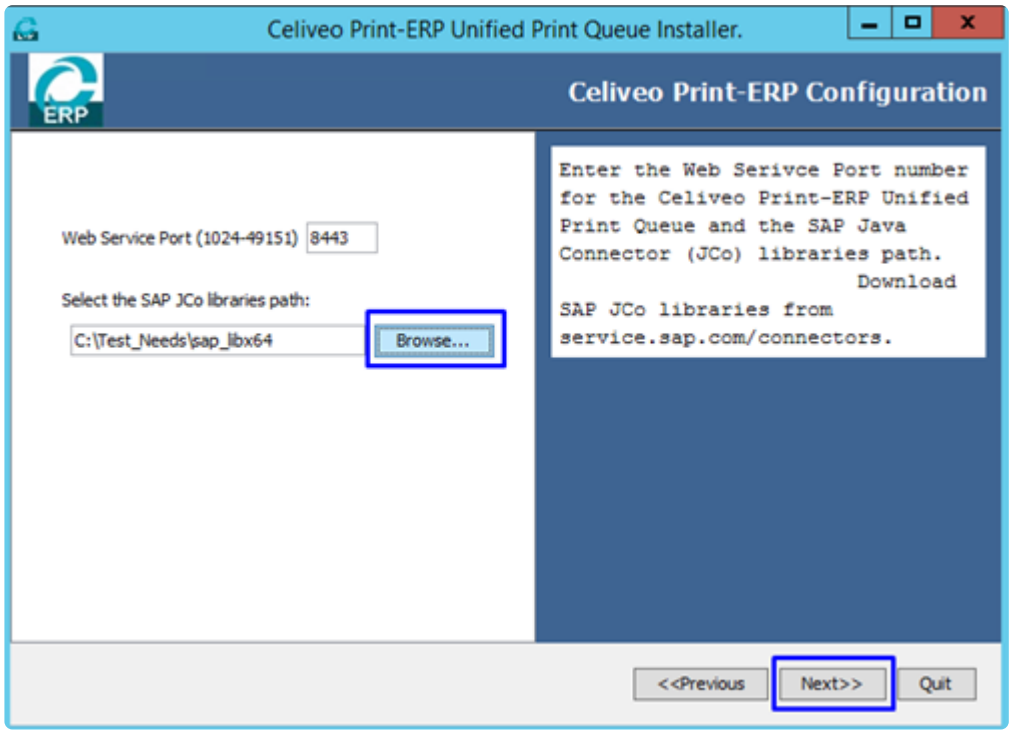


4. Confirm the installation path and click **Next** to proceed.



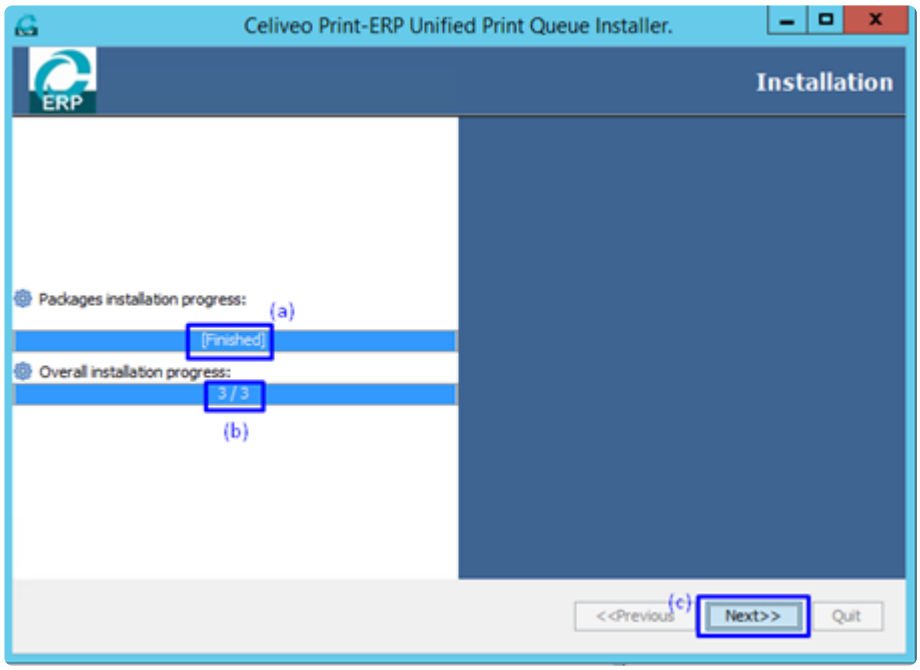
5. Browse the folder which includes Java Connector libraries **librfc32.dll, sapjco.jar, sapjcorfc.dll**. and click **Next** to proceed with the installation.

> Note: Celiveo will not provide SAP Java Connector libraries along with the package. These files need to be downloaded from *service.sap.com/connectors*.

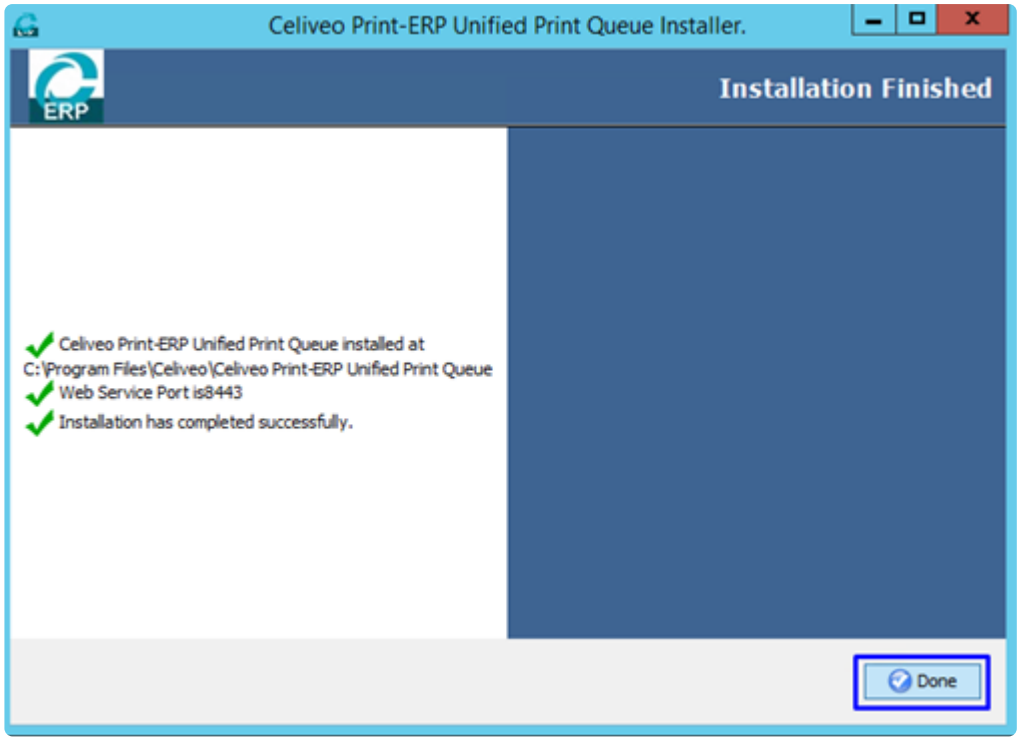


6. Once the installation is completed:
a. The status indicates **Finished**.
b. The overall installation progress is 3/3.

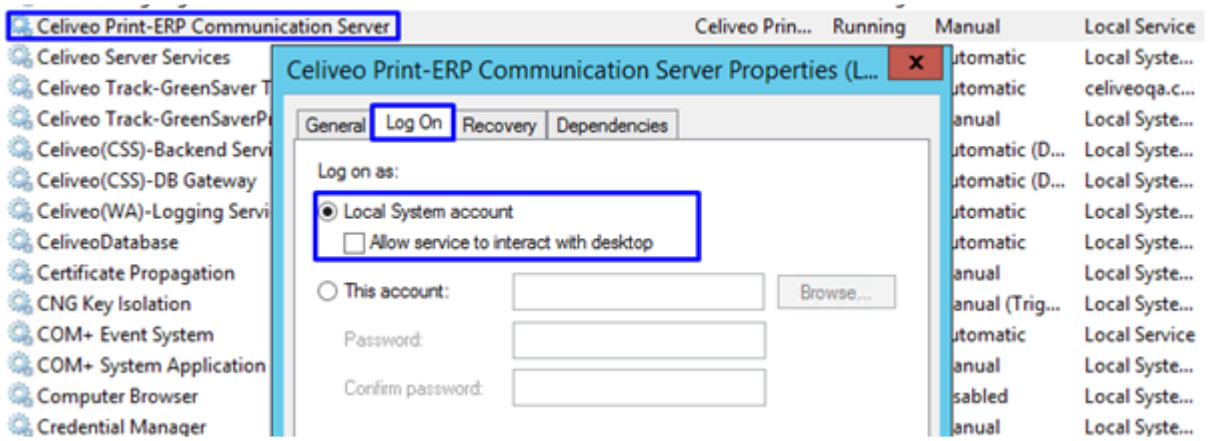
c. Click **Next** to complete the installation.



7. The overall status will have green checkmarks. Click **Done** to close the installation wizard.



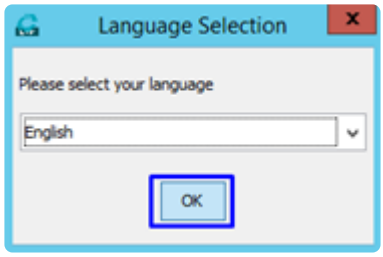
9. Open Windows services and change the **Log On** user for the **Celiveo Print-ERP Communication Server** service to **Local System account** and restart the service.



Install the Celiveo Print ERP for SAP BC-XOM Connector

The Celiveo Print ERP for SAP BC-XOM Connector needs to be installed on the SAP VM.

1. Right-click the **Celiveo_Print_ERP_for_SAP_BC-XOM_Connector_Windows.exe** installer and select **Run as administrator**.
2. Once the extraction is done, select the language and click **OK** to start the installation wizard.

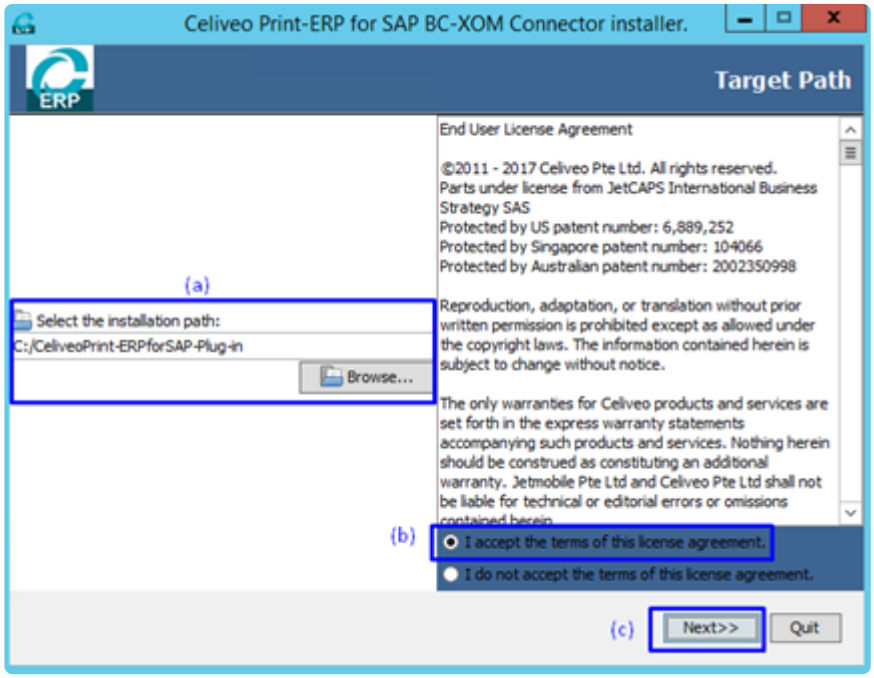


3. The installation wizard will open with the target path details and license agreement details.

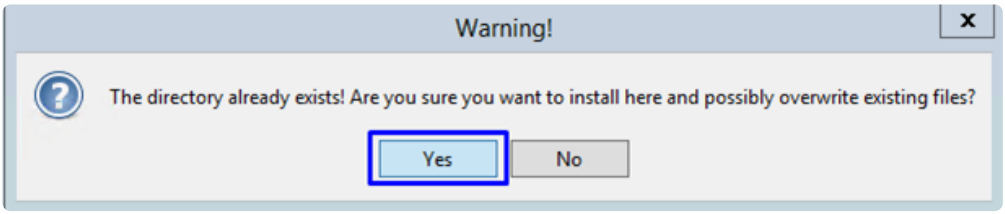
a. Select the path to be installed. The default installation path will be *C:\CeliveoPrint-ERPforSAP-Plug-in*.

b. Accept the terms of the license agreement.

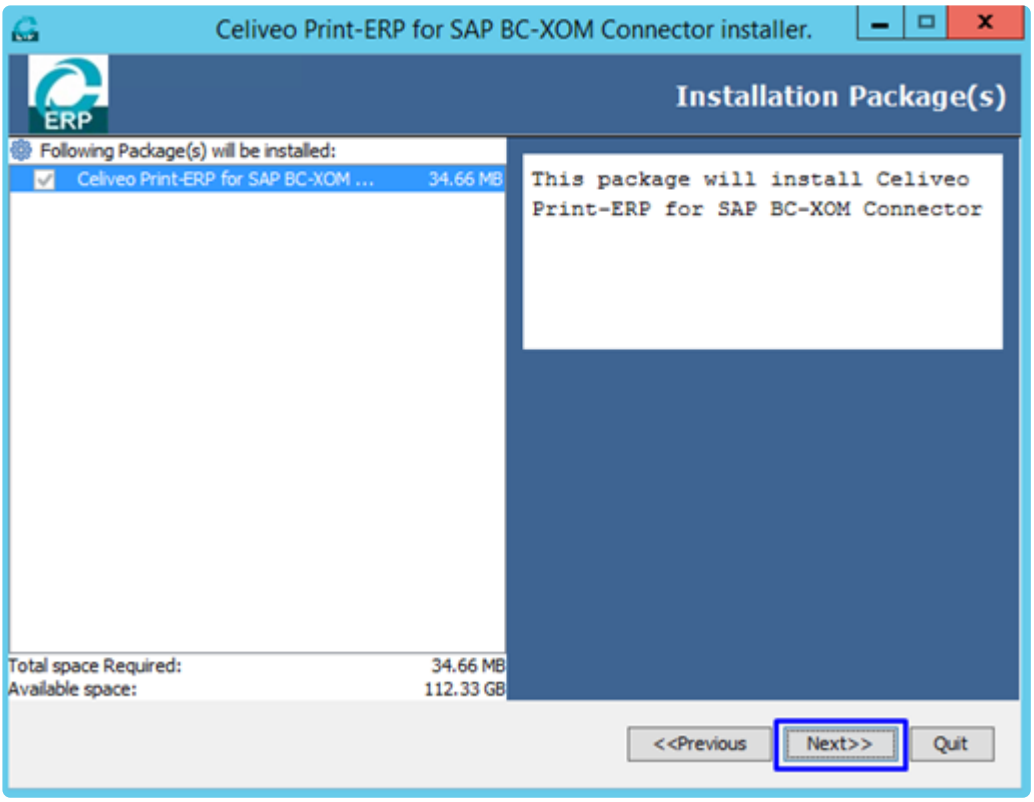
c. Click Next to proceed with the installation wizard.



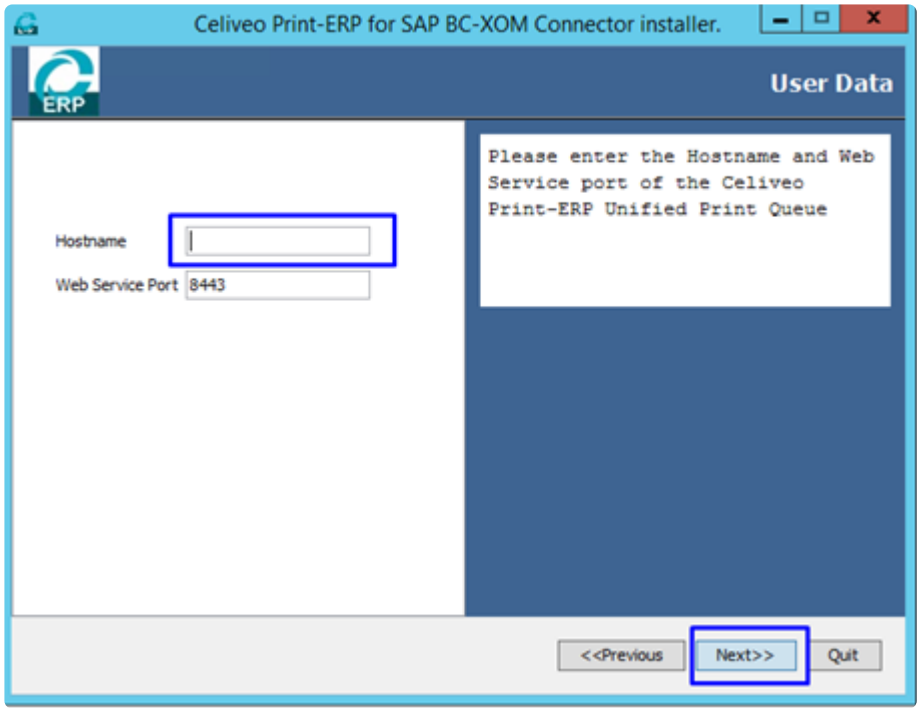
4. If the installation path is the same as in the previous installation, a confirmation message will appear as the root directory is available at the location with the same name. Select **Yes** to confirm the action. This will install the new application under the same path directory.



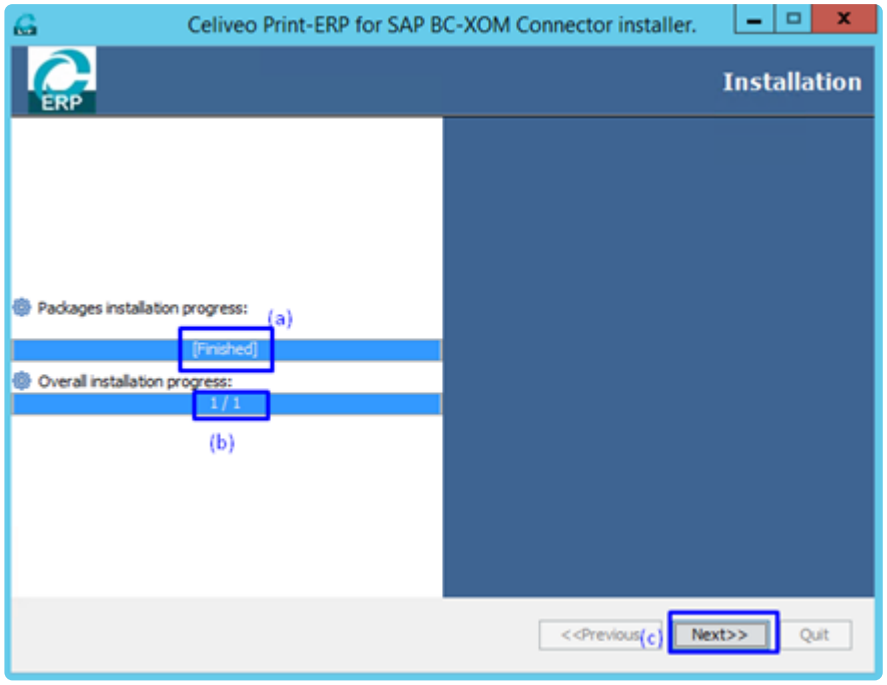
5. Click **Next** to proceed.



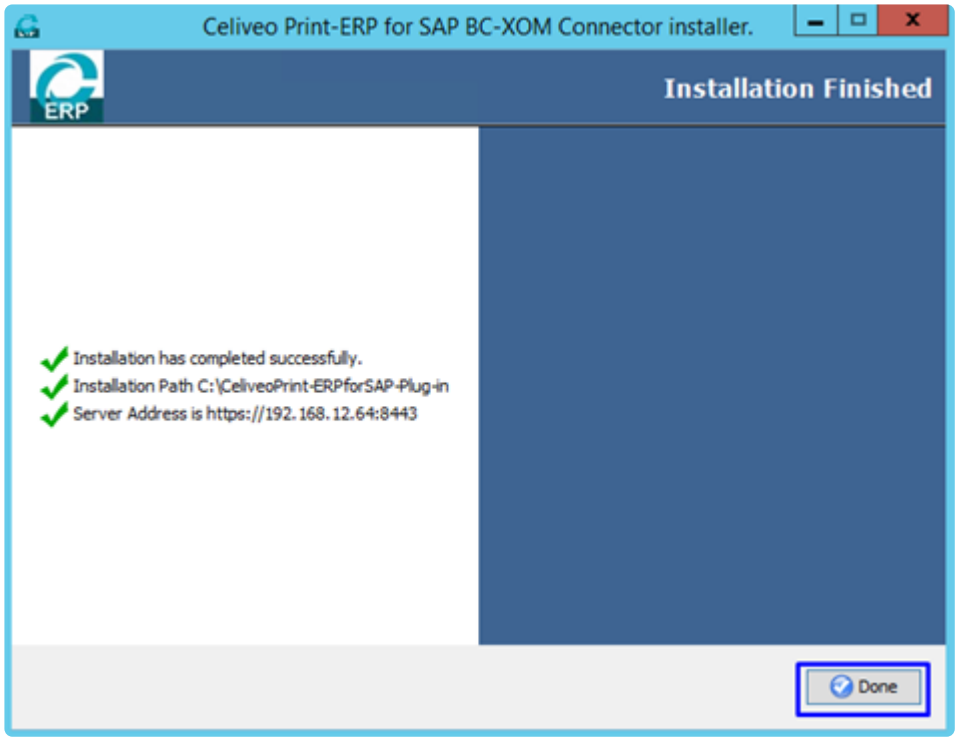
6. Enter the IP Address of the machine where the Celiveo Print-ERP Unified Print Queue is installed and click **Next** to proceed.



7. Once the installation is completed:
a. The status indicates **Finished**.
b. The overall installation progress is 1/1.
c. Click **Next** to complete the installation.

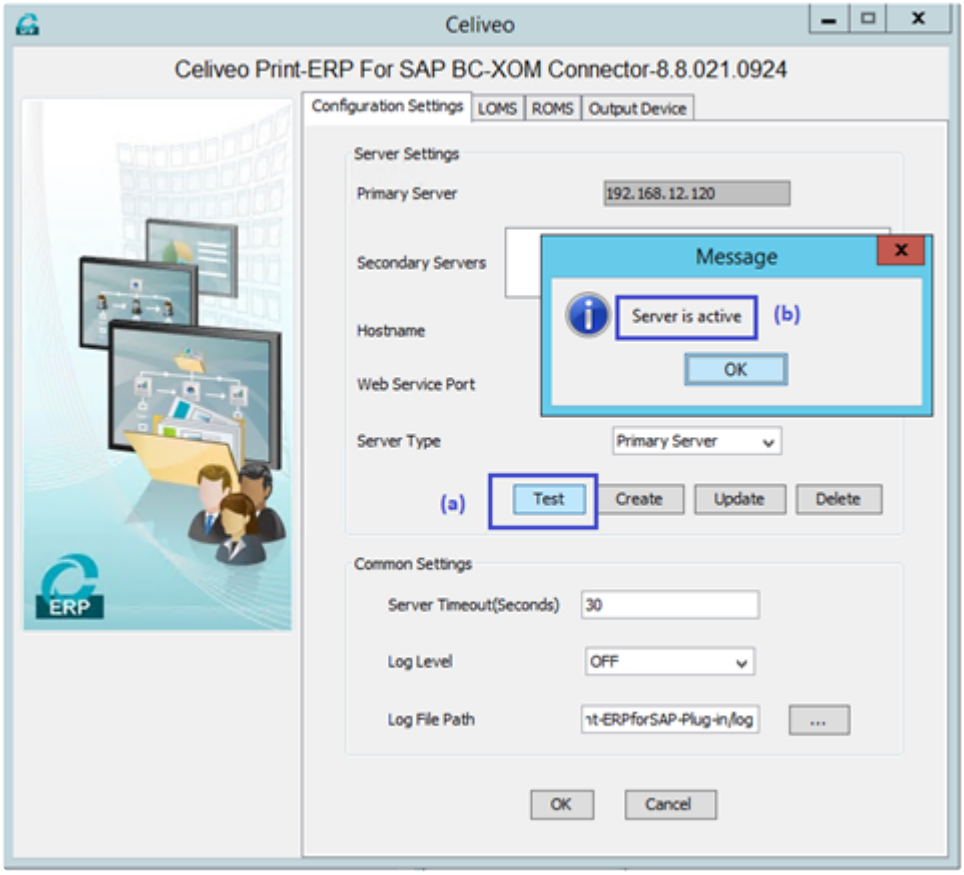


8. The overall status will have green checkmarks. Click **Done** to close the installation wizard.



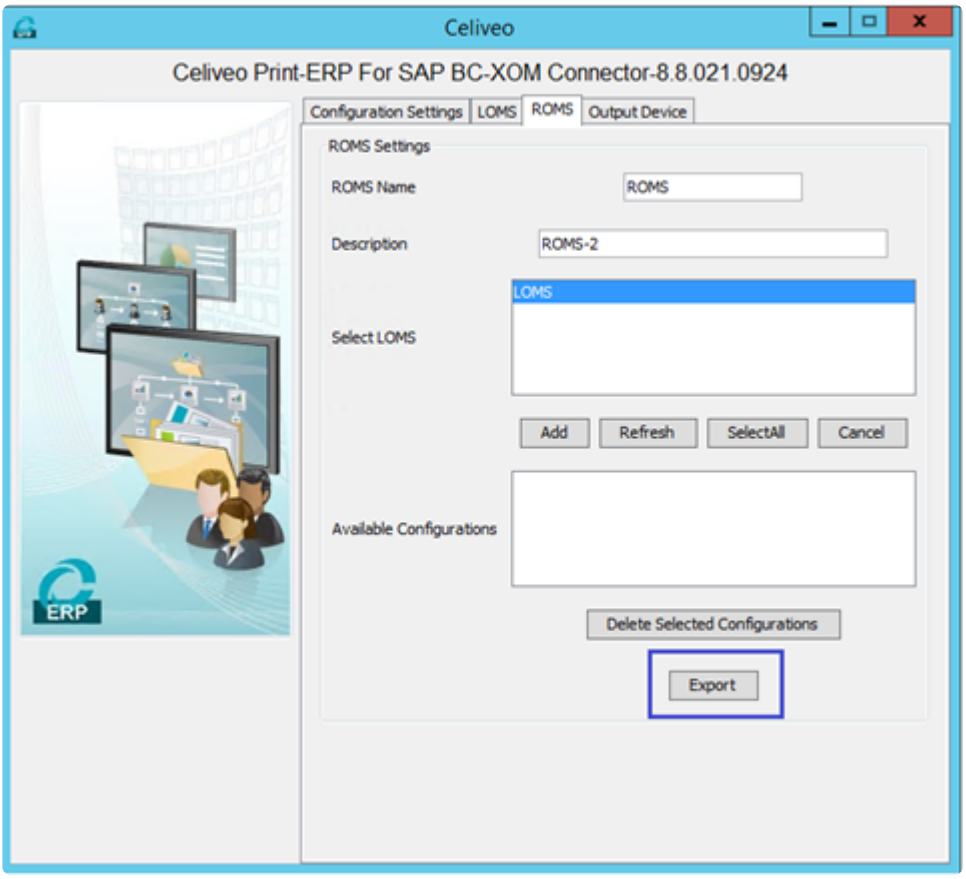
Test the server connection using the Celiveo Print ERP for SAP BC-XOM Connector

1. Navigate to the path given during the Celiveo Print ERP for SAP BC-XOM installation.
2. Open the *CeliveoPrint-ERPforSAP-Plug-in\bin* folder.
3. Double click the **Celiveo Print-ERP BC-XOM for SAP Connector Configuration** tool
4. The primary server is filled with the server IP provided during the installation.
5. Click **Test** to test the server connection.
6. The server status will be **Server is active** if the server connection is successful.



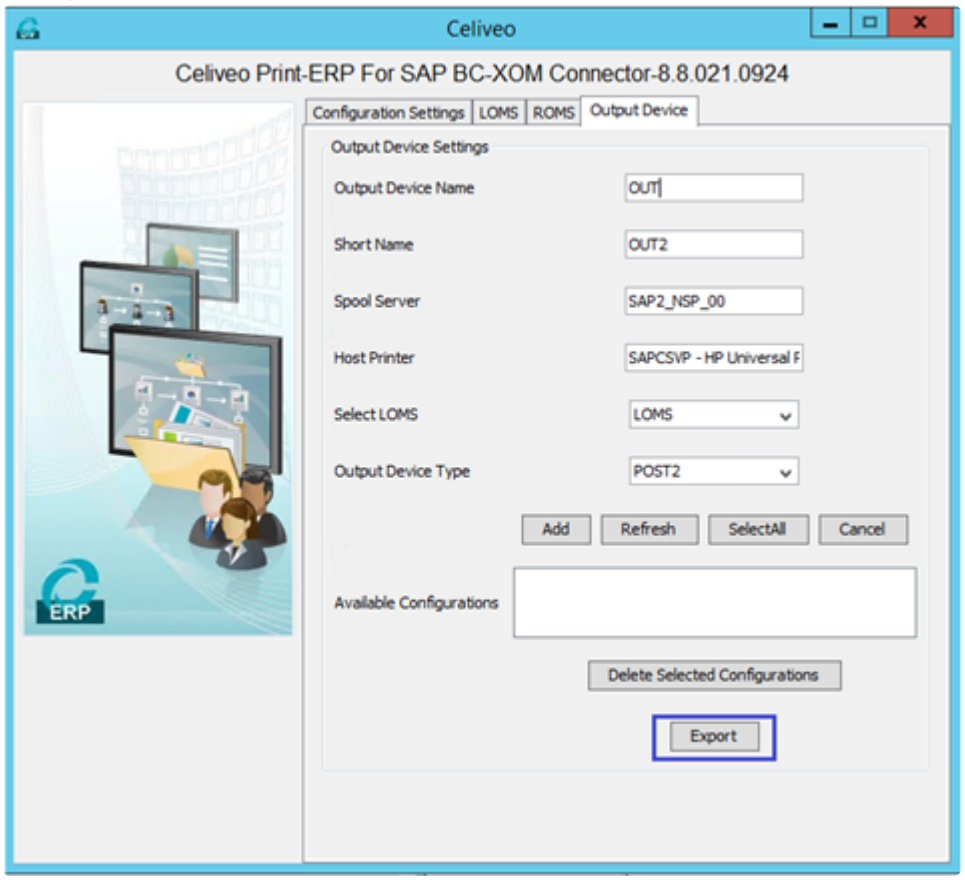
Export ROMS and Output Devices

1. Go to the ROMS tab and click on the **Export** button to download the ROMS configurations.



2. Go to the Output Devices tab and click on the **Export** button to download the Output Device

configurations.



Last modified: 29 September 2022

18. Troubleshooting

Find help about frequently encountered issues.
To access this section, you need to have a Celiveo Freshdesk account.
To create one, please click here.

Last modified: 29 September 2022

18.1. Common Questions

Frequently asked questions regarding the technical aspects of the Celiveo solution.

How to enable the Click button on the ID Code Generation Portal on Internet Explorer
Why are the printing rules configured on the physical printer not applied?
Users are unenrolled shortly after enrollment due to inactivity timeout.
Managing 32 and 64bit printer drivers
Windows could not connect to the Internet to download the necessary files during WA installation on Windows 8, 10, 2012, 2012R2
Discovery Agent wizard returns to blank screen in WA, when you perform cancel action while adding new printer driver for printer.
How to enable Open-API on Konica Minolta MFPs
Print Jobs are not cleared from Shared Print Queue and remains stuck with status ‘Sent to Printer’
How to initiate Celiveo Printing Services on macOS?
Ensure the Windows OS hosting Celiveo Web Admin supports all proper TLS 1.2 cipher protocols
Celiveo Services stop and does not start automatically when Print server is rebooted
Impact of SQL Database password change
Enrollment and authentication with a user account that is a member of more than 1,010 groups may fail on a Windows Server-based device

Last modified: 29 September 2022

18.2. Retrieve Logs

Enable and Download Log Files
Retrieve Web Admin Logs
Enable and retrieve CSA Logs
Retrieve Discovery Agent Log
Retrieve Celiveo Print Queue Client Application Log
Enable macOS CVP Logs

Last modified: 29 September 2022

18.3. Error Messages

Single Function Printers
Multi-Function Printers
Celiveo Product Installation
Serverless Pull Printing

Last modified: 29 September 2022

19. Disaster Recovery Plan

Disaster Recovery Plan

Last modified: 29 September 2022