PRINTERON®
PRINT SIMPLY ANYWHERE

PrinterOn Enterprise

Configuration Guide

Version 4.3.9

mobile printing solutions | enterprise | education | public printing locations

Contents

1

Introduction

This guide explains how to configure and monitor the PrinterOn® Enterprise software.

The PrinterOn solution allows your users to print without installing drivers and without a difficult setup or complicated configuration. Once your PrinterOn software is installed and configured, users can submit print jobs to PrinterOn connected printers in a variety of ways, including:

- using the PrinterOn Web Print portal
- using the PrinterOn Mobile App
- by email
- through Google Cloud Print
- through native Windows print queues, native iOS, or native IPP

PrinterOn also supports Secure Release Anywhere™ pull printing, which lets users print to a pool of printers and then pull their print job to the printer within that pool that is most convenient.

1.1 PrinterOn Server editions

Your PrinterOn Server installation will install one of the foll owing editions of the software:

- **PrinterOn Enterprise**: The Enterprise Edition is a full-featured print solution. This edition supports advanced features such as multi-server deployment, scalability through clustering, and integration with MDM/EDM solutions.
- **PrinterOn Server Express**: The PrinterOn Server Express edition is the starter package. Although it shares all the same basic features as PrinterOn Enterprise, it excludes many of the advanced configuration features of the Enterprise edition that are typically unnecessary for a small- to medium-sized business or organization.

    You can upgrade your Express edition to Enterprise at any time.

1.2 Key concepts of the PrinterOn solution

Before working with the PrinterOn solution, it is useful to understand two key concepts:

- PrinterOn printers
- Secure Release Anywhere pools

1.2.1 PrinterOn printers

A PrinterOn printer is not a physical printer, but rather a virtual printer. That is, it is a *definition* that maps to a physical printer and defines its printing behavior and supported features. The PrinterOn server acts as middleware between the user and a physical printer. When users submit jobs to a PrinterOn printer, the PrinterOn server directs those jobs to the physical printer or print queue defined for that printer, referred to as an output destination. Before users can submit print jobs to a PrinterOn printer, you must point define that printer's output destination.

PrinterOn printers need not map to physical printers on a one-to-one basis. The benefit of creating virtual printers is that you can specify different printing behavior or access privileges for the same physical printer. You simply create multiple PrinterOn printer definitions, apply different configuration settings to each, and then map them to the same physical printer. Although it is the same physical printer printing the jobs in each case, to the user, they appear as distinct printers with different available features.

For example, consider a hotel with a color printer. The hotel could create one printer definition that points to their color printer and allows users to print in colour at a specific price per sheet. They could then create a second printer definition that points to the same physical printer, but restricts print jobs to black and white, and charges a lower rate per sheet. For frequent guests, they could also create a third printer definition for the same printer that does not charge a fee at all.

1.2.2 Secure Release Anywhere pools

Secure Release Anywhere pools are groups of PrinterOn printers. To the user, a printer pool appears as just another printer. However, instead of distributing jobs to a single output destination, a printer pool can distribute print jobs to any of its member printers. Users can go to the output destination of any member printer and pull the print job down using their credentials or a secure release code.

The printers in a Secure Release Anywhere pool are not limited to a single network; you can include printers from disparate networks in a single printer pool. For example, a hotel chain could create a single Secure Release Anywhere pool that contains all the printers from their business centers in all their hotels worldwide. A guest in the Singapore location can print to the printer pool, go to the business center, and pull the job down. The same guest could travel to Seoul the next day, print to the same pool, go to the business center at the Seoul location, and pull the job down there.

1.3 The PrinterOn solution components

The PrinterOn server software consists of several components that work together to enable web-based printing from PCs and laptops with Internet access. The PrinterOn solution is comprised of the following components:

- **PrinterOn Central Print Services (CPS)**: The primary entry point for all requests submitted to the PrinterOn server. In addition to providing access to print services, the CPS also hosts the Web Print portal, and the CPS Administration Console.
- **PrinterOn PrintAnywhere® server (PAS)**: Provides document processing and rendering.
- **PrinterOn Print Delivery Station (PDS)**: Collects print jobs and provides privacy release capability.
- **PrinterOn Print Delivery Gateway (PDG)**: Provides support for printing from a variety of devices and systems including iOS, Google Cloud Print compatible applications or traditional print queues.

- **PrinterOn Print Delivery Hub (PDH)**: In Enterprise installations, distributes print jobs to PDSs installed on disparate networks.
- **PrinterOn Configuration Manager**: Provides a single centralized management console for all software components, servers and options.

For more information on the PrinterOn components, see PrinterOn Server components glossary and overview.

The PrinterOn solution can be configured for several popular system integration models or customized as needed using the available HTML and Java source code. It is easy to deploy and can be hosted in multiple local or remote network scenarios. The PrinterOn software has been designed for optional integration with existing network infrastructures, including LDAP and Print Management Systems.

1.3.1 Architecture overview

Simplified PrinterOn architecture
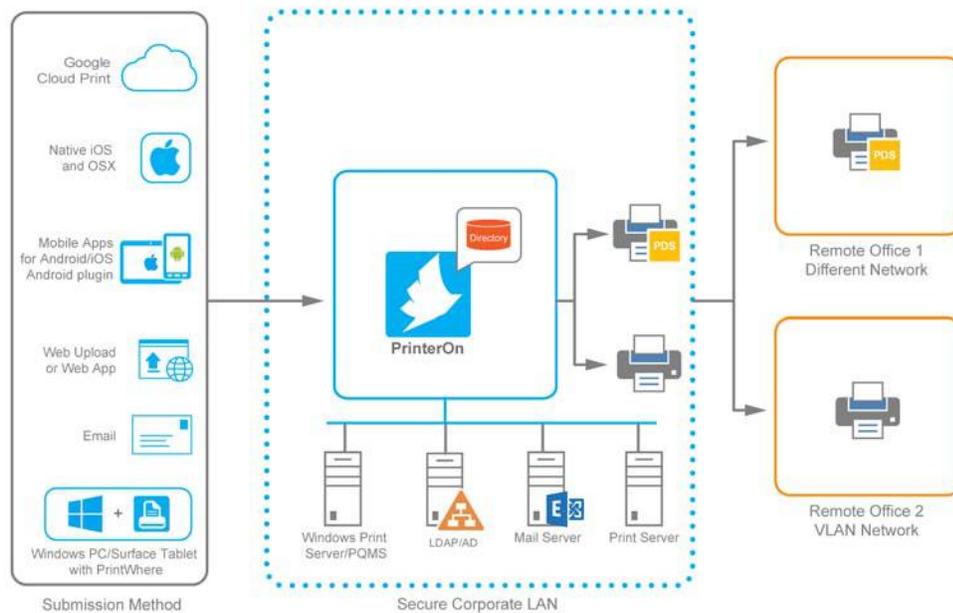
Detailed PrinterOn architecture with communication ports

The following diagram illustrates a distributed PrinterOn Enterprise deployment. In PrinterOn Express, all components must be installed on a single server; multiple networks and the PDH component are not supported.

Communication	PrintWhere: Port 443 Email: Port varies	Web Upload: Port 443 Native iOS: Port 6310	Mobile Apps: Port 443 PDS: Port 443/631	IPP Communication PDH: Port 443/631	Google Cloud Print: Port 443/5222
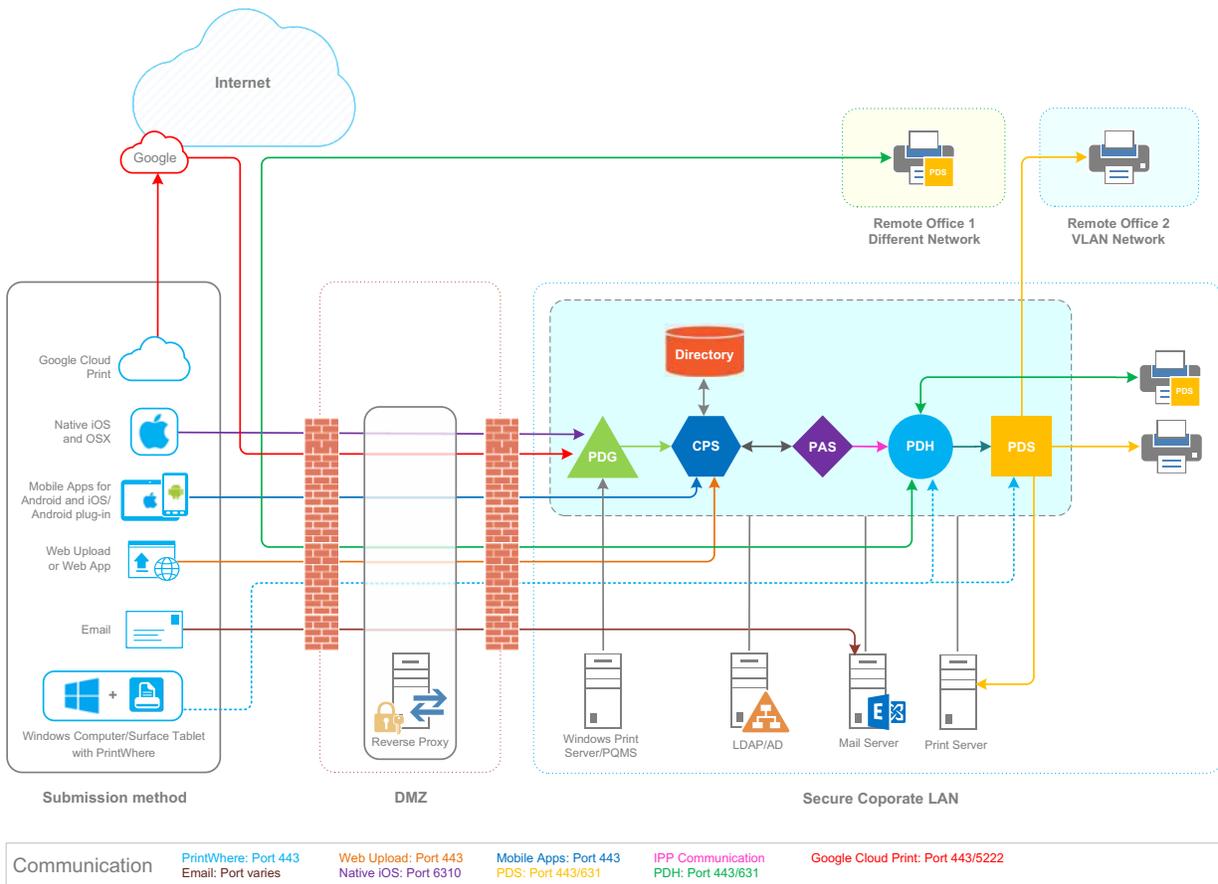
1.4 New in this release

This guide documents PrinterOn Enterprise Edition version 4.3.9. This release follows on previous releases of the product.

This release is focused primarily on bug fixes. In addition, the version of Apache log4j API installed with the software has been upgraded to log4j-comp v.2.17.1. There are no major new features added in this release.

2

Exploring the Configuration Manager

The Configuration Manager allows you to configure all PrinterOn Server settings, administer your printers, and synchronize printer settings.

2.1 Launching the Configuration Manager for the first time

The first time you launch Configuration Manager, you'll need to use the default credentials you received from PrinterOn. The credential information you receive differs depending on whether your PrinterOn service is an on-premise deployment, or a managed cloud deployment:

- Launching Configuration Manager in on-premise deployments.
- Launching Configuration Manager in managed cloud deployments.

2.1.1 Launching Configuration Manager in on-premise deployments

If you are logging in to the Configuration Manager in an on-premise deployment of PrinterOn for the first time, or you have reset the password or restored the Root user, you must log in using the default login credentials.

To open the PrinterOn Configuration Manager:

1. In your browser, navigate to the Configuration Manager URL that you received from PrinterOn. For example:

   https://ponconf-mycorp.printanywhere.com:8057

2. Log in to the Configuration Manager with the following credentials:

Field	Root User Authentication
Username	root

Password:	One of the following:
	
	• For a trial installation, enter **`Trial`**.
	
	• For a licensed installation, enter the APIsiteAuth value found in the [site] section of your PrinterOn license file (PrinterOnConfig.txt). For example:
	
	`[site]`
	`APIsiteUID = 562873393017`
	`APIsiteAuth = SzNQJxV7`
	`AdminEmail = email@printeron.com`

When you log in with your default password, the Configuration Manager immediately prompts you to change your password.

2.1.2 Launching Configuration Manager in managed cloud deployments

To open the PrinterOn Configuration Manager:

1. In your browser, navigate to the Configuration Manager URL that you received from PrinterOn. For example:

    https://ponconf-mycorp.printanywhere.com:8057

Log in to the Configuration Manager with the following credentials:

Field	CPS Authentication
Username	The email address in your PrinterOn license file.

Password:	For a licensed installation, enter the APIsiteAuth value found in the [site] section of your PrinterOn license file (PrinterOnConfig.txt). For example:
	
	`[site]`
	`APIsiteUID = 562873393017`
	`APIsiteAuth = SzNQJxV7`
	`AdminEmail = email@printeron.com`

When you log in with your default password, the Configuration Manager immediately sends an email requesting that you change your password change your password.

Once you've changed your password and have successfully launched the Configuration Manager, you can add new PrinterOn administrators to your service as necessary. For more information, see Managing access to Configuration Manager.

2.2 Navigating the Configuration Manager

After you successfully log in, the Configuration Manager displays the Home > Overview tab.
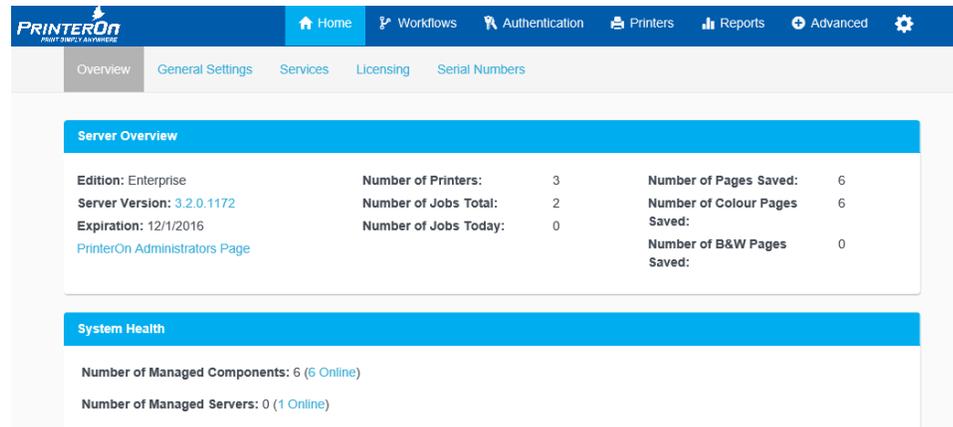
Before working with the Configuration Manager, you should have a general understanding of the Configuration Manager interface, including the following features:

- Basic and Advanced views
- Component-specific UI
- Tabbed interface

2.2.1 Basic and Advanced views

You can display the Configuration Manager in two views:

- **Basic view**: Displays commonly configured settings.
- **Advanced view**: Displays all Basic view settings plus additional advanced settings. Advanced settings are those that are only rarely configured or are specific to a particular deployment.

By default, the Configuration Manager opens in Basic view. You can toggle between the two views using the **Show Advanced Settings** switch on the **Settings** menu (see Showing or hiding advanced settings for detailed steps). As you turn Advanced view on and off, the interface is dynamically updated to show or hide the advanced settings.

> **Note:** For completeness, this guide documents all settings. Screen shots are typically shown in Advanced view. As a result, if you are displaying Configuration Manager in Basic view, images in this guide may appear slightly different than what appears on screen.

For a complete list of settings that are hidden when the Configuration Manager appears in Basic view, see Appendix A: Advanced configuration settings.

2.2.2 Component-specific UI

With version 3.2.2 and later, the Configuration Manager provides a flexible UI that adapts based on which components are present on the server.

The PrinterOn software can be deployed in a variety of ways based on the needs of an organization. For example, an organization may have a remote Print Delivery Service component, it might have a Print Delivery Gateway installed on its own server, or may deploy components in some other distributed scenario in which components are installed on multiple servers.

To simplify the configuration process in these scenarios, the Configuration Manager displays only those settings that are relevant to the installed components. When you open the Configuration Manager, it first checks which components are installed on the server, then excludes those settings that do not apply to the installed components.

As a result, depending on your deployment and the server you are configuring, you may not see all the screens or settings described in this guide.

2.2.3 Tabbed interface

The Configuration Manager workspace contains a number of tabs from which you can configure all aspects of your PrinterOn solution.

> **Note:** As of version 3.2.2, the Configuration Manager only displays configuration settings for those components that are installed on that server. Depending on which components you have installed, you may not see all of the tabs listed below.

Tab/Menu	Features
🏠 **Home**	Provides access to general information about your system health. You can also manage your PrinterOn license and add PDS, PDH, and Print Anywhere components to your PrinterOn deployment. For more information, see The Home tab.
⚐ **Workflows**	Lets you configure settings for the various printing workflows that users can use to print documents to your PrinterOn printers, such as Web Print or Mobile Print. For more information, see The Workflow tab.
🔑 **Authentication**	Lets you configure settings for your selected authentication method. For more information, see The Authentication tab.
🖨 **Printers**	Lets you add and configure your printers, Secure Release Anywhere printer pools, and Print Delivery Software. For more information, see The Printers tab.
👤 **Users**	Lets you define and assign roles to users or groups of users to control access to PrinterOn-managed resources. Used in conjunction with the **Internal Users**, **Azure AD**, and **Third-Party Identity Management Service** authentication methods. For more information, see The Users tab.
📊 **Reports**	Lets you generate reports on your overall PrinterOn deployment. For more information, see The Reports tab.
⊕ **Advanced**	Provides access to advanced configuration features, such as clustering and server stuff. For more information, see The Advanced menu.
⚙ **(Settings menu)**	Provides access to general administration tasks. For more information, see Accessing PrinterOn Server component configurations.

2.2.3.1 The Home tab

The Home tab provides access to general information about your system health. From the Home sub-tabs, you can also manage your PrinterOn license and add PDS, and PDH, and Print Anywhere components to your PrinterOn deployment.

The Home tab contains the following sub-tabs:

Tab	Features
Overview	Provides system information and an overview of system health.
General Settings	Lets you configure cross-component settings.
Services	Lets you view and change the status of the PrinterOn services.
Licensing	Lets you view and manage your license information.
Serial Numbers	Lets you view serial number information for server components and add additional PDS and PDH instances or PrintAnywhere Servers to your PrinterOn service.

2.2.3.2 The Workflow tab

The Workflow tab lets you configure settings for the various printing workflows that users can use to print documents to your PrinterOn printers, such as Web Print or Mobile Print.
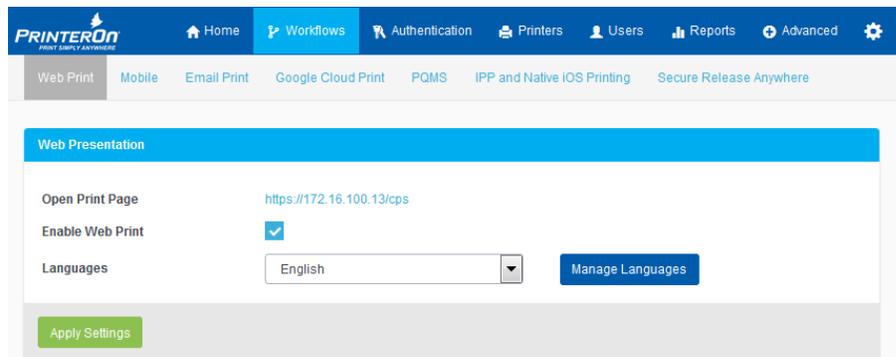
The Workflow tab contains the following sub-tabs:

Tab	Features
Web Print	Lets you configure settings for Web Print, which allows users to upload documents to the Web Print portal.
	For more information, see Configuring the Web Print workflow.
Mobile	Lets you configure settings to allow users to submit jobs using one of PrinterOn's mobile client apps.
	For more information, see Configuring the Mobile Print workflow.
Email Print	Lets you configure settings to allow users to email documents as printable attachments directly to a PrinterOn printer.
	For more information, see Configuring the Email Print workflow.

Tab	Features
Google Cloud Print	Lets you configure settings to allow users to submit print jobs via the Google Cloud. For more information, see Configuring the Google Cloud Print workflow.
PQMS	Lets you configure settings to allow users to print to Windows print queues that are mapped to PrinterOn printers. For more information, see Configuring the PrinterOn Queue Management System (PQMS) workflow.
IPP and Native iOS/macOS	Lets you configure settings to allow users to print using either IPP printers that are mapped to PrinterOn printers, or using iOS/macOS native printing. For more information, see Configuring IPP and native iOS/macOS workflows.
Secure Release Anywhere	Lets you configure behavior to support pull printing, which allows users to print to a pool of printers and pull the job down to whichever printer they want. For more information, see Configuring the Secure Release Anywhere workflow.

2.2.3.3 The Authentication tab

The Authentication tab lets you specify the authentication method you want to use with your PrinterOn solution, and to configure user lookup integration.
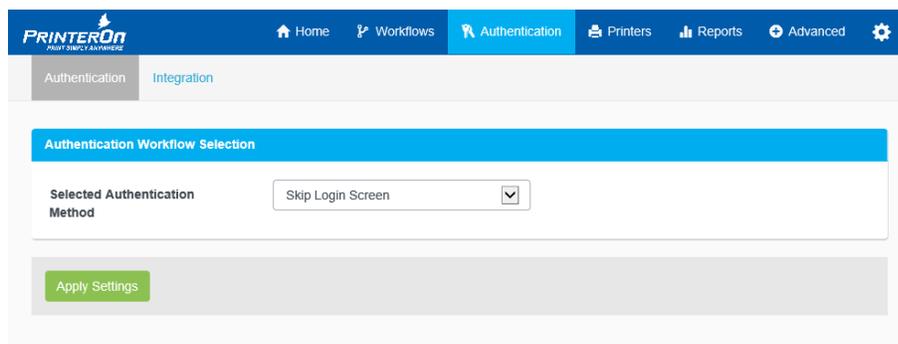
The Authentication tab contains the following sub-tabs:

Tab	Features
Authentication	Lets you specify and configure the authentication method.
	For more information, see Configuring authentication settings.
Integration	Lets you configure how the PrinterOn service identifies users, and how identified and unidentified users are permitted to interact with the service.
	For more information, see Integrating user lookup extensions.

2.2.3.4 The Printers tab

The Printers tab lets you define your PrinterOn printer definitions, monitor print jobs, create printer pools for pull printing, and configure the Print Delivery software.

The Printers tab contains the following sub-tabs:

Tab	Features
Printers	Lets you create and configure PrinterOn virtual printers and connect them to a physical printer or print queue.
	For more information, see Managing and configuring PrinterOn printers.

Tab	Features
Secure Release Anywhere Pools	Lets you assign your PrinterOn printers to printer pools. When printing, users choose a pool, and can pull their print job down to any of the printers in the pool. For more information, see Creating and configuring Secure Release Anywhere pools. **Note:** This tab is only available if you have Secure Remote Release enabled for your PrinterOn service.
Queue Monitor	Lets you monitor the status of print jobs sent to all your PrinterOn printers.
Servers	Lets you configure the Print Delivery Station and embedded agent software. For more information, see Managing and configuring Print Delivery Stations (PDS).

2.2.3.5 The Users tab

The Users tab lets you define users, groups, and access control rules to grant access to the PrinterOn printers, printer departments, and Print Delivery Stations.

The Users tab is accessible when you use one of the following Authentication methods:

- Internal Users
- Azure AD
- Third-Party Identity Management Service

The Users tab contains the following sub-tabs:

Tab	Features
Users	Lets you add and manage PrinterOn user accounts. A PrinterOn user represents an individual who administers or uses the PrinterOn service. A user can be added to one or more group or assigned to one or more access control rules. For more information, see Creating and managing user accounts.
Groups	Lets you add and manage user groups. A user group is a collection of users. You can group users in any logical way; for example, by department, by geographic location, or some other criteria. You can assign a group to one or more access control rules. For more information, see Creating and managing PrinterOn groups.
Access Control Rules	Lets you add and manage access control rules. An access control defines a set of privileges granted to a user or group for a specific printer, printer department, or Print Delivery Station. For more information, see Creating and managing PrinterOn Access Control Rules.

2.2.3.6 The Reports tab

The Reports tab lets you generate reports on your PrinterOn deployment.

The Reports tab contains the following sub-tabs:

Tab	Features
Summary	Provides a three-month summary of print behavior.
Printer Activity	Lets you generate a report for a selected printer.
Advanced	Lets you generate reports on key printing metrics of all your PrinterOn printers.

2.2.3.7 The Advanced menu

The Advanced menu lets you configure settings for the servers, components, and clusters in your PrinterOn deployment. The Advanced menu contains the following menu items:

Menu item	Features
Servers	Lets you configure server settings.
Components	Lets you configure component-specific settings for each of the PrinterOn server components—such as PDS, PDH, PrintAnywhere—installed on this server, or on any child server. For more information, see Accessing PrinterOn Server component configurations.
Clustering	Lets you configure clustering for PrintAnywhere Processing and Status Servers. For more information, see Advanced clustering and document processing scalability.

2.3 Accessing PrinterOn Server component configurations

In addition to the configuration settings that are applied to your PrinterOn service, you can also modify additional component-specific settings in the Configuration Manager. You can access these component specific configurations from the Advanced menu, or via the Home screen.

To access a component configuration for a component installed on the local server:

1. In the Configuration Manager, do one of the following:

    • Click **Advanced** > **Components**.

      or

    • Click **Home**, then in the **System Health** panel, click on the **Number of Managed Components** link.

The Managed Components page appears.

2. Click on the **Configure** button adjacent to the component you want to configure. The component configuration for the selected component appears.

2.4 Configuration Manager best practices

2.4.1 Specifying network addresses

Throughout the Configuration Manager interface, there are a number of locations where you must provide URLs/network addresses to facilitate communication between PrinterOn components, or between the PrinterOn server and external services, such as authentication services.

With PrinterOn Enterprise v4.2.3, key PrinterOn server components have been updated to support the IPv6 communication standard. However, some fields within the Configuration Manager may not have been configured to accept addresses in IPv6 notation (for example, [2001:470:b0df:b0df::1778]).

As a result, PrinterOn recommends that you enter network addresses as fully qualified hostnames. For example:

> myhost.mydomain.com

These fully qualified hostnames can be entered in any field that requires a network address. PrinterOn will automatically resolve the address to the IPv4 or IPv6 value as necessary.

2.5 Managing access to Configuration Manager

When your PrinterOn service is initially configured by PrinterOn support, a single default administrator account is created based on the email address included in your PrinterOn license. You'll use this account to access Configuration Manager for the first time.

To ensure your PrinterOn service remains secure, PrinterOn recommends that once you log into Configuration Manager with this default account, you immediately create additional administrator accounts for those users who will be administering the service, then disable the default account.

> **Note:** To use multiple administrator accounts for Configuration Manager, you must first ensure that you have CPS Authentication mode enabled. For more information, see Modifying the Configuration Manager Authentication mode.

2.5.1 Creating Configuration Manager administrator accounts

As of PrinterOn version 4.2.4, PrinterOn supports two PrinterOn roles to which you can assign all users in your system:

- **User**: The user role should be assigned to all users who will be using PrinterOn's printing services.
- **Administrator**: The Administrator role should be assigned only to those users who will be administering the PrinterOn service. PrinterOn users who are assigned the Administrator role can use their credentials to log into Configuration Manager to modify settings or assign the Administrator role to other users.

Administration privileges are granted through Access Control Rules that you apply a specific user or group of users. The easiest way to manage multiple administrators is to create a group, then apply an Access control rule to that group. You can then add or remove users from that group to grant or revoke Administrator privileges.

If you are using the PrinterOn Internal Users authentication method, you'll need to create PrinterOn accounts for each user who will be accessing the PrinterOn service.

> **Note:** If you are using Azure AD or another third-party IDM service, user account information is provisioned to the PrinterOn user store when a user authenticates to use the service for the first time. Therefore, in order to add a users to the Administrator group, they must first authenticate with the service.

2.5.1.1 Creating an Administrator group

To create PrinterOn Administrators:

1. In your browser, navigate to the Configuration Manager URL that you received from PrinterOn.
2. Log in to the Configuration Manager using the default administrator account credentials you received from PrinterOn.

   > **Note:** The first time you log in, you'll be prompted to change your password before you can continue. Once your password is changed, you can continue as necessary.

3. In the Configuration Manager, click **Users > Groups**. The User Groups tab appears.

4. In the Group Management panel, click **Create Group**. The Create Group dialog appears.

5. Name the group Admin Group, and provide a **Description**, if necessary.
6. Click **Save**.

Next, you can create an Access Control Rule and apply it to the group.

2.5.1.2 Creating an Access Control Rule for the Administrator group

To create an Access Control Rule and add it to the group:

1. In the Configuration Manager, click **Users** > **Access Control Rules**. The Access Control Rules tab appears.

2. Click **Add Rule**. The Add Rule dialog appears.

3. In the Add Rule dialog, name the rule Admin Access.
4. In the **Assign this Role** field, choose the Administrator role.
5. In the **To this User/User Group** field, choose the Admin Group you just created.
6. Click **Save**.

With the Rule is applied to the Admin Group you created, any user added to that group is granted Administrator privileges. You can add users to this group at any time. For information about adding users to a group, see Managing the list of users in a user group.

2.6 Administering the Configuration Manager

The Settings menu, identified by the gear icon ( ), lets you perform some general administration tasks:

- Showing or hiding advanced settings
- Changing your Configuration Manager password
- Resetting the Configuration Manager Password
- Connecting remote servers to a parent Configuration Manager
- Modifying the Configuration Manager Authentication mode
- Logging out

2.6.1 Showing or hiding advanced settings

To show or hide advanced settings:

1. In the Configuration Manager, click the **Settings** button ( ).

2. Click **Show Advanced Settings** to toggle advanced settings on or off.
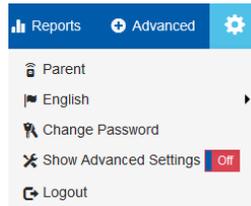
2.6.2 Changing your Configuration Manager password

You can change your password at any time from the Configuration Manager Settings menu.

To change your Configuration Manager password:

1. In the Configuration Manager, click the **Settings** button ( ).

2. Click **Change Password**. The Change Password dialog appears.

3. Enter your old password, then enter and confirm your new password and click **Login**.

Exploring the Configuration Manager

Your new password must meet the following criteria:

- It must not contain your Username.
- It must not have 4 or more consecutive letters or digits.
- It must be at least 8 characters in length, with at least 1 letter, 1 number, and 1 special character. Passwords of 10 or more characters must have at least 2 letters, 2 numbers and/or 2 special characters.

2.6.3 Resetting the Configuration Manager Password

In some cases, it might be necessary to reset your Configuration Manager administrator password. The steps to reset your password differ depending on whether your PrinterOn service is deployed on-premise, or is a managed cloud service.

- Reset your password for an on-premise deployment.
- Reset your password for a managed cloud deployment.

2.6.3.1 Resetting your password for an on-premise deployment

To reset your password in an on-premise deployment of PrinterOn, you need to provide your APIsiteAuth value. This value is the same value you used when you launched Configuration Manager for the first time. You can find the APIsiteAuth in your PrinterOn license file (PrinterOnConfig.txt).

To reset your password:

1. Launch the Configuration Manager.
2. In the PrinterOn Login dialog, click **Forgot Password?**

PrinterOn Enterprise v4.3.9 Configuration Guide | 37

The Reset Password dialog appears.
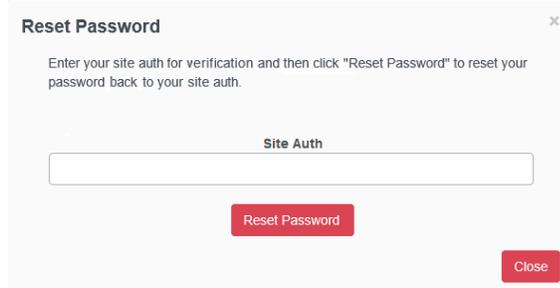
3. Enter your Site Auth value, then click **Reset Password**.

Your password is now reset to the default. When you login, you'll be prompted to change your password immediately.

2.6.3.2 Resetting your password for a managed cloud deployment

To reset your password in a managed cloud deployment of PrinterOn, you need to provide your email address. The PrinterOn server will send an email to that address with a link to the reset password page where you can set a new password for your account.

To reset your password:
1. Launch the Configuration Manager.
2. In the Login dialog, click **Forgot Password?** The Reset Password dialog appears.
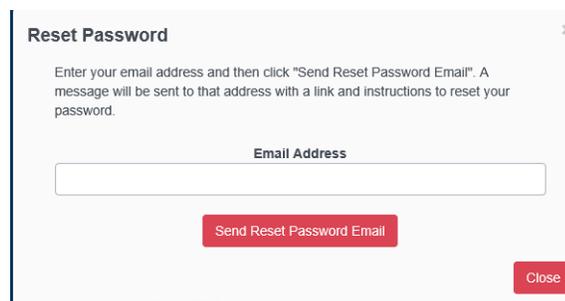
3. Enter your email address, then click **Send Reset Password Email**.

You should receive the following email in your inbox.
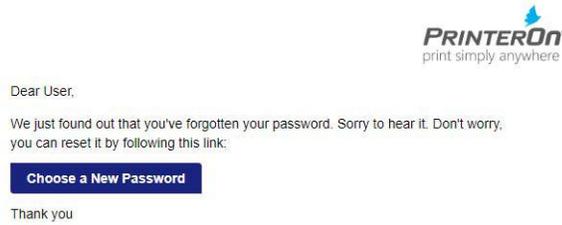
4. In the email, click **Choose a New Password**. You'll be redirected to the

5. On the Password Reset page, enter and confirm your new password, then click Change Password.

6. If there are no issues, you will receive a confirmation email indicating that the password was successfully reset.
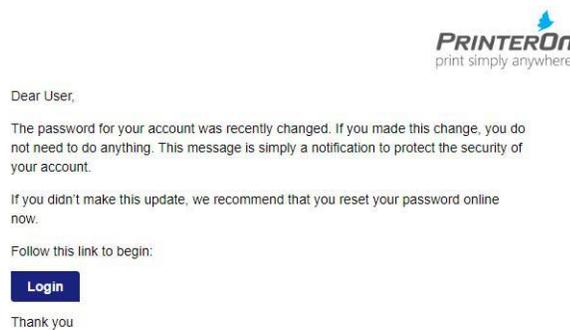
2.6.4 Connecting remote servers to a parent Configuration Manager

The PrinterOn Configuration Manager allows you to manage multiple servers from a single location. To complete this process, you must log into the Configuration Manager on the remote server and select a parent configuration server.

Note: You can still configure individual servers locally on each remote server, regardless of the parent configuration.

To connect to a parent server:

1. On the remote server, log into the Configuration Manager and click
    Settings (⚙) > **Settings**.

    The Settings page appears.

2. In the **Parent URI** field, enter the IP address and port of your central PrinterOn Server machine. The default port is 8057.
3. Press **Connect**.

You can now log into Configuration Manager on your parent server to manage and configure the PrinterOn components installed on the remote server.

2.6.4.1 Resetting the list of remote servers in Configuration Manager

The Configuration Manager maintains a database of all the remote servers that are connected to it; as new remote servers are attached as children to the parent PrinterOn server, the Configuration Manager updates the database with the new remote server information.

However, should you stop using a remote server, the Configuration Manager is unable to determine that the relationship is severed, so the database is not updated to reflect the change. Over time, the Configuration Manager may continue to maintain relationships unnecessarily.

PrinterOn provides a utility that you can run to clear the database and force remote servers to reregister. Running this utility ensures that the database is up-to-date, with all discontinued remote servers removed.

To reset all child servers:

1. On the command line, enter the following command:

    ```
    cd "C:\Program Files (x86)\PrinterOn Corporation\PrinterOn Server
    Install Manager\Tools\Encrpytor" "%PON_JAVA_HOME%\bin\java.exe" -jar
    ponconf-clear.jar
    ```

    Once the database is cleared, all remote servers will reregister, enabling Configuration Manager to maintain an accurate database.

2.6.5 Modifying the Configuration Manager Authentication mode

The Configuration Manager supports two authentication modes that PrinterOn administrators can use to access the Configuration Manager and manage the PrinterOn service. By default, your PrinterOn service will be configured to use only one authentication mode, but you can modify your authentication settings to use either or both authentication modes.

You can configure Configuration Manager to use the following authentication modes:

*   **Root User authentication**: Root user authentication provides a single root user as the administrator. If only Root User authentication is enabled, then if you have multiple PrinterOn administrators, all administrators use the same credentials to log in.

    If you have installed an on-premise version of PrinterOn Enterprise, this mode is the default authentication mode.

- **CPS Authentication**: CPS authentication allows each PrinterOn administrator to log in using their own unique credentials, based on the authentication method you have configured PrinterOn to use:

  - If the authentication method is set to **Internal**, an internal PrinterOn account that has been added to the Users tab and assigned the Administrator role is used.

  - If the authentication method is set to **LDAP/AD**, an account associated with an LDAP/AD server is used.

  - If the authentication method is set to **Azure AD** or **Third-Part Identity Management Service**, an account associated with Azure or another specified IDM is used.

  If you have subscribed to PrinterOn Enterprise Managed Service, this mode is the default authentication mode. At the time that your service is provisioned, a single internal user account is created and assigned the Administrator Role. The password for this account is emailed to the email address associated with the PrinterOn license.

You can enable one of both of these authentication modes, however, because CPS authentication allows for multiple administrator user accounts, it is considered to be the more secure option.

To use change the Configuration Manager authentication mode:

1. Log into the Configuration Manager.

2. Click **Settings** (⚙) and ensure that **Show Advanced Settings** are turned on.

3. Click **Settings** (⚙) > **Settings**. The Settings page appears.

4. In the Authentication Settings panel, enable or disable each authentication mode as appropriate.

5. Click **Apply Settings**.

6. If you have checked **Enable CPS Authentication** and intend to use one of **LDAP/ AD**, **Azure AD**, or a **Third-Party Identity Management Service** as your authentication method, you'll need make the following change on the Authentication tab:

   a) Click the Authentication tab.

   b) Choose your **Selected Authentication Method** from the drop-down. The authentication settings for the chosen method appear.

   c) if you are using Azure AD or Third-Party Identity Management Service, proceed to step d.

   If you are using LDAP/AD, in the **LPAD/AD Settings** panel, from the **LDAP/AD Server Profile** drop-down, choose which LDAP Server you want to configure, then click Edit, or create a new LDAP/AD Server profile. The LDAP/AD Profile Details page appears

   d) Locate the **Enable Configuration Manager Access** and ensure it is enabled.

2.6.5.1 Logging in with Single Sign-On

Once you have configured PrinterOn to use Azure AD or a Third-Party IDM to perform authentication on its behalf, PrinterOn administrators who have successfully authenticated for another service using the same IDM will be able to launch Configuration Manager directly, bypassing the Login dialog.

For users who have not already authenticated, the Login dialog provides a link the redirects the user to the Login page for the configured IDM. After logging in, the IDM will return the user to the Configuration Manager.
.

2.6.5.2 Restoring Root access to the Configuration Manager

If you disable the Root user and rely exclusively on LDAP/AD for authentication, should you lose access to the LDAP/AD server for some reason, you may be temporarily unable to log in to the Configuration Manager. If necessary, you can restore Root access to ensure that you can still manage your PrinterOn service.

To restore Root access to the Configuration Manager:

1. Open any text editor. You **must** open the editor as administrator. To open the text editor as the administrator:

    a) In the Windows **Start** menu or File Manager, right-click the text editor.

    b) Select **Run as Administrator**.

2. In the text editor, open the following file:

    C:\Program Files (x86)\PrinterOn Corporation\PrinterOn Server Install Manager\printeron-web\WEB-INF\classes\ponconf.properties

3. In the ponconf.properties file, locate the following entry:

    ponconf.rootUser = false

    and change it to the following:

    ponconf.rootUser = true

4. Save the file. The Root User is restored, and the password is reset to the default.

5. Restart the PrinterOn Configuration Manager service from Windows services.

2.6.6 Logging out

To log out of the Configuration Manager:

1. Click **Settings** (⚙) > **Logout**.

3

Managing and configuring PrinterOn printers

The **Printers** tab lets you to create, edit, and manage your PrinterOn printers. A PrinterOn printer is a virtual printer that you map to a physical printer. You can define the printing behavior and capabilities for that virtual printer to either expose or hide the features of the physical printer that it represents. For a more detailed description about PrinterOn printers, see PrinterOn printers.

You can add as many PrinterOn printers as your license permits. However, before users can submit print jobs to a PrinterOn printer, you must map the PrinterOn printer to a physical printer or print queue. The physical printer or print queue is known as the *output destination*.

When you add a new PrinterOn printer, it is preconfigured with a number of default settings. In fact, configuring the output destination for each of your printers is the only required configuration you must perform. However, it is strongly recommended that you take the time to change some of the default settings, such as the name and location of the printer, to values that are more meaningful.

When your install PrinterOn Enterprise, by default, the installer creates up to three default PrinterOn printers. When you first view the Printers tab, these printers are displayed in the list of available printers.

3.1 Viewing the Printers List

To view your PrinterOn printers:

1. In the Configuration Manager, click **Printers**. The Printers tab appears, displaying a list of currently available PrinterOn printer definitions.

3.2 Adding PrinterOn printers

You can add as many PrinterOn printers to your deployment as your PrinterOn license permits.

To add a new PrinterOn printer:

1. In to the Configuration Manager, click **Printers**.
2. Click **Add Printer**. A new virtual printer is added to the printers list.
3. Configure the printer definition settings as necessary.

3.3 Working with the Printers list

You can interact with the Printers list to perform a variety of functions.

Column	Description
Enabled	Indicates whether the selected printer appears in the user's list of available PrinterOn printers. Click the icon to enable or disable the selected printer.
Printer Name	The public name used to identify the printer for users.
Output Destination	The location of the physical printer, print queue, or file to which the PrinterOn printer directs print jobs. You must define the Output Destination for the PrinterOn Server to communicate with your physical printers, or with a print queue. You set the output destination in the Output Location settings panel of the Printer Configuration dialog. For detailed information, see Configuring Printer Output Destinations.
Guest	Indicates whether the printer allows guest users (that is, users without credentials) to submit print jobs. **Note:** This column only appears when the **Guest Login Enabled** setting selected for your Authentication method. Click the icon to enable or disable guest printing for the selected printer.
Approval	Indicates whether the approval screen appears, allowing the user the option to cancel the print job before it is submitted to the printer or to the print queue. Click the icon to enable or disable the approval screen for the selected printer.
PQMS	Indicates whether the printer is enabled for the PrinterOn Queue Management System. This column is read-only. To configure the printer to use Google Cloud Printing, see Configuring the PrinterOn Queue Management System (PQMS) workflow.
GCP	Indicates whether the printer supports Google Cloud Printing. This column is read only. To configure the printer to use Google Cloud Printing, see Configuring the Google Cloud Print workflow.
Discovery	Indicates whether the printer is discoverable by users of iOS or macOS devices that support AirPrint. Click the icon to enable or disable discovery.

3.4 Configuring individual printer settings

Individual PrinterOn printer settings are configured through the **Printers** tab. Each printer can be configured individually.

If you have a large number of printers to configure, you can configure a single printer and then use that printer as a template for other printers to quickly copy groups of settings. For more information, see Copying template settings to multiple printers.

To configure a single PrinterOn printer:

1. In the PrinterOn Printers list, click ● next to the printer that you want to configure. The printer actions appear.

2. Click **Configure**. The Printer Configuration dialog appears. The dialog contains the printer ID summary, along with a printer-specific QR code.

> **Note:** You can use the QR code to quickly locate and print to the printer using the PrinterOn Mobile apps.
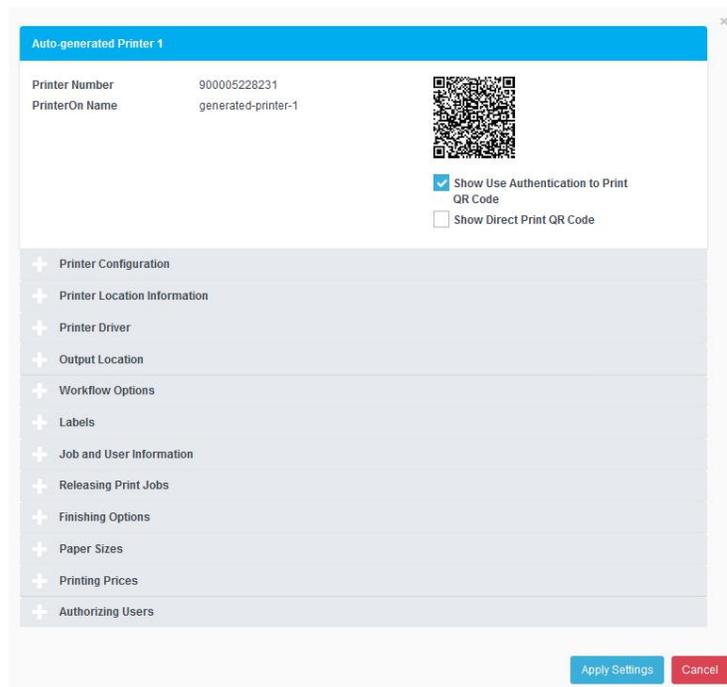
3. Click on any section to expand the configuration options. See the following sections for details.

    - Defining the printer identification settings

    - Defining the printer location settings

    - Specifying printer driver information

    - Configuring the printer's network location

    - Configuring printer-specific workflow options

    - Configuring user input labels

    - Configuring print job and user information

    - Configuring print release settings

    - Configuring finishing options

    - Configuring paper sizes

    - Configuring print service pricing

    - Configuring authorization settings

4. When you have finished modifying the printer configuration, click **Apply Settings**.

5. To ensure that your changes are pushed out to all PrinterOn components, click to synchronize your printers.

3.4.1 Defining the printer identification settings

The Printer Configuration settings define basic identification information for the printer. This information is displayed to users and can be used to search for and locate destination printers.

3.4.1.1 Printer Configuration settings

Setting	Description
Printer Description	A descriptive label that describes the printer to users. The value should be unique and descriptive. **Note:** PrinterOn does not enforce uniqueness on this value, but recommends that you set this value to a simple and easy-to-understand label for the printer.
PrinterOn Name	A unique printer queue name used throughout the software to both identify and organize printers. This value is combined with the email domain (specified in the Workflow Option settings) to create the email address for the printer, to which users can email print jobs. For example, if you name the printer warehouse-printer-1, and your email domain is defined as emailprint.com, the resulting email address for this printer would be: warehouse-printer-1@emailprint.com
Department	The Printer Department to which the printer belongs. The drop-down list only lists existing departments. Printer departments are used by PrinterOn to organize printers into groups. These departments can be used in conjunction with various authentication methods to define access control rules to control which users can access which printers. For information about creating departments, see Managing printer departments.
Default Printer Language	The default language for the printer, which the server uses to respond to email print jobs.
External ID	The external ID for this printer.
Web Services ID (*Advanced view* only)	The email address provided by HP for your HP printer. You can get this value by accessing the printer's Embedded Web Server (EWS), which lets you access the printer configuration settings remotely from any computer that is connected to the same network as the printer. For use with HP Printers only.

3.4.2 Defining the printer location settings

The Printer Location Information settings define the physical location of the printer, including address and GPS coordinates.

Printer Location Information	
Address	221 Mcintyre Drive
City	Kitchener
State/Province	ON
Country Code	CA
Postal Code	N2E 3S5
Latitude	43.402728
Longitude	-80.480358

3.4.2.1 Printer Location Information settings

Setting	Description
Address, **City,** **State/Province,** **Country Code,** **Postal Code**	The physical address for the printer. Mobile app users looking for a PrinterOn enabled printer can search on any value of the address to locate a printer. The mobile app also displays the address in the Printer Details.
Latitude, **Longitude**	The GPS coordinates for the location of the printer. The GPS coordinates are used to display the printer location on a map when users attempt to locate a printer using the PrinterOn Mobile app.

3.4.3 Specifying printer driver information

The Printer Driver settings define the printer driver used by the PrinterOn Server to convert documents for the destination printer.

PrinterOn includes a number of print drivers with the server installation that provide basic support for many common printers, including PCL, Postscript, and XPS print output.

Printer Driver	
Print Drivers	PrinterOn
	PrinterOn Generic PCL 6
Model	PrinterOn Inkjet
Printer Model Name	Printer

3.4.3.1 Printer Driver settings

Setting	Description
Printer Driver	The printer driver that the PrinterOn Server uses to process any jobs sent to the printer. Printer drivers are sorted by manufacturer. First, select the printer driver manufacturer from the upper list, then select the printer driver from the lower list. **Note:** If multiple servers are being used for document processing, ensure that the same driver is installed on all servers.
Model	Printer driver information that is presented to the user when viewing printer details. This value does not need to match the actual printer model.
Printer Model Name	The printer model name. This field is only used when you specified Samsung as the Printer Driver manufacturer and Samsung Universal EMU V2 as the printer driver, and allows the PrinterOn to optimize output for specific Samsung printer models. If you don't know the specific model, select **UnsupportedMono** or **UnsupportedColor**.

3.4.4 Configuring the printer's network location

The Output Location settings allow you to specify the network location of the physical printer to which this PrinterOn printer definition is mapped, and to define how the server delivers print jobs to this printer (for example, directly, via a PDS, or via a PDH). You can also specify whether the printer is an IPP printer that bypasses the PDS.

3.4.4.1 Output Location settings

Setting	Description
Printer is an IPP Printer	When checked, indicates that the printer supports the IPP protocol. When you enable this setting, the remaining settings change to simplify the configuration. **Note:** When **Printer is an IPP printer** is enabled, the remaining Output Location settings are disabled and set to **Direct Printing Only**, which indicates that jobs are sent directly to the printer. This setting is not configurable.
Printer Address	The IP address and port for an IPP printer. **Note:** This field is only displayed only when **Printer is an IPP Printer** is enabled.
Attach Printer To	Links the printer with a Print Delivery Station. This field is only displayed only when **Printer is an IPP Printer** is disabled. **Note:** You can also configure this setting for printers with an embedded PDS in the Link Printers dialog. For more information, see Linking printers with a Print Delivery Station.

Setting	Description
Output Destination	Defines the physical printer, print queue, or file to which the PrinterOn printer is mapped. You must define the Output Destination value to provide the target to which the PrinterOn Server directs all print jobs sent to the selected PrinterOn printer. For detailed information about defining the output destination, see Configuring Printer Output Destinations.
Allow Printing Directly to PDS	When checked, indicates that print jobs are sent to the PDS server. Note: Only select this option if the PDS is accessible from the main server. In some cases, print jobs can only be delivered to a PDS using an intermediate Print Delivery Hub (PDH).
Server Address	The fully qualified network address of the Print Delivery Station server that manages this printer. Select a scheme to indicate whether SSL will be used. Often, this is simply the address of the local server. Indicating an explicit port along with the server address can improve print performance. The server automatically uses the specified port, if provided. Otherwise, it scans ports 80, 443, and 631, as well as SSL and non-SSL connections, which can slow delivery. Note: This field is only displayed when **Allow Printing Directly to PDS** is selected.
Print Directly to PDS Only	When checked, all print jobs are printed directly to the PDS, and are not sent to a PDH. This setting only applies if a PDH is available. In most cases, you should enable this setting.
Use an Alternate/Local Print Delivery Hub to Host Print Jobs	When checked, indicates that a Print Delivery Hub server is available for printing. This option should be specified if a PDS is accessible directly by the server. In some cases, this option may be used if multiple PDS servers are deployed for the same printer, for redundancy. Configuring both a PDS and PDH server can assist desktop printing using PrintWhere for roaming users who may move between networks regularly and cannot always contact PDS.
Server Address	The fully qualified network address of the Print Delivery Hub server. Select a scheme to indicate whether SSL will be used. Indicating an explicit port along with the server address can improve print performance. The server automatically uses the specified port, if provided. Otherwise, it scans ports 80, 443, and 631, as well as SSL and non-SSL connections, which can slow delivery. Note: This field is only displayed when **Use an Alternate/Local Print Delivery Hub to Host Print Jobs** is selected.

3.4.5 Configuring printer-specific workflow options

The **Workflow Options** panel allows you to configure which print workflows are enabled, as well as some other printer-specific workflow settings.

Workflow Options	
Enable Web Printing	☑
Enable PrintWhere Printing	☑
Enable Document API Printing	☑
Email Domain	company.com
Enable Email Printing	☑
	784151735@company.com
	generated-printer-2@company.com
Print Body of the Email	☑
One Release Code for All Attachments	☐

3.4.5.1 Workflow Options settings

Setting	Description
Enable Web Printing	When checked, the Web Print workflow is enabled for this printer, allowing users to open their browser to the Web Print portal to upload and submit a document for printing.
Enable PrintWhere Printing	When checked, the PQMS workflow is enabled for this printer, allowing users to print from the Windows queue using PrintWhere
Enable Document API Printing	When checked, workflows including Mobile workflow, Google Cloud Print workflow, and iOS Native Print workflow are enabled for this printer.
Email Domain	The email domain that should be appended to the printer name (specified in the Printer Configuration settings) when advertising email print addresses to users.
Enable Email Printing	When checked, the Email Print workflow is enabled for this printer. If disabled, users receive a message indicating the service is disabled.
Print Body of the Email	When checked, the body of an email is printed when receiving email print jobs. If disabled, only attachments are printed.
One Release Code for All Attachments	When checked, a single release code is provided to users when submitting email print jobs with multiple attachments. This setting is only used when release codes are enabled.
	If using embedded solutions such as the Ricoh HotSpot embedded agent with touch panel screens, where jobs may be individually selected at release time, you should enable this setting.

3.4.6 Configuring user input labels

User Input Labels are used to request information from users when printing. If the server requires additional user input, such as user credentials or a release code, before it can proceed with the print job, it displays a form to the user to gather this information. The User Input labels define the text displayed in the form.

The Labels settings also supports multiple languages; you can customize labels for each language you support.

> **Note:** The **Labels** settings are displayed in Advanced view only.

3.4.6.1 Labels settings

Setting	Description
Label Language	Specifies for which language the settings below are displayed. Select the language, then define the labels for that language.
User Identifier	The text displayed to request the user's name.
Client UID	Reserved for some custom integrations.
Session Meta Data	Reserved for some custom integrations.
Privacy Release Code	The text displayed to request the user's release code.

3.4.7 Configuring print job and user information

Print jobs sent from the server may require additional information used to identify the sender. The Job and User Information allows you to control how your server will collect and use this information. This information is usually reserved for specific 3rd party integrations.

3.4.7.1 Job and User Information settings

Setting	Description
User Identifier	When selected, the user is asked to provide Job Owner information that will be included with a print job.
Client UID (*Advanced view* only)	Used in combination with custom integrations of third-party solutions to request user information. When the adjacent **Secured** check box is enabled, the server does not save the Client UID.
Session Meta Data (*Advanced view* only)	Used in combination with custom integrations of third-party solutions to request user information. When the adjacent **Secured** check box is enabled, the server does not save the session metadata.
Anonymity Level (*Advanced view* only)	Specifies what level of identifying information is stored within the system for a print job. This setting allows you to suppress identifying information, including user data (such as a person's email address), or print job metadata (such as job size or page count). Valid values are: • **Optional**: The printer uses the Anonymity Level specified in the print request. • **Anonymous**: Suppresses user data. • **Minimal**: Suppresses print job metadata. • **Anonymous + Minimal**: Suppresses both user and job data.

3.4.8 Configuring print release settings

The Release Print Jobs settings define how jobs will be managed after printing. The Release settings are divided into basic settings for the PrinterOn solution, and Third-party integration settings required for integration of third-party print/output management solutions.

> **Note:** The third-party integration settings are displayed in Advanced view only.

3.4.8.1 Basic release settings

Setting	Description
Release Print Jobs	How print jobs are released. There are two options: • **Automatically when they arrive**: When selected, print jobs are automatically released to the printer or print queues without being held. When integrating with most print/output management solutions, you should select this option. • **Using a PrinterOn Solution or HotSpot printer**: Print jobs are released using a PrinterOn solution. Users must supply a Release Code or other identifying information to access their print jobs.
Privacy Release Code	Indicates if users must provide a release code to retrieve their print jobs. You should typically set this value to **Required** or **Optional** when using a PrinterOn Print Valet or embedded agent that supports entering a release code.
Always use numbered release codes (*Advanced view* only)	When checked, generated Release Codes contain only numbers. Available only when **Privacy Release Code** is set to **Required** or **Optional**.
Auto-generate release codes (*Advanced view* only)	When checked, the server creates unique Release Codes for jobs and supplies them to the user. Available only when **Privacy Release Code** is set to **Required** or **Optional**.
Enable Remote Job Release	When checked, indicates that Secure Remote Release is enabled for this printer, allowing users release print jobs without being present at the printer. Remote job release is supported by the Web, Mobile, and Email Print workflows. **Note:** Secure Remote Release requires specific printer, PDS, and workflow settings to be properly configured. For complete step-by-step instructions on setting up this feature for a printer, see Managing printer departments.

3.4.8.2 Third-Party Integration settings

> **Note:** The third-party integration settings are displayed in Advanced view only.

Setting	Description
Enable 3rd Part Integration	When checked, lets you set the following settings to define release settings for your third-party Print Management Integrations:
Print Management Integration	When **Enable 3rd Part Integration** is enabled, defines the integration that is used with your PrinterOn Server.
Additional Integration Options	When **Enable 3rd Part Integration** is enabled, defines the additional integrations, if required by the selected **Print Management Integration**. In some cases, multiple integrations need to be combined to provide a final workflow.
Enable Advanced Integration Features	When **Enable 3rd Part Integration** is enabled, defines whether customized delivery of information is enabled. Please consult with your integration partner to determine if you should set this option. **Note:** Enabling this option when not required will result in incorrect job information being transmitted to the integration.
Enable Printer Based Authorization Integration	When **Enable 3rd Part Integration** is enabled, defines whether the PrinterOn Server supports printer-based authorization of jobs.
Inject a PJL Header container if none exists	When checked, the PrinterOn Server injects a PJL header into the print job. Many printers and print/output management solutions use PJL headers to collect job information. Some print drivers do not automatically include these PJL headers. If you encounter issues with your integration, enabling this option may be required.
Manage PJL headers for Passthrough Jobs	When checked, the PrinterOn Server modifies PJL headers. PrinterOn is able deliver print jobs from 3rd party systems through the print service. In some cases, those jobs may be pre-rendered data that contains PJL headers. This setting allows the PrinterOn server to process and modify these headers as necessary to prevent jobs from failing.

3.4.9 Configuring finishing options

The Finishing Options settings allow you to configure what finishing options are supported, and set additional limits or default behavior.

3.4.9.1 Finishing Options settings

Setting	Description
Include a Cover Page with print jobs	When checked, a cover page is added to each print job, identifying the sender and the time the job was submitted.
Use Document Conversion	When checked, the PrinterOn Server attempts to convert the document into an electronic presentation format such as XPS, rather than render it for printing. Any web links in the original document are preserved and functional in the converted file.
	Currently, PrinterOn only converts Microsoft Office formats (.pptx, .docx, and .xlsx). The only output format supported is XPS.
	Notes:
	• To support document conversion, Microsoft Office must be installed on the same machine as the PrinterOn Server.
	• To convert documents, you must specify the XPS Driver in the Printer Driver settings.

Setting	Description
Print Embedded Documents	When checked, the PrinterOn Server will attempt to extract and print any documents that are embedded in the original document.
	Notes:
	• Currently, the PrinterOn Server only supports printing of documents that are embedded in PowerPoint (.ppt, .pptx) documents.
	• Only documents embedded in the master document are printed. If an embedded document itself contains embedded documents, those documents are ignored.
Late Binding Options	When checked, users can modify change finishing options for the print job at the printer before printing the document.
	Note: For this option only impacts those printers with the PrinterOn Agent for HP installed.
Color Printing	Defines whether color printing is supported. This setting allows users searching for printers to limit their search to those printers that support color.
	If you have a color printer but wish to discourage users from printing in color, select **Does not support color printing**.
BW/Color Default	Defines the default color option that is displayed to the user, when **Color Printing** is set to **Supports color printing**. If **Color Printing** is set to **Does not support color printing**, then this setting does not appear.
	You can choose from the following options:
	• **Black & White Only**: The printer only prints in black and white.
	• **Color Only**: The printer only prints in color.
	• **Black & White Default**: The user can choose between black and white or color printing, with **Black & White** selected by default.
	• **Color Default**: The user can choose between black and white or color printing, with **Color** selected by default.

Setting	Description
Copy Management	Specifies how print copies are managed when the user has chosen to print multiple copies of a document. You can choose from the following options: • **Application-based**: The source application for the document determines how to manage print copies. Typically with application-based copy management, the document print data is simply sent to the printer once for each copy specified. Because multiple copies of the document data are sent to the printer, this option can result in large print data streams. This is the default setting. • **PJL-based**: Some printers and MFPs support managing print copies though PJL headers instead of in the print data stream itself. If the printer connected to the queue supports PJL-based copy management, choosing this option can reduce print data size when multiple copies are printed. • **Driver-based**: The printer driver determines how to manage print copies based on the capabilities of the printer. If the driver can determine that the printer supports PJL headers and that it has a hard disk, it will use the PJL header to specify the number of copies to print. Otherwise, the document print data is sent to the printer the specified number of times.
Duplexing Type	Defines the duplexing configuration. If you prefer to let the printer control duplexing, select **Not Managed**.
Maximum Page Count	The maximum number of pages a print job may use. Print requests exceeding this limit will are accepted. The maximum page count includes the cover page.
Maximum Printed Size	The maximum data size of a print job. Print requests exceeding this limit will are accepted.
N-Up Supported	Defines whether multi-page layouts, in which multiple pages are printed on a single sheet of paper, are supported.
PJL Encoding (*Advanced view* only)	Specifies the Printer Job Language encoding. If your printer needs to support double-byte characters, set this to UTF-8 and check **Override Encoding Specification**.

3.4.10 Configuring paper sizes

You can configure which paper sizes are available for the printer and manage what paper-selection options the user can choose when they print.

3.4.10.1 Paper Sizes settings

Setting	Description
Search	Lets you search a specific paper size. Enter a partial paper size to filter results.
Supported	When checked, the adjacent paper size is supported by the printer. You cannot disable this setting for the default paper size.
Make Default	When clicked, the adjacent paper size is used as the default paper size for the printer. When a user prints to this printer, this paper size is selected by default in all print workflows.

3.4.11 Configuring print service pricing

The Printing Prices settings configure pricing information and behavior when charging for print services.

Printing Prices

Charge for Print	☑
Currency	USD
Media Size	Single-sided Price
Letter	$ 0 /pg
Minimum charge per job	$ 0
Price includes all taxes	☐
Tax Rate in Percentage	% 0.00
Charge for cover page if cover pages are enabled	☐
Show price to users	☐
Show job price on cover page	☐

3.4.11.1 Printing Prices settings

Setting	Description
Charge for Print	When checked, users are charged a fee for each print job sent to this printer. When you enable this setting, additional settings appear, letting you define the specific payment details, such as currency, cost per page, and others.

3.4.12 Configuring authorization settings

The Authorizing Users settings configure an authentication loop to ensure that users have been authenticated and are authorized to print before the job is released to the printer. The user is redirected to a specified URL to provide the necessary credentials before they can continue.

3.4.12.1 Authorizing Users settings

Setting	Description
Requires Authentication to Print	When checked, users are prompted for their credentials when scanning the QR code via the PrinterOn mobile apps.
User Authentication URL	When checked, users are redirected to the URL specified in the adjacent field for authentication.
Web Authorize URL	When checked, users are redirected to the URL specified in the adjacent field for authorization to use Web Print job submission.
Mobile Authorize URL	When checked, users are redirected to the URL specified in the adjacent field for authorization to use Mobile Print job submission.
Security Protocol	The level of security that must be passed before PrinterOn continues to process the print job. The value can be one of: • **ClearText**: Basic validation. PrinterOn only checks to determine that the user has been authorized/approved to print using the selected workflow. • **MD5**: Increased validation. PrinterOn checks that the users is authorized/approved to print, and checks for an MD5-based security token, which must also be validated before printing can continue.

3.5 Configuring Printer Output Destinations

The Output Destination setting defines the physical printer, print queue, or file to which the PrinterOn printer directs print jobs. You must define the Output Destination for the PrinterOn Server to communicate with your physical printers, or with a print queue. The Output Destination is defined in the Output Location settings panel of the Printer Configuration dialog.

Output Destination	http:// ▾	192.168.1.116/cps	✕

The following table outlines how to define the Output Destination.

If your printer...	Then use this scheme:	And define the destination as follows:	Examples
Connects directly to the PDS computer	local://	Click **Map** and select the correct printer from the list, OR enter the printer name in the text field.	local://HP LaserJet 4000 Series
Connects to the printer via a network or print spooler	share://	Click **Map Network** and select the correct printer from the list, OR enter the share name in the text field.	share://printer_server/my_share share://192.168.1.2/my_share
Can be reached directly by its IP address	tcp://	Enter the IP address and optionally, the port.	tcp://172.16.1.1:9100 raw://172.16.1.1:9100
Supports the IPP protocol	ipp:// ipps:// https://	Enter the IP address or URI of the printer followed by the printer queue. If your printer supports SSL, use the https:// or ipps:// schema.	ipp://172.16.1.1/ipp/port1 ipps://172.16.1.1/ipp/port1 https://172.16.1.1/ipp/port1
Supports the LPR protocol	lpr://	Enter the IP address or URI of the printer.	lpr://172.16.1.1
Outputs print jobs to file	file://	Enter the folder to save the printed jobs.	file://C:\Documents\printjobs

If your printer...	Then use this scheme:	And define the destination as follows:	Examples
Is integrated with the LRS VPSX server	lrsq://	The LRS VPSX server as well as port and queue name. **Note:** When using an LRS queue, the LRS Queue Data Transmission Application should be installed on the same machine that is hosting PDS.	lrsq://192.168.3.2:6612/my_docs

3.6 Managing and configuring Print Delivery Stations (PDS)

PrinterOn supports a wide range of deployment options. In many cases a single release station, referred to by PrinterOn as the Print Delivery Station, or PDS, is all that is required. In some deployments, multiple Print Delivery Stations will be used to distribute printers, provide redundancy, or connect printers in remote locations.

Note: The Print Delivery Station is only available with On-Premise Deployments.

3.6.1 Adding Print Delivery Station instances

The PrinterOn Server supports unlimited PDS instances. Generally, each PDS links to a list of printers for which it will receive jobs. The association between the PDS and its printers is done using a unique ID referred to as a Serial Number. Each PDS instance receives a Serial Number and Label to help identify it.

Adding a PDS is a two-step process:

1. First, you add and configure one or more new PDS instances, which generates the unique serial number and label for each instance.

2. Then, you install the PDS software on each computer that will host a PDS instance.

   During the PDS installation process, the installer requests that you supply your PrinterOn service license file. It then prompts you to select which PDS serial number that will be applied to the PDS software installed on that computer.

   For more information, see Installing and configuring a remote PDS.

To add a PDS instance:

1. Click **Home** > **Serial Numbers**.

2. Scroll to the bottom of the page and click **Add Print Delivery Station**.

3. In the Add Print Delivery Station dialog, enter the **Server Description** for the PDS. The server description is used to identify the PDS, so it should be meaningful.

4. Click **Add**.

3.6.2 Configuring the Print Delivery Station software

You can configure the PDS software from the Servers tab.

To configure a Print Delivery Station:

1. In the Configuration Manager, click **Printers** > **Servers**. The Servers tab appears.
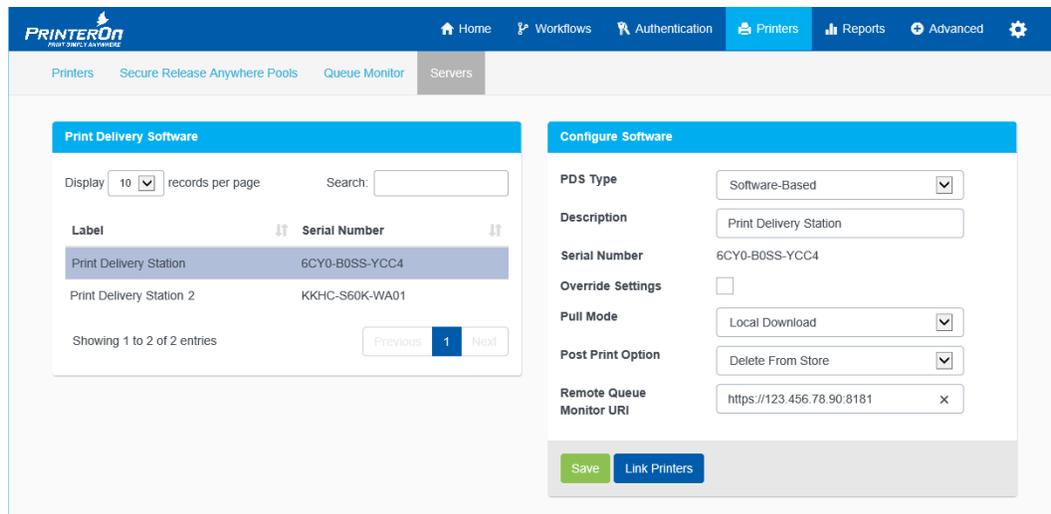
2. In the **Print Delivery Software** panel, select the PDS instance that you want to configure. If necessary, you can search a specific PDS instance using the **Search** field.

3. In the **Configure Software** panel, select the **PDS Type**. You can choose:

    *   **Software-Based**: Indicates that the PDS is a stand alone component installed on a server.

    *   **PrinterOn Agent for HP**: Indicates that the PDS is embedded within an HP printer or MFP.

        > **Note:** This PDS Type can only be used if you have subscribed to the Managed Cloud version of PrinterOn Enterprise.

    *   **Ricoh Hotspot**: Indicates that the PDS that is embedded within a Ricoh printer or MFP.

    > **Note:** If the **PDS Type** is a PrinterOn Agent for HP or a Ricoh HotSpot that will serve as a PDS agent for multiple devices, you must define the device as a host. For more information, see Editing the printer network destination for an embedded PDS agent.

    Each PDS Type has its own configuration requirements. The PDS Type you select determines which configuration settings appear in the panel.

    Software-based: Ricoh Hotspot:

    PrinterOn Agent for HP:

4. In the Configure Software panel, configure the remaining PDS software settings as necessary.

5. To configure which printers to associate with the selected PDS, click **Link Printers**. For more information, see Linking printers with a Print Delivery Station.

6. Click **Save** to save the PDS configuration.

3.6.2.1 Configure Software settings

Setting	Description
Serial Number	The serial number supplied by PrinterOn for this PDS instance. Each PDS instance that you add, regardless of type, is assigned a unique PrinterOn serial number. This value may be useful when configuring a software-based PDS installation to assist in identifying the specific instance.
PDS Type	The type of Print Connector used for this PDS instance. Select the PDS type that is appropriate for your deployment. Options include: • **Software-Based**: A PDS instance installed on a network server. • **PrinterOn Agent for HP**: A PDS instance that is installed on an HP device. This agent is only used in conjunction with a Managed Cloud version of PrinterOn Enterprise. • **Ricoh Hotspot**: A PDS instance that is embedded in a Ricoh device. Each PDS Type has its own configuration requirements. The PDS Type you select determines which configuration settings appear in the panel. **Note:** If the PDS Type is a Ricoh HotSpot or PrinterOn Agent for HP that will serve as a PDS agent for multiple devices, you must define the device as a host. For more information, see Editing the printer network destination for an embedded PDS agent.
Description	A description of the Print Connector to help you differentiate it from other PDS instances in a deployment. The description is a searchable value.
Machine ID *(PrinterOn Agent for HP, Ricoh HotSpot only)*	The serial number or machine identifier of the physical printer or MFP on which the PDS software is embedded. PrinterOn uses this value to validate the license and connect to the physical printer/MFP.

Setting	Description
PDH URI *(Ricoh HotSpot only)*	The fully qualified domain name of the Print Delivery Hub (PDH) server used by the embedded PDS to locate and download new print jobs. The URI should include the URL scheme (http:// or https://) and the port that is configured for the server. When using SSL, the server must be configured with a fully qualified SSL certificate. This value is downloaded by the software during initialization, which provides an easy way to pre-configure or modify the configuration of the software without interacting with the physical device. **Note:** Set this value only if you are integrating your embedded PDS with a Print Delivery Hub.
PDH Password	The password required to connect to the PDH server located at the **PDH URI**. In an on-premise deployment of PrinterOn Enterprise, this password must be configured in the PDH server software settings and supplied by the PDH server administrator to be entered in this field; if the value in this **PDH Password** field does not match the password specified in the PDH software settings, then the PDS will be unable to connect to the PDH to retrieve jobs. Beginning with version 4.2.4, in a Managed Cloud deployment of PrinterOn Enterprise, each PDS agent has its own unique password that it uses to connect to the PDH, so no password need be configured in the PDH software settings. **Note:** In PrinterOn Enterprise v.4.2.4 and later, if you are adding a password to a software-based PDS, you must also enter the same password in the PDS Configuration Settings (**Advanced** > **Components** > **PDS** > **Networking**, then locate the **PDH Password** field).

Setting	Description
Check Jobs URI *(Ricoh Hotspot only)*	The fully qualified domain name of the URI that this PDS instance polls to determine if new print jobs are available. Communication with this URI is very lightweight. No job data is communicated via this URI. All communication of Job data occurs via the PDH URI.
	The URI should include the URL scheme (http:// or https://) and the port (typically a non-SSL port, such as port 80) configured for the server.
	Note: If using SSL with a Ricoh HotSpot, the server must be configured with a fully qualified SSL certificate. Due to compatibility challenges with the Ricoh SDK/J platform, self-signed certificates are not supported. Use the scheme to determine whether SSL is enabled or not.
Check Jobs Interval *(Ricoh Hotspot only)*	How often the software should perform a Check Job operation to locate new jobs. The minimum time interval is 1 minute.
	Software versions that support PrinterOn's Push Notification do not use this value, and instead rely on the push notification technology. However, this value is still used when the software cannot establish a successful notification connection and must revert to polling.
Push Notification Timeout *(Ricoh Hotspot only)*	The length of time before push notifications time out and are considered expired.
	Only used when the software versions supports PrinterOn's Push Notifications.
Status Check Interval *(Ricoh Hotspot only)*	How often the software should check the status of the current print job.
Override Settings *(Software-Based PDS, Ricoh HotSpot only)*	Used by desktop PDS deployments to indicate if output destinations should be overridden by online settings if local settings have been made.
	Note: If you intend to import printers using a CSV file but want to set the printer's output destination in the PDS, you must enable this setting.
Pull Mode *(Software-Based PDS, Ricoh HotSpot only)*	How jobs are handled after being delivered to the Print Delivery Hub. The value can be one of:
	• **Local Download:** Indicates that jobs should be download locally to the PDS. Jobs are also kept on the PDH after download.
	• **Central Store:** Indicates jobs should not be automatically downloaded to the PDS; they are held on the Print Delivery Hub and downloaded on demand.

Setting	Description
Post Print Option *(Software-Based PDS, Ricoh HotSpot only)*	How jobs should be handled after being printed by the software on the printer/MFP. The value can be one of: • **Delete from Store:** Indicates that jobs should be deleted from the PDH after the user request the jobs are printed • **None:** Indicates that jobs should be left on the PDH after printing. Jobs will be purged automatically by PDH after its configured time.
API Token *(Ricoh Hotspot only)*	A security token used by the embedded PDS software on the agent to secure communication with the PrinterOn service. This value can be retrieved from the PrinterOn Configuration Manager and copied to this location to be downloaded and used by the software.
Enable Card Authentication *(PrinterOn Agent for HP, Ricoh HotSpot only)*	When selected, the PrinterOn Agent embedded on the printer should look for and use a card reader for authentication information. **Note:** For Ricoh Hotspot, this setting is only available if you have Ricoh Card Authentication Package enabled for your PrinterOn service.
Bypass User Login Page for Cards *(Ricoh HotSpot only)*	When selected, and **Enable Card Authentication** is also selected, the HotSpot software skips the Login page. **Note:** This setting is only available if you have Ricoh Card Authentication Package enabled for your PrinterOn service.

Setting	Description
User Authentication Workflow *(Ricoh HotSpot only)*	Indicates how the Ricoh Hotspot App determines what screen should initially be displayed to the user.
	You can select one of the following four values:
	• **Automatically Choose Workflow**: The HotSpot determines the most appropriate screen to display, based on the other configuration settings.
	• **Always Display Home Screen**: The HotSpot always displays two options to the user: **User Login**, which takes them to the User Login Page; and **Release Code**, which takes them to the Release Code Page.
	• **Always Display User Login**: The HotSpot displays the User Login Page.
	• **Always Display Release Code**: The HotSpot displays the Release Code Page.
	Note: If you have a hybrid deployment, you need configure your printer settings on the PrinterOn.com web admin portal to enable authentication:
	1. Log in to the PrinterOn.com web admin portal at www.printeron.com/administrators.
	2. Click the **Printers** icon.
	3. Locate the printer listing for the MFP with the Ricoh HotSpot embedded software, then click **Payment and Authentication**.
	4. In the **Authorizing Users** section of the Payment and Authentication page, enable **Requires Authentication to Print**, then save your changes.
Remote Queue Monitor URI	The URL and port used by CPS to communicate with the PDS to display the remote queue monitor, which is used to remotely release a print job to the printer.
	Defining this URI simplifies remote release for users by allowing them to access a central URL hosted by the PrinterOn Server to release their print jobs remotely, instead of requiring them to connect directly to the PDS host machine.
	By default, this URI is set to https://127.0.0.1:8181, which points to the local machine hosting the PrinterOn Server.

3.6.3 Linking printers with a Print Delivery Station

The **Link Printers** button provides a simple way to connect printers to Print Delivery Stations with simple drag and drop actions.

You can link printers with a PDS automatically or manually.

- Linking printers automatically
- Linking printers manually

3.6.3.1 Linking printers automatically

In order to automatically link printers to a PDS, you must first ensure that each printer and, if applicable, printer pool, that you want to link has the **Machine ID** value of the PDS in it's name. The PrinterOn Server searches for this value as it attempts to locate printers to attach to the PDS.

> **Note:** Only one printer pool can be automatically linked to a PDS. If more than one printer pool contains the PDS **Machine ID** value in its name, the PrinterOn Server links the first one it finds and ignores the rest.

To automatically link printers with a PDS:

1. Click **Printers** > **Servers**.

2. In the **Print Delivery Software** panel, select the PDS that you want to configure. If necessary, you can search a specific PDS instance using the **Search** field.

3. In the **Configure Software** panel, locate the **Machine ID** field and note the value.

4. Ensure that the **Machine ID** value is in the name of each printer you want to link.

5. If each printer includes the **Machine ID** value, return to the **Print Delivery Software** panel and click **Auto Linking**.

   The server will scan the list of printers and link every printer that contains the Machine ID of the PDS in its name to the PDS

3.6.3.2 Linking printers manually

To manually link a printer with a PDS:

1. Click **Printers** > **Servers**.

2. In the **Print Delivery Software** panel, select the PDS that you want to configure. If necessary, you can search a specific PDS instance using the **Search** field.

3. In the **Configure Software** panel, select **Link Printers**.
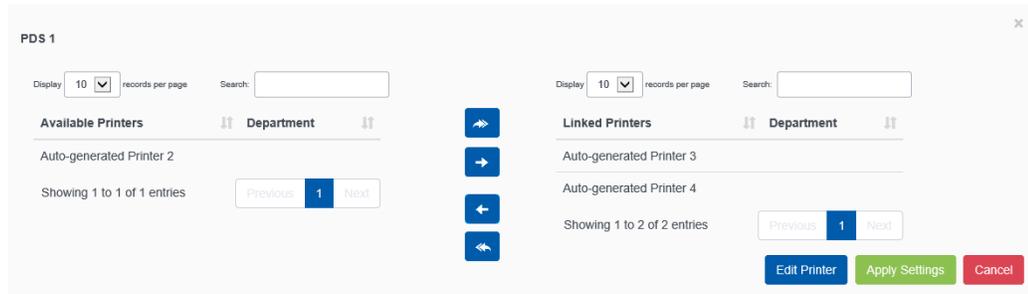
4. Link the printers to the PDS by moving them from the **Available Printers** list to the **Linked Printers** list:

   a) Select one or more printers from the **Available Printers** list.

   b) Drag the printers to the **Linked Printers** list, or click the arrow.

5. To unlink printers from the PDS:

   a) Select one or more printers from the **Linked Printers** list.

   b) Drag the printers to the **Available Printers** list, or click the arrow.

6. To edit the printer connection settings, click **Edit**. For more information, see Editing the printer network destination for an embedded PDS agent.

7. Click **Apply Settings**.

> **Note:** A printer can only be linked with a single PDS. Linking a printer to a PDS automatically unlinks it from any other PDS instance it might have previously been linked to.

3.6.4 Editing the printer network destination for an embedded PDS agent

When linking a printer to a PDS instance, you can edit the individual printers linked with that PDS to define a network destination for the device. The Edit Printer dialog also allows you to specify whether the device is a Ricoh device with an embedded PDS agent that will serve other devices.

> **Note:** The **Edit Printer** button only appears if the selected PDS is an embedded PDS agent, such as a Ricoh HotSpot.

To edit printer connection settings:

1. In the Link Printers dialog, select the printer you want to configure and click **Edit Printer**. The Edit printer dialog appears.

2. Configure the following settings as necessary:

Setting	Description
Local IP Address	The local IP address of the printer.
Port	The port the printer uses for communication.
Host *(PrinterOn Agent for HP or Ricoh Hotspot only)*	When enabled, indicates that the device has an embedded PDS agent that serves other devices.

3. Click **Apply Settings**.

3.6.5 Installing and configuring a remote PDS

Having a PDS on a different machine than the PrinterOn server is a common deployment scenario. You may need to install a PDS together with a PDH on a server that's located on a different network, or you might need to embed a PDS on a printer or MFP.

3.6.5.1 Before you begin

Before you install a remote PDS, you'll need to complete the following tasks:

1. Add a new PDS instance to your PrinterOn server. This creates a new PDS serial number. When you install the PDS on the remote server, you'll choose this serial number, which links the configuration settings to the PDS component.

2. Configure the PDS instance as necessary. Ensure that you select the PDS you just created in Step 1.

3. Link printers to your new PDS instance.

4. Configure each linked printer as necessary. Because the PDS is on a different machine, at minimum, you'll need to configure **Server Address** in the Print

Delivery settings to properly define the IP address of the machine that is hosting the new PDS.

5. Ensure that the Internal Service URI value is correctly configured. The Internal Service URI is used by the subcomponents to communicate with the Central Print Services in a distributed deployment.

6. Download your license file on the parent PrinterOn server and copy it to the remote server that will host the PDS.

3.6.5.2 Installing the PDS on a remote server

Once you have complete the configuration steps above, you can install the PDS component on the remote server.

To install a remote PDS:

1. Run **PSIM.exe** to launch the PrinterOn Installation Wizard. The wizard guides you through the installation of the PrinterOn software. You can download the PSIM.exe from printeron.com.

2. Click **Next** at the Welcome screen, then accept the License Agreement to proceed with the installation.

3. On the License Summary File screen, browse to your PrinterOn license file and select it, then click **Next**.
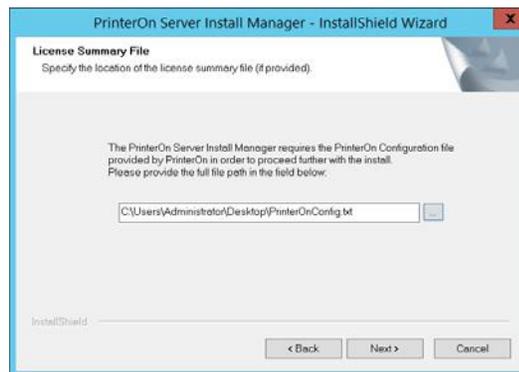
4. On the Setup Type screen, choose **Custom**, then click **Next**.
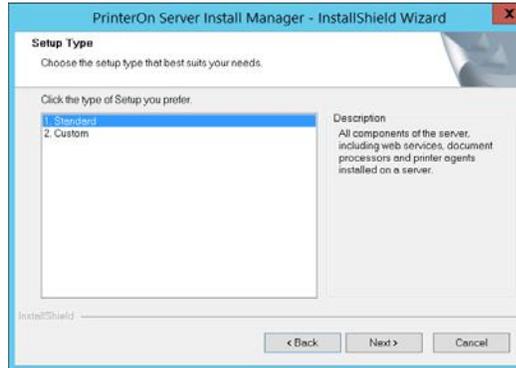
5. In the Select Features screen, select only **Print Delivery Station**, then click **Next**.
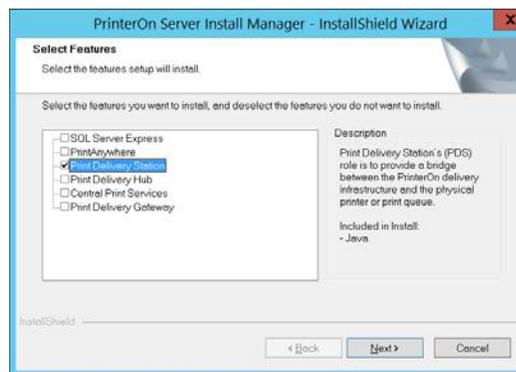
6. On the Serial Numbers screen, select the serial number for the PDS instance you are installing on the remote host, then click **Next** to install the PDS.
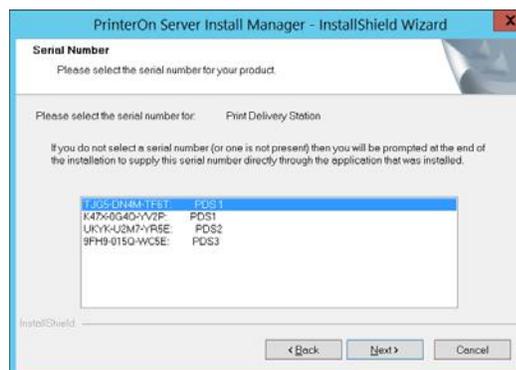
7. When the installation is complete, click **Finish**, and then reboot the computer.

8. If you choose, you can connect this PDS to a parent configuration server. For more information, see Connecting remote servers to a parent Configuration Manager.

3.7 Enabling Secure Remote Release for printers

Secure Remote Release allows users to submit a release code to the printer remotely, from their mobile device or browser, instead of requiring them to type the release code in at the printer. Once the user releases the print job, the printer adds it to the print queue and prints it in sequence.

To set up Secure Remote Release, you'll need to perform the following tasks:

1. Define the Remote Queue Monitor URI for each remote PDS.
2. Configure a printer to support Secure Remote Release.
3. Ensure that the PDS that services that printer uses SSL.

> **Note:** If you intent to support Secure Remote Release with the Mobile Print workflow to allow users to release their jobs directly from their mobile devices, you'll also need to ensure that the **Document API URI** is properly configured to point to the external service URI. For more information, see Configuring the Mobile Print workflow.

3.7.1 Defining the Remote Queue Monitor URI for each remote PDS

The Remote Queue Monitor URI is the URL through which the PrinterOn Server accesses the print job queue on a remote PDS. By default, the server is configured to point to port 8181 on the local host (127.0.0.1:8181). If the PDS is installed on a different server than the PrinterOn Server, then you must configure this value to reflect the IP address of the PDS host computer.

Defining a Remote Queue Monitor URI allows users to connect to the PrinterOn server to release their print jobs remotely, instead of requiring them to connect directly to the PDS host machine.

To configure the Remote Queue Monitor for a for a printer:

1. In the Configuration Manager, click **Printers** > **Servers**.
2. In the Print Delivery Software panel, select the PDS instance you want to configure from the list of available Print Delivery Stations. The values in the Configure Software Panel change to reflect the selected PDS.
3. In the Configure Software panel, locate the **Remote Queue Monitor URI** field.
4. Enter the IP address of the machine hosting the remote PDS, and the port on which the PDS listens. By default, PDS listens on port 8181.
5. Click **Save**.

3.7.2 Configuring a printer to support Secure Remote Release

To configure the Secure Remote Release feature for a printer:

1. In the Configuration Manager, click **Printers**.
2. In the PrinterOn Printers list, click ⊕ next to the printer that you want to configure to use the Secure Remote Release feature. The printer actions appear.

3. Click **Configure**.
4. In the Printer Configuration dialog, expand the **Releasing Print Jobs** settings and ensure that:

    • **Privacy Release Code** is set to **Optional** or **Required**.
    • **Enable Remote Release** is selected.
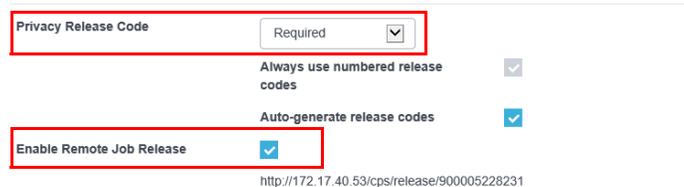
Expand the Print Delivery settings and ensure that:

    • **Server Address** points to the IP address of the machine hosting the PDS instance that services the selected printer.
    • **Server Address** uses the HTTPS scheme.

5. Click **Apply Settings**.

3.7.3 Ensuring that the PDS is configured to use SSL

To configure the PDS to use SSL:

1. In the Configuration Manager, click **Advanced** > **Components**.

2. Click the **Configure** button adjacent the **Print Delivery Station** component. The PDS component configuration appears.

3. Click **Listeners**, then locate the **Default IPP Port** and check **SSL**.

4. Click **Apply Settings**.

3.8 Managing printer departments

Printer departments are used by PrinterOn to organize printers into groups. These departments can be used in reports to determine usage of certain printers, but more importantly, printer departments can be used along with LDAP/AD Organization Units and AD Groups to create user rules that provide additional access control options, and limit groups of printers to existing user groups.

For more information about using printer departments to control user access, see Configuring LDAP/AD access control rules.

The PrinterOn Server provides a simple, drag & drop interface to manage and configure departments.

> **Note:** Department management only applies to On-Premise Deployments.

3.8.1 Adding, removing, and editing departments

New Printer Departments can easily be added, and existing departments can be deleted or renamed using the Manage Departments dialog.

To manage your departments:

1. Select **Printers**.
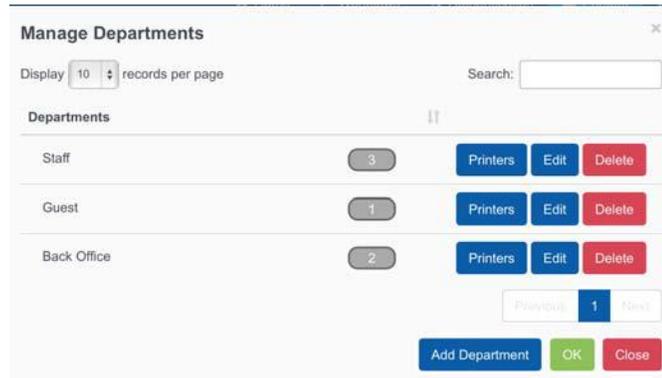
3. Click the **Printers** button adjacent to the department you want to add printers to. The Link Printers dialog appears.
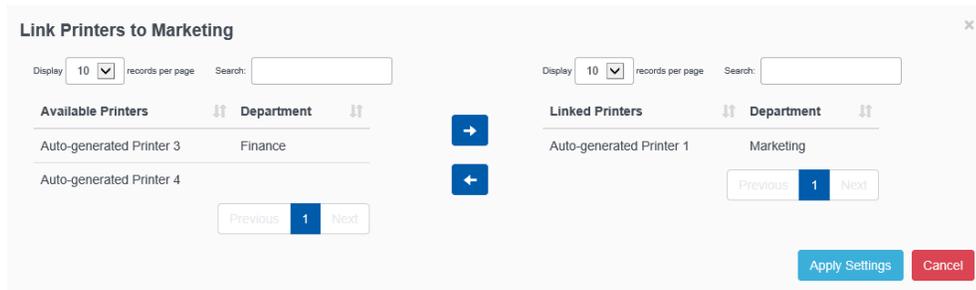
4. To add printers to a department:

   a) Select one or more printers from the **Available Printers** list.

   b) Drag the printers to the **Linked Printers** list, or click the arrow.

5. To remove printers from a department:

   a) Select one or more printers from the **Linked Printers** list.

   b) Drag the printers to the **Available Printers** list, or click the arrow.

6. Click **Apply Settings**.

3.9 Configuring multiple printers at once

To simplify adding and configuring printers for organizations with multiple printers, PrinterOn offers a couple of solutions:

- Copying template settings to multiple printers
- Configuring printers using configuration profiles

3.9.1 Copying template settings to multiple printers

The PrinterOn Configuration Manager allows you to copy settings across printers to quickly configuring multiple printers at once.

> **Note:** To avoid performance issues, you should limit the copy operation to a maximum of 100 printers.

To copy settings, you must first configure at least one printer to use as a configuration template. You can then copy those settings to one or more additional printers in bulk. You can even choose which groups of settings you want to copy, allowing you to omit certain settings from the copy process.

To copy printer settings:

1. In the PrinterOn Printers list, click ⊕ next to the printer that you want to use as the template configuration. The printer actions appear.

2. Click **Copy**. The Template page appears.
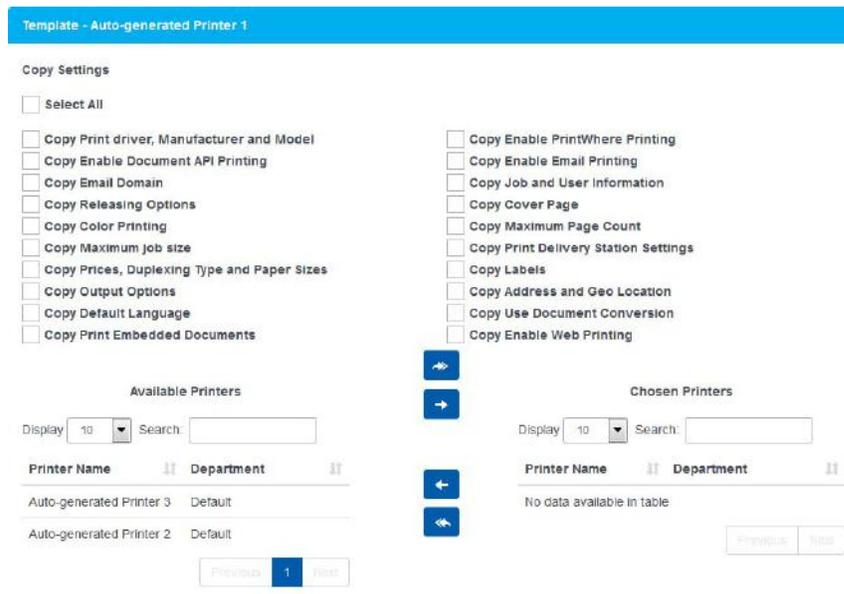
3. The **Copy Settings** are organized into groups. Select one or more groups of settings that you want to copy to other printers.

4. Select the printers to which you want to apply changes by moving them from the **Available Printers** to the **Chosen Printers** list.

5. Click **Apply Settings**.

3.9.2 Configuring printers using configuration profiles

To create and configure multiple PrinterOn printers at once, you can create a printer configuration profile and then import that file into the Configuration Manager. A configuration profile is a CSV text file that defines configuration properties of multiple printers. Configuration profiles simplify the printer creation and configuration process when you have a large number of printers. For information on creating a configuration profile, see Appendix G: Creating a printer configuration profile.

A printer configuration profile defines a number of settings, including:

- Printer Name
- Printer Description/Location Settings
- Print Workflows Options
- Print Driver Settings
- Printer Capabilities

To further simplify the process, you can use printer configuration profiles in conjunction with printer templates. For certain properties, if values are left blank, the server applies the value found in the specified template.

3.9.2.1 Importing a printer configuration profile into the Configuration Manager

To import a printer configuration profile:

1. In the Configuration Manager, click **Printers**. The Printers tab appears, displaying a list of currently available printers.

2. Click the **Import** icon.
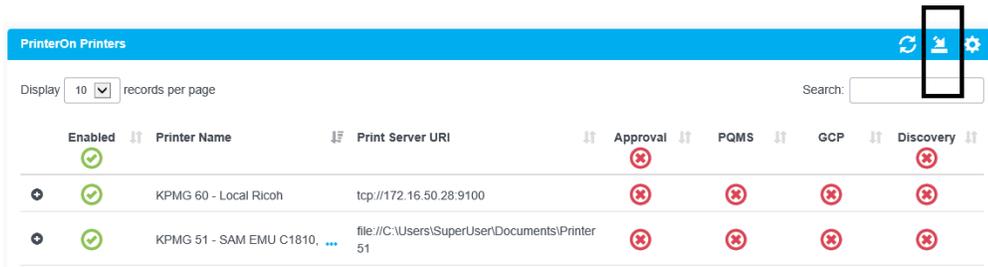
3. Click **Browse** and locate the CSV Data Set file to import.

4. Click **Upload**.

    Wait for the transaction to be processed. If there are no validation errors, the printers will be added or modified accordingly.

5. Verify the results by checking one or more printer settings.

4

Configuring Secure Release Anywhere pull printing

The PrinterOn solution supports pull printing through the Secure Release Anywhere feature. Pull printing simplifies printing for users; rather than require users to know the physical location of the specific printer they printed to, users simply print, then go to the nearest printer, enter their credentials or release code, and pull the job to that location to be printed.

PrinterOn's Secure Release Anywhere supports a variety of printers, MFPs, and release stations, and can be configured to work with built-in browsers, keypads, or with PrinterOn's PrintValet connected to single function printers.

To setup your PrinterOn Server to support Secure Release Anywhere, you need to perform the following tasks:

1. Add and configure your individual printers. Define the output destination to link the PrinterOn printer definition with a physical printer. For more information, see Managing and configuring PrinterOn printers.
2. Create one or more Secure Release Anywhere printer pools, and link the individual printers with a pool. For more information, see Creating and configuring Secure Release Anywhere pools.
3. Configure Secure Release Anywhere workflow options. For more information, see Configuring the Secure Release Anywhere workflow.
4. Set up your release stations to pull down print jobs. For more information, see Configuring Secure Release Anywhere release stations.

4.1 About Secure Release Anywhere

To implement pull printing, Secure Release Anywhere uses the concept of printer pools. A Secure Release Anywhere pool is a group of output destinations, or printers. Each output destination is represented as a PrinterOn virtual printer in the PrinterOn solution.

To the user, a Secure Release Anywhere printer pool appears as just another printer; users print to a Secure Release Anywhere pool just as they would any printer.

Secure Release Anywhere pools have the following features:

- Secure Release Anywhere pools can be configured like any other printer. You can configure options such as descriptive information, color/B&W, duplex, and supported driver.

  > **Note:**
  >
  > - The configuration you apply to the pool applies to every printer that is a member of that pool, regardless of the capabilities of the individual printer.
  >
  > - It is important to ensure that all printers in the pool can use the same driver and language. PrinterOn provides both generic PCL and Postscript drivers with the installation, which should work in most cases.

- Users can access Secure Release Anywhere Pools using any enabled PrinterOn workflow, including mobile apps, web print, Google Cloud Print, email, etc.

- Secure Release Anywhere pools are backwards compatible with existing PrinterOn apps and workflows. Once they have been configured and added to your solution, Secure Release Anywhere pools are available to all users.

- You can apply role-based access control to Secure Release Anywhere Pools, just as with regular printers.

- A single PrinterOn printer can be a member of multiple Secure Release Anywhere Pools.

4.1.1 Secure Release Anywhere deployment modes

To support different network requirements, PrinterOn supports two deployment modes for Secure Release Anywhere: Basic and Advanced.

Each deployment mode provides additional configuration options to further customize the options.

4.1.1.1 Basic Secure Release Anywhere

Basic Secure Release Anywhere is intended for networks where all servers and printers are accessible and can communicate on the same network.

Users may still submit using any print method and from any network. The PrinterOn server must be able to deliver jobs to printers on the same network.
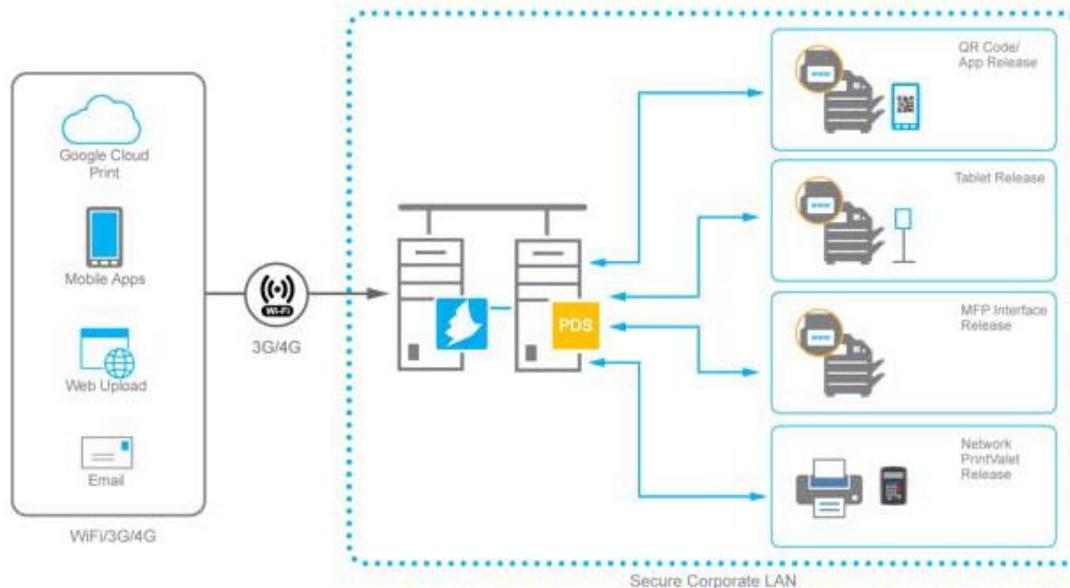
4.1.1.2 Advanced Secure Release Anywhere

Advanced Secure Release Anywhere extends the support for pull printing beyond a single network and provides global access for users.

Using the PrinterOn secure print delivery solution, jobs can be delivered between networks without requiring major changes to network configuration, opening ports between networks, or a wide area network.

Using the PrinterOn Print Delivery Hub, jobs can be delivered to, or made available to, multiple networks automatically. Administrators can then decide the optimal deployment based on their specific needs.

The advanced deployment mode is useful when enabling Secure Release Anywhere Pools across multiple networks. It allows a copy of print jobs to be delivered to each network automatically and decreases the time to complete the print. It also allows users to release their jobs in any network.
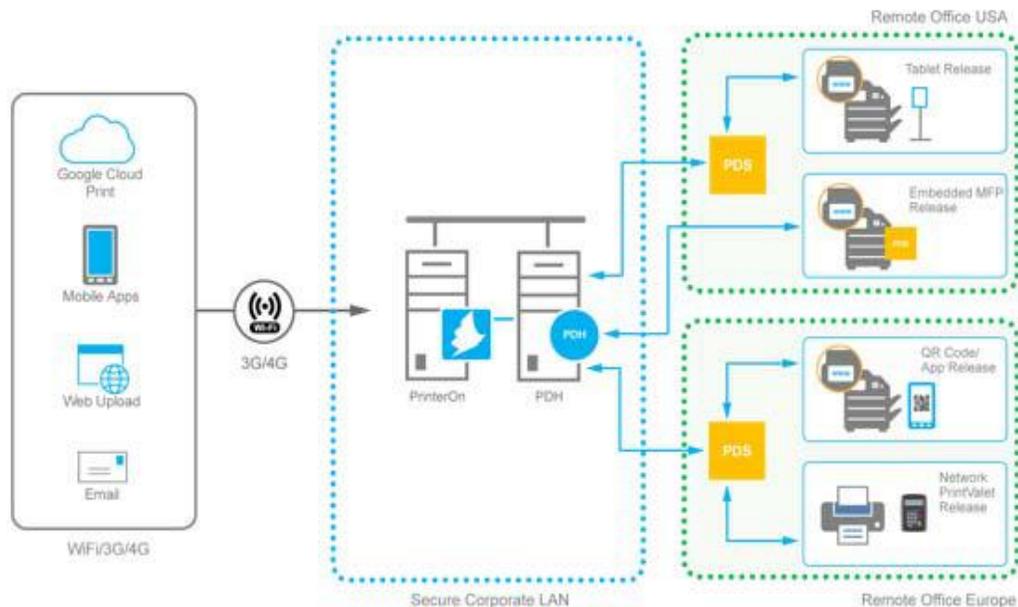
4.2 Creating and configuring Secure Release Anywhere pools

Before creating and configuring Secure Release Anywhere pools, ensure that all printer definitions are configured and their output destinations are defined.

> **Note:** Ensure that the **Release And Privacy** mode for all printers is set to **General Delivery** to ensure jobs are correctly held.

Setting up a Secure Release Anywhere pool is a four-step process:
1. Add your pool.
2. Configure the pool settings.
3. Add printers to your pool.
4. Link the pool with a Print Delivery Station.

4.2.1 Adding a Secure Release Anywhere pool

To add a Secure Release Anywhere pool:

1. In the Configuration Manager, click **Printers** > **Secure Release Anywhere Pools**. The Secure Release Anywhere Pools list appears.
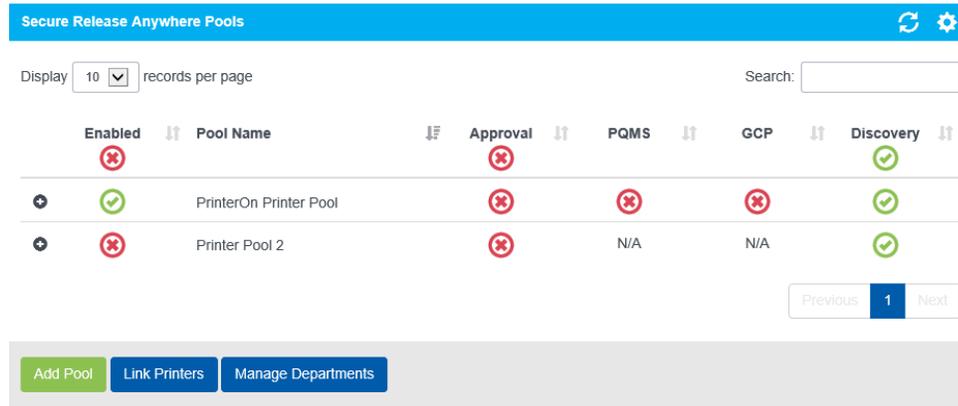
2. Click **Add Pool**. A new printer pool is added to the pool list.

You can now configure the pool settings.

4.2.2 Configuring the printer pool settings

The configuration settings that you apply to the Secure Release Anywhere pool apply to all printers that are members of the pool, regardless of their capabilities.

> **Note:** It is important to ensure that all printers in the pool can use the same driver and language. PrinterOn provides both generic PCL and Postscript drivers with the installation, which should work in most cases.

To configure the printer pool settings:

1. In the Pools list, click ⊕ next to the printer pool that you want to configure. The printer pool actions appear.

2. Click **Configure**. The Pool Configuration dialog appears.

3. Configure all settings. You configure the same settings for a printer pool as you do for an individual printer. For information on those settings, see Configuring individual printer settings.

4. Click **Apply Settings**.

You can now add printers to your pool.

4.2.3 Adding printers to a Secure Release Anywhere pool

Once a Secure Release Anywhere Pool has been created and configured, you can attach printers to the pool. A single PrinterOn printer can be added to multiple Secure Release Anywhere pools.

To link printers to a Secure Release Anywhere pool.

1. In the Pools list, click ⊕ next to the printer pool that you want to configure. The printer pool actions appear.

2. Click **Manager Printer Pool**.
3. Select one or more printers from the **Available Printers** column on the left
4. Click the **Right Arrow** or drag and drop the printers to the **Linked Printers** column.
5. Click **Apply Settings** to complete the configuration.

You can now link the pool with a Print Delivery Station.

4.2.4 Link a Secure Release Anywhere Pool to a Release Station (PDS)

In order for jobs to be delivered to a Print Delivery Station (PDS), the Secure Release Anywhere pool must be linked to one or more Print Delivery Stations.

A Secure Release Anywhere Pool MUST be associated with all Print Delivery Stations that will support release. Normally, any Print Delivery Station with a child printer should also have the Secure Release Anywhere Pool linked.

To link a pool with a PDS:

1. In the Configuration Manager, click **Printers** > **Secure Release Anywhere Pools**.

2. At the bottom of the Secure Release Anywhere Pools list, click **Link Printers**. The PDS Server dialog appears.
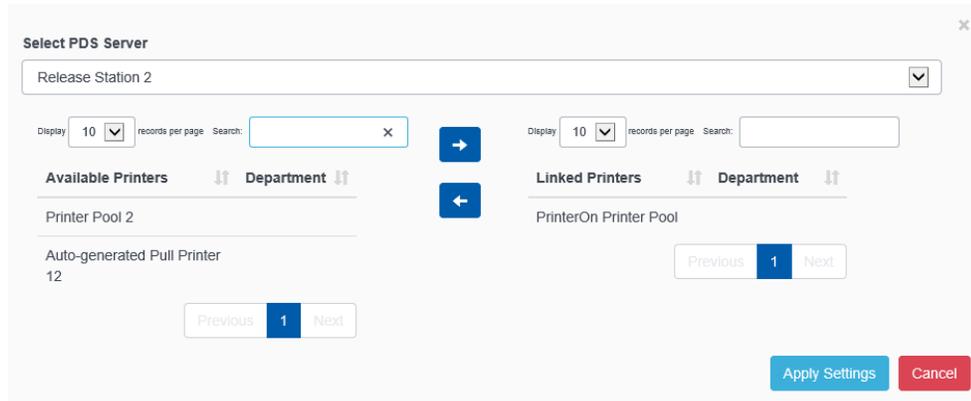
3. From the **Select PDS Server** drop-down, select the Print Delivery Station to which you want to link a Secure Release Anywhere pool.

4. Select the Secure Release Anywhere pool from the **Available Printers** column on the left.

5. Click the **Right Arrow** or drag and drop the printers to the **Linked Printers** column.

6. Click **Apply Settings**.

4.3 Configuring the Secure Release Anywhere workflow

You can configure PrinterOn's Secure Release Anywhere solution to meet specific workflow and network requirements. This allows you to configure behavior for job retention before and after printing, as well as configuring how jobs will be distributed throughout the network.

To configure the Secure Release Anywhere workflow:

1. In the Configuration Manager, click **Workflows** > **Secure Release Anywhere**.

2. From the **Secure Release Anywhere Mode** drop-down, choose which deployment workflow you are configuring:

    *   **Basic**: All servers and printers are accessible and can communicate on the same network. For more information on this deployment, see Basic Secure Release Anywhere.

    *   **Advanced**: Extends beyond a single network and provides global access for users. For more information on this deployment, see Advanced Secure Release Anywhere.

    The configuration panel for the selected mode appears.

3. Configure the workflow options as necessary:

    *   Configuring Basic Secure Release Anywhere

    *   Advanced Secure Release Anywhere workflow options

4. Click **Apply Settings**.

4.3.1 Configuring Basic Secure Release Anywhere

Selecting the Basic Secure Release Anywhere mode displays the **Standard Release Anywhere Settings**:

Standard Release Anywhere Settings		
Job Handling		
Enable Unreleased Job Cleanup	✓	
Cleanup Unreleased Jobs After	66	Hours
Cleanup Released Jobs After	22	Hours

Note: Jobs released by the user when Basic Secure Release Anywhere is enabled cannot be released to multiple printers in the pool.

4.3.1.1 Basic Secure Release Anywhere workflow options

Setting	Description
Enable Unreleased Job Cleanup	When checked, the Print Delivery Station automatically deletes print jobs that have not been released by users. If this option is not selected, print jobs are never deleted.
Cleanup Unreleased Jobs After	The length of time that print jobs that have not been printed are held by the Print Delivery Station. This applies to all printers managed by the Print Delivery Station.
Cleanup Released Jobs After	The length of time (from the moment they were first printed) that printed jobs should be held by the Print Delivery Station.

4.3.2 Configuring Advanced Secure Release Anywhere

Selecting the Advanced Secure Release Anywhere mode displays the **Advanced Release Anywhere Settings**:

Advanced Release Anywhere Settings	
Job Delivery	
Automatically Distribute Jobs	☑
Delete Jobs From Hub After Printing	☑
Job Handling	
Enable Hub Job Cleanup	☑
Cleanup Hub Jobs After	72 Hours
Enable Unreleased Job Cleanup	☑
Cleanup Unreleased Jobs After	66 Hours
Cleanup Released Jobs After	22 Hours

4.3.2.1 Advanced Secure Release Anywhere workflow options

Setting	Description
Automatically Distribute Jobs	When checked, print jobs are automatically downloaded by all Print Delivery Stations linked to the Secure Release Anywhere pool.
	This option is useful when enabling a Secure Release Anywhere pool across multiple networks. It allows a copy of print jobs to be delivered to each network automatically, which decreases the time to complete the print. It also allows users to release their jobs in any network.
	Note that although enabling this option increases network bandwidth, PrinterOn attempts to minimize the impact by compressing data during delivery.
Delete Jobs From Hub After Printing	When checked, the Print Delivery Station informs the Hub when the job is printed, and deletes the job from the central storage. The job cannot be downloaded to other release stations after printing.
	If you want jobs to be accessible and reprintable at multiple locations when jobs are NOT being distributed automatically, disable this option.
Enable Hub Job Cleanup	When checked, the Print Delivery Hub automatically deletes print jobs that have not been released by users. If this option is not enabled, print jobs are never deleted.

Setting	Description
Cleanup Hub Jobs After	The length of time that jobs that have not been printed are held by the Print Delivery Hub. If jobs are not distributed automatically, this indicates how long the jobs remain available for users to release.
Enable Unreleased Job Cleanup	When checked, the Print Delivery Station automatically deletes print jobs that have not been released by users. If this option is not selected, print jobs are never deleted.
Cleanup Unreleased Jobs After	The length of time that jobs that have not been printed are held by the Print Delivery Station. This applies to all printers managed by the Print Delivery Station.
Cleanup Released Jobs After	The length of time (from the moment they were first printed) that printed jobs should be held by the Print Delivery Station.

4.4 Configuring Secure Release Anywhere release stations

A Secure Release Anywhere release station is a printer that has been configured to accept input from the user to pull a print job to that device.

> **Note:** A Secure Release Anywhere release station depends on communication with a Print Delivery Station to access and release print jobs.

PrinterOn's solution supports using a variety of release station interfaces to support a range of devices:

Release interface	Description
Web-based release	Many devices provide access to a web browser to allow users to pull their print job down to the device. The web release interface can be used by: • MFPs with integrated web browsers • Dedicated tablets • User phones or tablets • A Windows PC running a full Print Delivery Station To configure web-based release, you'll need to define the URL used to communicate with the PDS. For more information, see Formatting the Secure Release Anywhere URL for web-based release.

Release interface	Description
Samsung Smart UX printers and MFPs	Samsung Smart UX devices support web-based release. To improve the user experience, you can add a bookmark to the Secure Release Anywhere URL on the Home page.
	For more information, see Bookmarking the Secure Release Anywhere URL for Samsung Smart UX.
Ricoh MFPs	Ricoh MFPs support web-based release. However, because browser capabilities and screen sizes vary across devices, you might need to customize the URL. To improve the user experience, you can also add a link to the Secure Release Anywhere URL on the Home page.
	For more information, see Configuring the Ricoh device browser.
Brother BSI-enabled print devices	Brother BSI-enabled devices support web-based release. However, these devices require a custom URL to receive Brother-specific content, and must be configured to provide a method of quickly accessing the URL.
	For more information, Configuring a Brother BSI (local network) Secure Release Anywhere release station.
PrinterOn PrintValet	You can attach the PrinterOn PrintValet to transform single-function printers and MFPs with no keypad or touch screen into network-based secure release code terminals.
	To configure PrintValet, see the Network PrintValet Administration Guide.

4.4.1 Formatting the Secure Release Anywhere URL for web-based release

Using PrinterOn's Secure Release Anywhere solution, any device that includes a web browser can be used as a release station.

The Secure Release Anywhere Scheme is defined as follows:

```
http(s)://<PDS_IPAddress_or_DNS>:8181[/basic]/
    printerNumber=<PON_printer_number>&num=<rows>&lang=<lang_code>
```

By formatting the URL used to communicate with a Print Delivery Station you can:

- Customize the Secure Release Anywhere landing page to link directly to the User Login or Privacy Release page. For more information, see Displaying a custom Secure Release Anywhere landing page.

- Specify where a job should be released. Normally a release station is deployed near the printer or MFP. In many cases, MFPs include browsers installed within the firmware or device platform. Using the browser, these devices can be used as Secure Release Anywhere release stations. For more information, see Specifying output printer information.

- Use a basic web interface compatible with older browser technologies that cannot support the default modern and responsive release interface. For more information, see Displaying basic mode content for limited browsers

- Specify the number of job rows to be shown on the screen to support smaller touch panels. For more information, see Limiting the number of jobs displayed on small screens.

- Specify a default language when the page loads. For more information, see Specifying the display language.

4.4.1.1 Base URL Port and HTTP Scheme Information

The Secure Release Anywhere web release interface can be accessed using SSL or non-SSL. To enable non-SSL communication, disable the option under the Print Delivery Station Settings in the PrinterOn Configuration Manger.

If using SSL, by default, only port 8181 is SSL-enabled. The URL should be configured using https://. For example:

```
https://172.12.12.12:8181/
```

4.4.1.2 Displaying a custom Secure Release Anywhere landing page

By default, accessing the Secure Release Anywhere web page loads a page from which users can select whether to release jobs using a Privacy Release Code or by Authenticating. If you don't want users to have the option, you can link directly either the Privacy Release page or User Login page.

To access the Privacy Release page, add `/publicRelease.html` to the URL. For example:

```
https://172.12.12.12:8181/
    publicRelease.html?printerNumber=900123456789
```


> **Note:** For screens with limited display space, you can add **/publicReleaseBasic.html** to the URL to display a basic version of the page.

To access the User Login page, add `/userLogin.html` to the URL. For example:

```
https://172.12.12.12:8181/userLogin.html?printerNumber=900123456789
```


> **Note:** For screens with limited display space, you can add **/userLoginBasic.html** to the URL to display a basic version of the page.

4.4.1.3 Specifying output printer information

It is important to associate the Secure Release Anywhere web interface with the printer where jobs should be delivered. This is done by including the PrinterOn printer number in the request.

When specified, the Print Delivery Station will use this value to lookup the printer on the server and direct the job to the output destination configured.

To specify the output printer, add the `printerNumber` parameter to the URL and specify the PrinterOn printer number. For example:

```
https://172.12.12.12:8181/?printerNumber=900123456789
```

4.4.1.4 Displaying basic mode content for limited browsers

By default, the web release interface will use uses modern HTML technology including advanced CSS and JavaScript to provide an optimal experience. The server attempts to detect the capabilities of the browser to adapt the browser's capabilities.

In some browsers, it is not possible to use full CSS and JavaScript functionality. In these browsers, you can display a Basic version of the interface that disables most advanced JavaScript and CSS.

The display the basic version, add `/basic` to the URLs. For example:

```
https://172.12.12.12:8181/basic
```

4.4.1.5 Limiting the number of jobs displayed on small screens

In some browsers and panels where the size of the screen is limited, you may need to limit the number of print job rows that are displayed on the screen. In most cases, using a value of 2 (the default) is recommended.

> **Note:** This only applies when using the basic mode for the web interface.

You can specify the number of rows using the `num` parameter.

Because PrinterOn supports multiple workflows to allow users to list their print jobs (by entering their user credentials or by entering a release code), you'll need to add the parameter for each release workflow you intend to support:

- When the user is providing user credentials to access their print jobs:

  ```
  https://172.12.12.12:8181/basic/userLoginBasic.html
          ?printerNumber=900123456789&num=4
  ```

- When the user is entering a release code to their print jobs:

  ```
  https://172.12.12.12:8181/basic/publicReleaseBasic.html
          ?printerNumber=900123456789&num=4
  ```

4.4.1.6 Specifying the display language

By default, the Secure Release Anywhere web page will provide users with options to select their desired language. In some cases, it may be desirable to specify the language to show when loading the page.

You can specify the language using the `lang` parameter and supplying the language code. For example:

```
https://172.12.12.12:8181/?printerNumber=900123456789&lang=en_US
```

Supported languages include:

Language	Code	Language	Code
English	en_us	Brazilian Portuguese	pt_br
French	fr_fr	Danish	da_dk
German	de_de	Korea	ko_kr
Dutch	nl_nl	Japanese	ja_jp
Italian	it_it	Simplified Chinese	zh_zn
Spanish	es_es	Traditional Chinese	zh_tw

4.4.2 Bookmarking the Secure Release Anywhere URL for Samsung Smart UX

Every Samsung printer or MFP that includes the Samsung Smart UX can configured to act as a Secure Release Anywhere release station. Smart UX includes a browser from which users can access the Secure Release Anywhere URL.

To simplify the pull process for users, you can create a bookmark for the URL and add it to the Home page, so that it is easily accessible.

To add a bookmark to the Secure Release Anywhere URL to the Home Screen:

1. On the Smart UX panel, launch the browser.

2. Navigate to the PrinterOn Secure Release Anywhere URL:

   ```
   http(s)://<PDS_IPaddress_or_DNS>:8181?printerNumber=<900123456789>
   ```

3. Create a bookmark for the URL by clicking ☆.

4. In the **Bookmark this Page** dialog, validate that the connection and printer information is correct.

5. Tap the **Add To** menu, then select **Home Screen**.
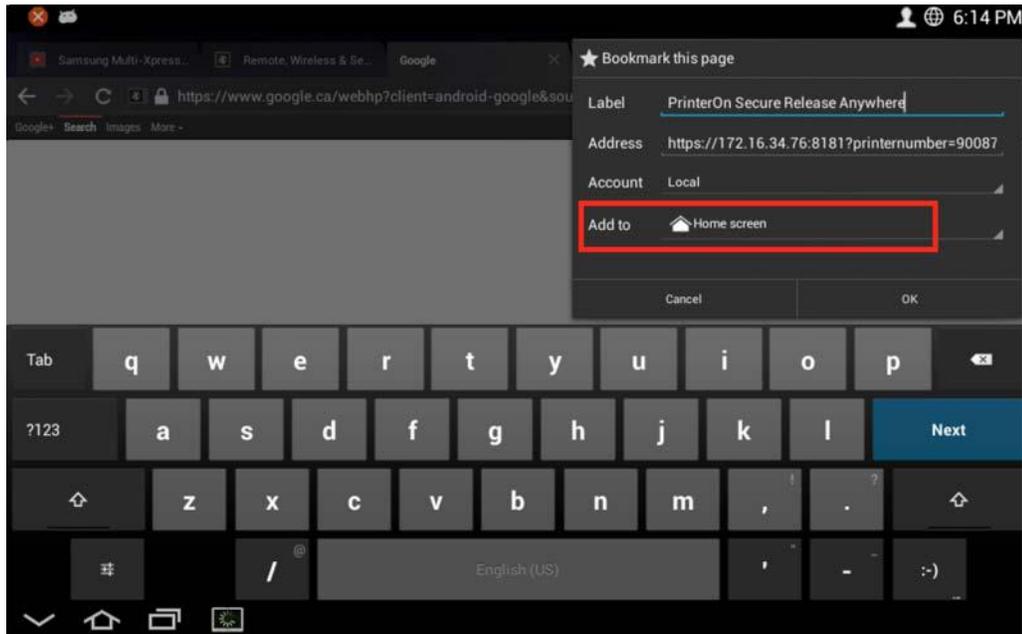
4.4.3 Configuring the Ricoh device browser

Every Ricoh MFP configured with a browser can act as a Secure Release Anywhere release station. Users can access the Secure Release Anywhere URL from the browser to release their print job to the device.

Because some Ricoh browsers are limited, or displayed on small screens, you might need to modify the URL so that the PDS sends device-appropriate content.

To simplify the process for users, you can create a link the URL and add it to the device Home page, so that it is easily accessible.

Note: The Ricoh device browser MUST be installed to support Secure Release Anywhere.

4.4.3.1 Configuring the Secure Release Anywhere URL

To configure the Secure Release Anywhere URL:

1. At the MFP, select **User Tools**.
2. Select **Browser Settings**.

   > **Note:** On some devices, you might need to select **Extended Feature Settings** >
   > **Browser Settings**.

3. Select **Browser Default Settings**.
4. Select **Bookmarks** or **Favorites**.

   > **Note:** If required, select **Common Favorites**.

5. Select **New Program**.
6. Create a new URL using one of the following formats:

Browser/screen size	URL
Full feature browser, 10" panel	`http(s)://<IPaddressOrDNS>:8181/` `        ?printerNumber=<900123456789>`

Basic browser	For browsers versions that do not support CSS or JavaScript, point to the basic Secure Release Anywhere page:
	
	`http(s)://<IPaddressOrDNS>:8181/basic/`
	`        ?printerNumber=<900123456789>`

Small panels, such as 4" touch panels	Use the **num** parameter to set the number of rows to **2**. This will Limit the number of jobs shown when selecting a job and reduce scrolling
	
	`http(s)://<IPaddressOrDNS>:8181/basic/`
	`        ?printerNumber=<900123456789>&num=2`

7. Save the URL.

4.4.3.2 Setting a Link on the Ricoh Home Screen

After creating a URL on the device, it is possible to create a link on the Home Screen of the MFP for users to quickly access the page.

1. Select **User Tools**.
2. Select **Edit Home**.

3. Select **Add Icon,** then **Select Icon to Add**.

4. Select **URL**, then select the newly created URL and the location to save the icon.

Users can now quickly access the URL from the Home Screen.

4.4.4 Configuring a Brother BSI (local network) Secure Release Anywhere release station

The PrinterOn Secure Release Anywhere feature supports Brother BSI by default. However, Brother BSI-enabled devices require a unique URL to communicate with the Print Delivery Station.

> **Note:** The Brother BSI Secure Release Anywhere integration only supports PrinterOn Secure Release Codes.

4.4.4.1 Creating the Brother BSI service URL

The Print Delivery Station provides access for the BSI workflow using a custom path and port:

- The PDS stores the Brother BSI-specific content in the **/bsi** folder.
- The PDS listens for Brother BSI requests on port 8182.

You must also specify the Printer Number of the destination printer, configured specifically for the Brother device, in the URL.

> **Note:** Ensure that you specify the number of the destination printer, not the Printer Number of the Secure Release Anywhere printer pool.

For example:

```
http(s)://<adAddress>:8182/
    bsi?type=pull&pid=<outputPONPrinterNumber>
```

4.4.4.2 Using Brother BSI devices with self-signed certificates

By default, a Print Delivery Station is configured to accept SSL communication only, and provides a self-signed certificate. However, Brother BSI-enabled devices only communicate with a self-signed certificate if the certificate is loaded into the printer/MFP.

There are three workarounds to this issue:

- Purchase and install a valid certificate.
- Upload the self-signed certificate into the printer/MFP.
- Disable SSL for BSI in the Print Delivery Station settings.

4.4.4.3 Configuring the Brother BSI for Secure Release Anywhere

To configure the Brother BSI device to access the Secure Release Anywhere URL:

1. Using a web browser, navigate to the Brother printer admin web page. For example:

    `http://<ipAddress>`

2. Log in to the Brother device as an administrator.

3. Click on **Administration Settings** or **Administrator**.

4. Select **Solution Settings** > **Solutions Application Entry**.

5. Select the **Menu Item** that you want to configure.

6. In the **Display Name** field, enter the name that users will see on the device.

7. In the **URL** field, enter the address of the Print Delivery Station managing the printer. For example:

    `http(s)://172.16.23.32:8182/bsi?type=pull&pid=900123456789`

8. Click **Submit** to save the changes.

5

Configuring workflows

The PrinterOn server allows users to print in a variety of ways, from a variety of devices. For example, users can submit print jobs using the PrinterOn Mobile App, or by emailing the print server directly. The **Workflows** tab lets you edit workflow-specific settings.

To configure workflows:
1. In the Configuration Manager, click **Workflows**. The Workflows tab appears.
2. Select the workflow you want to configure.

Workflow	Description
Web Print	Allows users to upload documents to the Web Print portal.
Mobile Print	Allows users submit jobs using one of PrinterOn's mobile client apps.
Email Print	Allows users email documents as printable attachments directly to a PrinterOn printer.
Google Cloud Print	Allows users submit print jobs via the Google Cloud.
PrinterOn Queue Management System (PQMS)	Allows users print to Windows print queues that are mapped to PrinterOn printers.

Workflow	Description
IPP and Native iOS printing	Allows users print using either IPP printers that are mapped to PrinterOn printers, or using iOS/macOS native printing.
Secure Release Anywhere	Allows users print to a pool of printers and pull their print job down to any printer that is a member of the pool. To use this workflow, you must also configure one or more Secure Release Anywhere printer pools.

5.1 Configuring the Web Print workflow

The PrinterOn Server lets users submit print jobs using any connected web browser. Users upload their documents to the Web Print portal and can choose the printer to which to submit the job.

The Web Presentation settings let you customize the Web Print Workflow.

To configure the Web Print workflow:

1. In the Configuration Manager, click **Workflows** > **Web Print**.

2. Configure your Web Presentation settings as necessary.

3. Click **Apply Settings**.

5.1.0.1 Web Presentation settings

Setting	Description
Open Print Page	Provides a link to the Web Print portal. The default value is: http://127.0.0.1/cps. You can modify this URL to display the DNS name or the IP address of the PrinterOn Server. This is configured in the PrinterOn web admin portal at www.printeron.com/administrators. For more information, see Updating the Service URL. This link is provided as a shortcut for the PrinterOn administrators; however, end users can still access the Web Print portal regardless of this configuration option.
Enable New Web Print UI	When checked, the Web Print portal displays PrinterOn's updated Web Print portal User Interface. This UI offers an improved end-user experience, with fewer steps in the printing workflow, allows users to submit multiple documents at once, and displays a jobs list so users can monitor the print status of each submitted job. For more information on using the new Web Print interface, see Enabling and using the new PrinterOn Web Print UI. By default, the updated UI is disabled, and users will view the older UI if they launch the Web Print portal.
Enable Web Print	When checked, the Web Print portal is accessible to all users. Disabling this feature disables the Web Print portal for all users. By default, this option is disabled. **Note:** You can also disable Web Print for individual printers, so that the printer is not listed among the available printers when users submit a print job through the Web Print portal. For more information, see Configuring printer-specific workflow options.
Languages	Specifies a list of the languages in which the Web Print portal can be displayed. The server can display the page in the following languages: English, French, Spanish, Italian, German, Dutch, Danish, Portuguese, Simplified Chinese, Traditional Chinese, Japanese, or Korean. By default, English is the only language in the list. You can modify the languages included in the list by clicking **Manage Languages** and adding or removing them as necessary. When more than one language is enabled, the user can choose in which language to display the page.

Setting	Description
Job Submit Refresh Interval (*Advanced view* only)	Specifies the how often, in seconds, that the Web Print portal updates the status of a submitted print job. By default, the status of submitted jobs is refreshed every two seconds.
Job Approval (*Advanced view* only)	When checked, the user must confirm the print job before the Web Print portal sends it to the printer. By default, this option is disabled.
Smart Printer Selection (*Advanced view* only)	When checked, the Web Print portal skips the printer selection page if the user only has a single printer available. By default, the user is prompted with a page to select their printer. By default, this option is disabled.
Department Sidebar View (*Advanced view* only)	When checked, the Web Print portal displays the department selection side bar, which allows users to filter which printers are displayed by selecting one or more departments. By default, this option is disabled.
Number of Printers Displayed Per Page (*Advanced view* only)	Specifies how many printers are displayed per page. By default, ten printers are displayed per page.
Number of Departments Displayed Per Page (*Advanced view* only)	Specifies how many departments are displayed per page in the Department sidebar. By default, ten departments are displayed per page.

5.2 Configuring the Mobile Print workflow

The Mobile Print workflow lets users locate and print to the PrinterOn service using the PrinterOn Mobile App on their smartphone or tablet.

The PrinterOn Server supports mobile apps developed for iOS and Android. To allow these apps to communicate with the PrinterOn Server, you must define the Service URI, also called the Document API URI. This URI is the IP address that the apps use to communicate with your PrinterOn installation. Once this address is configured, Mobile Apps will be able

to both search for printers and independently submit print jobs.
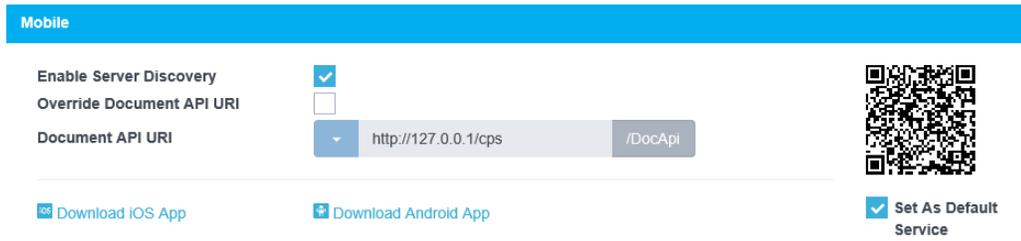
To configure the Mobile print workflow:

1. In the Configuration Manager, click **Workflows** > **Mobile**.

2. Check **Override Document API URI**.

    The Document API URI is the URL that the app uses to submit documents to the server.

3. Click the **Document API URI** drop-down and select the address provided. This address is determined automatically by the software based on your server's IP address and should always be concluded with /cps.

4. Click **Apply Settings**.

5.2.0.1 Mobile print settings

Setting	Description
Enable Server Discovery	The PrinterOn Server can be used to broadcast itself as well as its printers. When enabled, this option allows the PrinterOn Mobile Apps to locate the PrinterOn Server automatically on the network.
	This option is useful if printers are organized in different servers on the network, and you would like to limit access to certain services.
	By default, this option is disabled.
Override Document API URI	When checked, the Document API URI is the URL returned by the server to the Mobile Apps when searching for printers. It is used by the App to submit documents to the server.
	By enabling this option, you can provide a value in the **Document API URI**.
	By default, this option is disabled.

Setting	Description
Document API URI	An alternative Document API URI that is used when you enable the **Override Document API URI** setting. This value overrides the value configured on the PrinterOn Directory.
	Set the value in one of the following ways:
	• Select the address from the drop-down. The software determines this value automatically, based on the IP address of your server.
	• Manually enter an address. When entering an address manually, you must add /cps to the end of the URL.

5.3 Configuring the Email Print workflow

When you add a new printer to your PrinterOn service, the PrinterOn server automatically assigns the printer an email address. Users can email the printer directly to print email messages or attachments.

To configure your server to accept email print jobs, you will need to configure some settings for your mail service.

When configuring your mail service it is important to know prior to configuring what method your service will use to connect to the mail server. The PrinterOn Server supports the following email systems:

• Microsoft Exchange Web Services (EWS)

• IMAP4 mail protocol

• Lotus Notes/Domino API

The PrinterOn Enterprise Server uses the standard SMTP protocol for sending emails for EWS and IMAP4 installations.

Note: For information on incorporating email printing into your existing mail system deployment, see Configuring your mail server for PrinterOn email printing.

To configure your email print workflow:

1. In the Configuration Manager, click **Workflows** > **Email Print**.

2. To configure your inbound service settings, choose the **Email Type** used by your organization.

The configuration panel for the selected service appears, allowing you to set service-specific settings:

- Exchange Web Services (EWS)

- IMAP4

- Domino (Available for Enterprise Edition only)

3. If you configured the server to use EWS or IMAP4, configure the SMTP settings used for outbound messages.

4. Configure any advanced email print settings, if necessary. For example, you can set the minimum size for an attachment, or auto-detect forwarded messages.

   Note: The **Advanced Email Settings** panel is displayed in Advanced view only.

5. Click **Apply Settings**.

5.3.1 Configuring Exchange Web Services (EWS) settings

Selecting **EWS** as your **Email Type** displays the EWS Configuration and OAuth Configuration settings:

EWS Configuration	
Service URI	https://outlook.office365.com/EWS/Exchange.asmx
Mailbox Username	devpon@ponpp.onmicrosoft.com
Mailbox Password	••••••••
Listener Port	80
Response Address	no-reply@dev.printspots.com
Accept Request to response address ❓	☑
Enable SMTP ❓	☐
Test	

OAuth Configuration	
Enable OAuth	☑
Type	ClientCertific ⌄
Client ID	
Scope	https://outlook.office365.com/.default
CertificateSubject	
StoreName	AddressBook ⌄
StoreLocation	CurrentUser ⌄
Tenant ID	

Microsoft's Exchange Web Services supports both MS Exchange server hosted internally and Office 365 cloud-based email services.

Configuration settings are divided into to sections:

- EWS Configuration settings: Configures the connection settings for the mail service.
- OAuth Configuration settings: Configures the connection settings for the OAuth authentication service, which can be used in conjunction with Office 365 cloud-based email services.

5.3.1.1 EWS Configuration settings

Setting	Description
Service URI	The EWS server's IP address or hostname. The URI depends on which service you're using: • Office 365 mail services: https://outlook.office365.com/EWS/Exchange.asmx • MS Exchange mail service: https://*Your_Exchange_Server*/EWS/Exchange.asmx
Mailbox Username	The username used to connect to the Exchange server and to monitor the incoming mailbox. This account could also be the same account used to install and run the PrinterOn server services. **Note:** If you're using Office 365, the value must be the complete email address.
Mailbox Password	The password used to connect to the EWS server and monitor the incoming mailbox.
Listener Port	The port the PrinterOn Server uses when communicating with the EWS server. The default is port 80.
Response Address	The email address used by the mail server when responding to email requests. When an email is sent to the default address, the PrinterOn server will automatically delete the message and not respond to the user. Typically this should be set to an address such as: no-reply@print.company.com
Accept requests to response address (*Advanced view* only)	When enabled, this option causes the PrinterOn Server to respond to requests sent to this address. By default all emails sent to the response address are automatically deleted. This option is generally only used for diagnostic purposes.
Test	Clicking **Test** checks the configured settings to ensure that the PrinterOn Server can successfully connect to and communicate with the EWS server.

5.3.1.2 OAuth Configuration settings

If you are using Office 365 cloud-based email services with an OAuth-based Identity Management service (that is, Microsoft Azure AD) to authenticate users, you'll need to provide connection information for your OAuth service.

> **Note:** If you are enabling OAuth authentication for your EWS service, you must first register your EWS service with Azure AD and define the level of access to the EWS service the user has once authenticated. For more information, see Registering your EWS mail client with Azure AD.

Once you have registered your EWS service with Azure AD, you can configure the OAuth Configuration settings.

Setting	Description
Enable OAuth	When enabled, this option indicates that the EWS service uses OAuth-based authentication. Once enabled, the following options appear.
Type	The OAuth grant type used to request an access token on behalf of the user. Three grant types are available. The remaining OAuth Configuration settings will vary, depending on which of the following grant types you select. • **ClientSecret:** The EWS server requires a shared secret, specified in the **Client Secret** field, and application permissions to receive access tokens. • **ClientCertificate**: The EWS server requires a valid certificate and application permissions to receive access tokens. • **ROPCFlow**: The EWS server requires a specified credential and delegated permissions to receive access tokens.
Client ID	Required for all grant types. The unique ID of your EWS service, generated when you registered the service with Azure AD. For more information on registering your client app, see Registering your EWS mail client with Azure AD. The EWS service requires this value to authenticate with Azure AD.
Scope	Required for all grant types. Specifies the scope
ClientSecret	This field appears only when **Type** is set to **ClientSecret**, and enables you to specify the secret generated when you registered the EWS server in Azure AD.
Certificate Subject	This field appears only when **Type** is set to **ClientCertificate**. It specifies the name of the Distinguish Name of the certificate being used with the PrinterOn service.

Setting	Description
StoreName	This field appears only when **Type** is set to **ClientCertificate**, and specifies the name of the X.509 certificate store to open. You can choose between the following: • **AddressBook**: The X.509 certificate store for other users. • **AuthRoot**: The X.509 certificate store for third-party certificate authorities (CAs). • **CertificateAuthority**: The X.509 certificate store for intermediate certificate authorities (CAs). • **Disallowed**: The X.509 certificate store for revoked certificates. • **My**: The X.509 certificate store for personal certificates. • **Root**: The X.509 certificate store for trusted root certificate authorities (CAs). • **TrustedPeople**: The X.509 certificate store for directly trusted people and resources. • **TrustedPublisher**: The X.509 certificate store for directly trusted publishers.
StoreLocation	This field appears only when **Type** is set to **ClientCertificate**, and specifies the location of the X.509 certificate store. You can choose between the following: • **CurrentUser**: The X.509 certificate store used by the current user. • **LocalMachine**: The X.509 certificate store assigned to the local machine.
ROPCFlowType	This drop-down appears only when Type is set to ROPC, and lets you specify whether the server will use the **Tenant ID,** or the **OAuthAuthority** as the credential used to retrieve the access token.
Tenant ID	The Tenant ID of the EWS server in Azure AD. This value should be copied from the **Directory (tenant) ID** field when you register the EWS server. This value needs to be passed to Azure AD along with a Client Secret or Certificate in order to retrieve Access tokens. When **ROPCFlowType** is set to **Tenant ID**, this value alone is used to retrieve Access tokens.
Authority	This field appears only when **ROPCFlowType** is set to **OAuthAuthority**, and allows you to specify the URL of the Security Token Service (STS) from which the EWS will acquire the access tokens.
ADFS Authority	This field appears only when **ROPCFlowType** is set to **OAuthADFSAuthority**, and allows you to specify the Authority of the ADFS server as the identifier.

5.3.2 Configuring IMAP4 settings

Selecting **IMAP4** as your **Email Type** displays the IMAP4 Configuration settings:

IMAP4 Configuration

Server Address	127.0.0.1
Server Port	143
SSL/TLS	None ☑ Strict SSL ☐
Username	username
Password	
Response Address	no-reply@print.company.com
Accept Request to response address ⍰	☐
Enable Polling	☐

Test

5.3.2.1 IMAP4 Configuration settings

Setting	Description
Server Address	The IMAP4 server's IP address or hostname.
Server Port	The port on which the PrinterOn Server should connect when communicating with the IMAP4 server. Default ports are: • Non-SSL default port: 143 • SSL default port: 993
SSL/TLS	The type of SSL used when communicating with the IMAP4 server. Select from one of three options for SSL. You may need to contact your server administrator to identify the type of SSL used by your server. The configuration automatically adjusts the SMTP port based on the most commonly used ports. • **None**: SSL will not be used for this server. • **Implicit SSL**: Typically used with port 993, this type of SSL is often referred to as IMAP-over SSL. • **Explicit SSL**: Typically used with port 143, this type of SSL is often referred to as IMAP-TLS.

Setting	Description
Strict SSL	When enabled, the service only connects to services when the SSL certificate is valid and signed by a valid certificate authority. If your service is configured for SSL but is using a self-signed certificate, disable this option. **Note:** To ensure the security of your system, PrinterOn recommends that you use a valid certificate from a certificate authority.
Username	The username used to connect to the IMAP4 server and monitor the incoming mailbox.
Password	The password used to connect to the IMAP4 server and monitor the incoming mailbox.
Response Address	The email address used by the mail server when responding to email requests. When an email is sent to the default address, the PrinterOn server will automatically delete the message and not respond to the user. Typically this should be set to an address such as: no-reply@print.company.com
Accept requests to response address (*Advanced view* only)	When enabled, this option causes the PrinterOn Server to respond to requests sent to this address. By default all emails sent to the response address are automatically deleted. This option is generally only used for diagnostic purposes.
Test	Clicking **Test** checks the configured settings to ensure that the PrinterOn server can successfully connect to and communicate with the IMAP4 server.

5.3.3 Configuring Domino settings (Enterprise Edition only)

Selecting **Domino** as your **Email Type** displays the Domino Configuration settings:

To use Lotus Domino with the PrinterOn Server, you must:

- Have a licensed version of PrinterOn Enterprise installed.
- Install the Lotus Notes client on the PrinterOn Server as a Single-User installation. A Single-User installation lets the PrinterOn Server access the Notes executable files and the Domino data files.
- Launch the Lotus Notes client and validate that the server can connect to the user's mailbox.

5.3.3.1 Domino Configuration settings

Setting	Description
Server Address	The Lotus Domino server's IP address or DNS name. This information is used by the Domino address book look-up feature to fetch the SMTP address of the recipient.
Password	The mailbox account password information used to connect to the Lotus Domino server and monitor the incoming mailbox.
Response Address	The email address used by the mail server when responding to email requests. When an email is sent to the default address, the PrinterOn server will automatically delete the message and not respond to the user.
	Typically this should be set to an address such as:
	no-reply@print.company.com
Accept requests to response address *(Advanced view only)*	When enabled, this option causes the PrinterOn Server to respond to requests sent to this address. By default all emails sent to the response address are automatically deleted.
	This option is generally only used for diagnostic purposes.
Printer Name	Optional. When specified, this setting defines the destination PrinterOn printer name for all the incoming requests. If the value is not set, the server will use the Domino Address Book Look-up feature to fetch the SMTP address of the recipient.

Setting	Description
Lotus Notes INI Path	The Lotus Notes (Notes.ini) configuration file path. This file can usually be found in the following location: 　　C:\Program Files(x86)\IBM\Lotus\Notes Clicking the Browse button should launch the appropriate directory location where this configuration file can be found. **Note:** Depending on which version of Lotus Notes you're using, you may need to specify the filename in the path as well. For example: 　　C:\Program Files(x86)\IBM\Lotus\Notes\Notes.ini
Synchronize	Clicking **Synchronize** registers the PrintAnywhere application with the IBM Lotus Notes client software to start monitoring the mailbox. It also reconfigures the PrintAnywhere server to use the appropriate (32-bit) version of the PrinterOn server binaries to interface with the Lotus Notes client software.

5.3.4 Configuring the SMTP Server for outbound messages

When you select **EWS** or **IMAP4** as your **Email Type**, the PrinterOn Server uses SMTP to send messages to users about their print job.

SMTP Server Configuration (Outbound)

Server Address	127.0.0.1
Server Port	25
SSL/TLS	None ▾　　Strict SSL ☐
Username	
Password	
Sender Name	Mobile Print
Sender Address	no-reply@print.company.com
Reply to Address	no-reply@print.company.com

Test

When a print job is submitted via email, the PrinterOn Server sends emails to the initiating end user about the status of the print job, for example, notifying them of issues, or advising that the print job was completed and can be picked up at the printer. To send these emails, you must configure the PrinterOn Server so that it can connect to the mail server using the SMTP information entered into the SMTP configuration page for each

email protocol. Without this information, the user will not receive a response email advising if there are any errors while trying to submit a document to be printed.

5.3.4.1 SMTP Server Configuration (Outbound) settings

Setting	Description
Server Address	The SMTP server's IP address or hostname.
Port	The port the PrinterOn server uses when communicating with the SMTP server. The default SMTP port is 25.
SSL/TLS	The type of SSL used when communicating with the mail server. Select from one of three options for SSL. You may need to contact your server administrator to identify the type of SSL used by your server. The configuration will automatically adjust the SMTP port based on the most commonly use ports. • **None**: SSL will not be used for this server. • **Implicit SSL**: Typically used with port 993, this type of SSL is often referred to as IMAP-over SSL. • **Explicit SSL**: Typically used with port 143, this type of SSL is often referred to as IMAP-TLS. To only connect to services when the SSL certificate is valid and signed by a valid certificate authority, enable **Strict SSL**. If your service is configured for SSL but is using a self-signed certificate, disable this option.
Username	The username used to connect to the mail server and monitor the incoming mailbox.
Password	The password used to connect to the mail server and monitor the incoming mailbox.
Sender Name	The name of the sender shown in email responses sent from the server.
Sender Address	The sender address used when responding to the user. This is typically the same as the "Default Address" configured under the incoming mail server settings.
Reply to Address	The reply-to address to set when responding to the user. This is typically the same as the "Default Address" configured under the incoming mail server settings.
Test	Clicking **Test** checks the configured settings to ensure that the PrinterOn Server can successfully connect to and communicate with the SMTP server.

5.3.5 Configuring the Advanced Email Settings

The Advanced Email Settings let you configure some additional options for email print jobs.

Note: The **Advanced Email Settings** panel is displayed in Advanced view only.

5.3.5.1 Advanced Email settings

Setting	Description
Min. Attachment File Size	The threshold at which the PrinterOn Server processes or ignores attachments. This setting is useful when dealing with some attachments that are included as part of signatures of emails.
Ignore Empty HTML Attachments	When enabled, the PrinterOn Server attempts to detect when an email contains HTML-based attachments that contain no visible content. The server attempts to read the attachment and ignores the file if it detects an empty file, or no values between the HTML tags.
ZIP Archive Support	When enabled, the PrinterOn Server processes ZIP files attached to email messages. PrintAnywhere extracts the contents of the ZIP file and processes each file individually.
Ignore Requests To Invalid Printers	When enabled, the PrinterOn Server doesn't respond to requests submitted to unknown email accounts. The user is not notified that the destination printer address is invalid and the email is silently ignored.
Auto Detect Forwarded Messages	When enabled, the PrinterOn Server attempts to detect when a message has been forwarded from a client. The client may wrap the original email message in an embedded message before forwarding it to the server. Generally this option should be left enabled unless you encounter a specific issue with your mail server.

5.4 Configuring the Google Cloud Print workflow

PrinterOn allows users to print from any Google Cloud Print client applications to a PrinterOn printer.

The PrinterOn Connector for Google Cloud Print (GCP) is an extension to the Print Delivery Gateway component of the PrinterOn Server that allows users to print seamlessly from any of the GCP Client Applications to PrinterOn printers.

The GCP Connector helps bridge the gap between the existing Google Cloud Print workflows and the PrinterOn Server. Once the connector is configured, users can submit jobs to PrinterOn printers from Google clients such as ChromeOS or Chrome Browser.

The PrinterOn Server with the GCP connector greatly simplifies printing management in environments where users bring their own devices—smartphones, tablets, Chromebooks, and Notebooks—that do not connect exclusively to existing print infrastructure.

This unique approach extends the following advanced capabilities for jobs submitted through the Google Cloud Print workflows:

- LDAP/Active Directory or SSO Authentication
- User-based Access Control
- Print Management Integrations
- Guest Print Workflows

Note: As you add and configure your Google Cloud printers, you will be redirected to the Google Cloud Print website to enter your credentials and provide the PrinterOn Server access to your Google printers. Before continuing, see Google Cloud Print authentication to learn how to ensure that you are prepared to add Google Cloud Printers.

To configure the Google Cloud Print workflow:

1. In the Configuration Manager, click **Workflows** > **Google Cloud Print**.
2. Add your Google Cloud printers by providing a printer name and mapping it to an existing PrinterOn printer.
3. Configure the general settings for the printer.
4. Share the printer to make it available to Google Cloud users.
5. To rename a printer queue, select the printer in the list then click **Rename**.
6. To delete a printer queue from both the PrinterOn Server and the Google Cloud Printer services, click **Delete Printer**.
7. Click **Apply Settings**.

5.4.1 Google Cloud Print authentication

The PrinterOn Server uses Google's OAuth2 based system for identifying users and printers. This provides a secure method of linking Google printers and users to PrinterOn. During the setup process, you will be redirected to the Google Cloud Print website to enter your credentials and provide the PrinterOn Server access to your Google printers.

Before starting your Google Cloud Print setup:

- Create a Google Account to manage your printers and Google Cloud Print workflow.

- Ensure that pop-up windows are allowed for the PrinterOn Server.

  During the setup process, the Configuration Manager will load a pop-up window or tab and redirect you to the Google website.

5.4.2 Adding a Google Cloud printer

To add a Google Cloud Printer to your PrinterOn solution, you must create a map that links a Google printer to a PrinterOn printer

To map a Google Cloud Printer to a PrinterOn printer:

1. On the Google Cloud Print screen, click **Add Google Printer**. The Add Google Printer dialog appears.

2. Set the following values:

Setting	Description
Printer Name	The user-friendly Google Cloud Print printer name that will be assigned to this printer.
Map to Printer	The PrinterOn printer that was previously created in the Configuration Manager.

3. Click **Add Google Printer** to create the printer on the Google Cloud Print servers. The printer is added to the Google Cloud Print Printers list.

5.4.3 Configuring Google Cloud Print general settings

Once you add a new Google Cloud printer, you can configure some general print settings for it.

Setting	Description
Proxy (Identifier)	The Google Service identifier that uniquely identifies the instance of the PrinterOn server. The Google Cloud Print service allows a printer proxy (PrinterOn server GCP Connector) to register more than one physical/virtual printer. If the printers linked to the Google Cloud Account do not have an associated proxy-identifier value, then the PrinterOn server Application auto-generates a new value.
Fetch Jobs Interval	How often the PrinterOn Server restarts the connection with Google to receive new print jobs. The PrinterOn Server registers for notifications from Google regarding new print jobs. In some cases, this connection may become unstable or unresponsive. This value allows the software to adapt to various network types.

5.4.4 Sharing a Google Cloud printer

Once the Google Cloud Printer has been added, you must then share the printer so that users can see the printer in the GCP client. You can share the printer with individual users or groups of users, provided the users all have access to a GCP client.

To share a Google Cloud printer:

1. In the Select column of the Google Cloud Print screen, check the printer you would like to share.

2. Click **Share Printer**.

3. In the Share Printer dialog, select **Yes** to be redirected to the Google Cloud Print site.
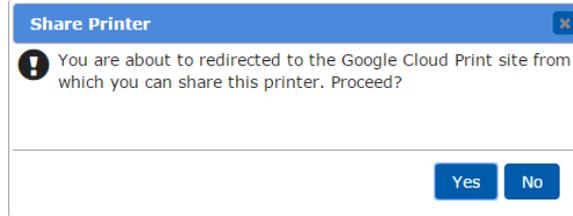
4. Log in to the Google Cloud Print services and share the printer.

5.5 Configuring the PrinterOn Queue Management System (PQMS) workflow

The PrinterOn Print Queue Monitoring Service Connector is an extension to the Print Delivery Gateway component of the PrinterOn Server that enables jobs submitted to the standard Windows Print Server queues to be delivered to remote printers through the PrinterOn Server infrastructure.

> **Note:** PQMS is only available for PrinterOn Enterprise edition.

To configure the PQMS workflow:

1. In the Configuration Manager, click **Workflows** > **PQMS**.

2. Configure your PQMS settings as necessary (Advanced view only). In most cases, you should not need to change the default settings.

3. Map the local Windows printer queue to a PrinterOn printer. The PQMS integration supports the following printer mapping configuration types:

   • One-to-One: Each printer device queue can be mapped to a unique PrinterOn printer

   • Many-to-One: Multiple printer device queues can be mapped to the same PrinterOn printer.

   To map a print queue:

   a) Select the local printer queue that will be routed through the PrinterOn server.

   b) Select a PrinterOn Printer from the list.

4. Click **Apply Settings**.

5.5.1 Configuring the PQMS connector

The PDG PQMS Connector helps bridge the gap between the existing Windows Print Queue workflows and the PrinterOn Server. It allows print users to submit jobs using standard Windows workflows (for example, using **File** > **Print**) and leverage the capabilities of the PrinterOn Server to deliver the pre-rendered data content to printers located anywhere in the world.

> **Note:** The **PQMS Settings** panel is displayed in Advanced view only.

PQMS Settings

Folder to Monitor	C:\ProgramData\PrinterOn Corporation\PDG\gateway\printjobwatch
Max Concurrent Jobs	10
Retry Failed Job Attempts	3
Job Processing Timeout	5 Minutes
Enable Monitor Logging	☐

5.5.1.1 PQMS Settings

Setting	Description
Folder to Monitor	The directory in which the PrinterOn Server stores print data.
Max Concurrent Jobs	The maximum number of print jobs that can be processed by the PrinterOn Server at any given time. This setting helps avoid overloading the PrinterOn Server and reduces job delays during periods of heavy usage. If you are using multiple servers, you can increase this value.
Retry Failed Job Attempts	The maximum number of job retries per print job before abandoning the request. The default number of retries is 3.
Job Processing Timeout	The maximum amount of time the PQMS connector waits for confirmation after job submission before abandoning the job request and freeing up the print slot. The default timeout is 5 minutes.
Enable Monitor Logging	When enabled, the PQMS Connector creates a new log file in the PDG Log Directory and starts logging information pertaining to PQMS integration.

5.5.2 Mapping the Windows Print Queue to a PrinterOn printer

The Printer Mappings section lets you map the existing Local Windows Print Queues to PrinterOn printers.

Printer Mappings

Local Printer Name	PrinterOn Printer
PrintWhere 5.2	
Microsoft XPS Document Writer	

To map a Windows print queue to a PrinterOn printer, select the PrinterOn printer from the drop-down.

5.6 Configuring IPP and native iOS/macOS workflows

The Internet Printing Protocol is a protocol designed to allow devices to connect to printers without the device needing to be on the same LAN as the printer.

The PrinterOn Server includes an IPP connector that allows administrators to deliver print jobs generated by third-party IPP print servers and clients to designated printers located in remote locations.

Native iOS/macOS printing is identical to IPP printing (it uses the IPP protocol), but includes a discovery service. The discovery service allows devices that support AirPrint to scan the network for available printers to populate the printer list. To support native iOS/macOS printing, the PrinterOn Server must be configured to broadcast the printer information so that these devices can find and connect to the printers.

You can configure:

- native iOS/macOS printing
- IPP printing

5.6.1 Configuring native iOS/macOS printing

You can configure the PrinterOn Server to let iOS- and macOS-based devices discover printers and submit print jobs to PrinterOn printers. It allows users to submit jobs to printers that are located both inside and outside the enterprise network.

This approach extends the following advanced capabilities for jobs submitted through the Native iOS Print workflow:

- SSO Authentication
- User-based Access Control
- Print Management Integrations
- Guest Print Workflows
- Enabling Printing from Multiple Networks

Note: To enable Native iOS Printing for a specific PrinterOn printer, you must first enable discovery for that printer. To enable the printer discovery setting:

1. Navigate to the **Printers** tab.
2. Locate the printer in the printers list.
3. In the **Discovery** column, click the X.
4. Select **Synchronize** to save the settings and update all components within the PrinterOn server.

To configure the Native iOS printing workflow:

1. In the Configuration Manager, click **Workflows** > **IPP and Native iOS Printing**.
2. Configure the Network and Broadcast Settings as necessary.

3. Click **Apply Settings**.

5.6.1.1 Network and Broadcast Settings

Setting	Description
Service URI	The address iOS/macOS devices will use to retrieve the list of PrinterOn printers with discovery enabled. The Service URI should be the following value: *<PrinterOn_Server_IP>*/cps Click **Test Connection** to verify that the URI is properly defined.
Broadcast Interface	The network interface to use for advertising printer information. If multiple network cards or interfaces are available on the server, such as when using a Virtual Machine, select the interface that is mapped to the same network as your mobile devices. When using a virtual machine, it is important that this is the externally visible network adaptor. The IP address used by each interface is displayed in the drop-down list to help you identify the appropriate interface.
Default IPP Port	The default port on which the IPP Listener service listens for print jobs from iOS devices. The default port is **6310**. • To enable the port, check **Enable**. • To transfer the print data securely, check **SSL**. This setting is checked by default for the Default IPP Port.
Additional Port 1, Additional Port 2 *(Advanced view only)*	Additional ports on which the IPP Listener service listens for print jobs, to be used by iOS devices when the default port is blocked. • To enable the port, check **Enable**. • To transfer the print data securely, check **SSL**.

5.6.2 Configuring IPP Printing

The PrinterOn Server includes an IPP connector that allows administrators to deliver print jobs generated by third-party IPP print servers and clients to designated printers located in remote locations.

To configure the IPP printing:

1. In the Configuration Manager, click **Workflows** > **IPP and Native iOS Printing**.

2. Configure the IPP Printers settings as necessary.

3. Click **Apply Settings**.

5.6.2.1 IPP Printers settings

Setting	Description
Enable	When enabled, the printer can receive IPP print jobs.
Printer Data Type	Specifies whether the job data must be processed by the PrinterOn Server or can be delivered as is to the destination printer. • **Rendered**: The print job data is already prepared for the destination printer and no additional processing by the PrinterOn Server is necessary. For example, the client may submit PCL, or other printable data to the PrinterOn server. • **Unrendered**: The PrinterOn server must provide additional processing and conversion before the destination printer can accept the print job data. For example, the client may generate and submit a PDF file to the server that must then be converted by the PrintAnywhere server before being delivered to the printer.

5.6.2.2 Configuring IPP printing on your Windows Server

To set up IPP Printing on your Windows Server:

1. Configure your Windows Server roles to support print services:

   a) In the Server Manager, click **Server Roles**, then check **Print and Documentation Services**.

   > **Note:** In Windows Server 2008, you must also check the Printer Server role service.

2. Install the IPP Printing Client:

    a) In the Server Manager, click **Features**, then check **IPP Printing Client**.

3. Reboot the server.

5.6.2.3 Connecting an IPP printer in Windows

You can use the following steps to connect Windows to PrinterOn using IPP. You'll need the IP address of the server hosting the PrinterOn software.

> **Note:** The specific panels in Control Panel may vary depending on which version of Windows you are running.

To connect an IPP printer to a Windows:

1. Enable IPP printing:

    a) Click **Control Panel** > **Programs and Features**, then select **Turn Windows Features On or Off**.

    b) In the features list, expand **Print and Document Services** and verify that **Internet Printing Client** is checked.

2. Return to the Control Panel home page, then open **Devices and Printers**.

3. On the Devices and Printers screen, click **Add a Printer**.

4. In the Add Printer dialog, choose **Network**, then click **The printer I want isn't listed**.

5. Choose **Select a shared printer by name** and enter the IP address of the machine where the PDG is located. Include the port number used by the PDG. For example:

    http://172.16.100.101:6310/generated-printer-1

    If necessary, you can validate that the port is open by using Telnet.

6. Click **Next**. Windows attempts to connect to the PrinterOn printer using IPP.

7. Select the printer driver that you want to use.

5.6.2.4 Supporting IPP over HTTPS

If you intend to print using IPP over HTTPS, you'll need to install a valid self-signed SSL certificate on the PrinterOn server, and the server hosting the PDG, if it is installed on another server.

> **Note:** Only install SSL certificates from servers that you trust.

To install a certificate:

1. Log in as an administrator.

2. Right-click on Internet Explorer, and click **Run as administrator**.

3. In Internet Explorer, browse to the following URL:

    https://*PDG_Server_IP_Address*/

4. Because there is no certificate installed in the server, you'll receive a certificate error. Click on the error.

5. Click **View Certificates**.

6. In the Certificates window, click **Install Certificate...**.

7. Select **Place all certificates in the following store**, then click **Browse**.

8. Select **Trusted Root Certification Authorities**, then click **OK**.

9. Click **Next**, then click **Finish**.

10. A security warning will appear informing you that you are adding a certificate from a source that cannot be validated. Click **Yes** to trust this certificate.

6

Managing your PrinterOn deployment

From the **Home** tab, you can access a number of general settings and details about your server.

This tab contains several subtabs:

- Overview: Provides system information and an overview of system health.
- General Settings: Lets you configure cross-component settings.
- Services: Lets you view and change the status of the PrinterOn services.
- Licensing: Lets you view and manage your license information.
- Serial Numbers: Lets you view serial number information for server components and add additional PDS and PDH instances or PrintAnywhere Servers to your service.

6.1 Viewing system information

The **Overview** tab is mostly informative, and provides high-level details about your server. This information can help you quickly identify when there are issues. Additionally, when issues do occur, knowledge about your system is often necessary to help diagnose the problem.

To view system information:

1. In the Configuration Manager, click **Home** > **Overview**.

2. Review the information in the panels:

- **Server Overview**: Provides information about your PrinterOn Server software version. Click **PrinterOn Administration Page** to open the PrinterOn.com web admin portal at www.printeron.com/administrators.

- **Usage Overview:** Provides an overview of the system usage, displaying basic printer and print job metrics that detail how many jobs have been processed, and how many pages have been saved.

> **Note:** The server calculates the number of pages saved as follows:
>
> - If a job is submitted and held for release but the user never releases the job, all pages in the job are considered saved. This usually is when the printer has been configured for secure release.
>
> - If duplex is used when printing, each physical piece of paper saved is counted as a saved page.
>
>   For example, when printing a 4-page document with duplex selected, the system considers that 2 pages are saved, since only 2 physical pages are used. When printing a 3-page document with duplex, only 1 page is saved, since 2 physical pages are still used.
>
> - If a job is printed as Color, then the savings are tallied as **# of Color Pages Saved**.
>
> - If a job is printed as Black and White, then the savings are tallied as **# of B&W Pages Saved**.

- **System Health**: Provides an overview of the current components and remote servers managed by this Configuration Manager. Click the links to view and configure the components.

- **System Information**: Provides an overview of the Windows Server currently being used.

> **Note:** This information represents the server where the parent Configuration Manager is installed. When installing all components on multiple servers, you should load this page in the Configuration Manager for each server.

6.1.1 Viewing version information for all installed server components

In addition to seeing the server software version, you can also view the specific version for each component installed as part of the PrinterOn Server installation.

To view component version information:

1. In the Configuration Manager, click **Home** > **Overview**.
2. In the **Server Overview** panel, click the value for **Server Version**. The Installed Components Versions dialog appears.

<div align="center">

Installed Components Versions   ✕

Server Version	3.2.0.1172
Central Print Services Version	3.2.0.789
PrintAnywhere Version	5.2.0.483
PrintWhere Version	5.2.0.439
Print Delivery Gateway Version	3.2.0.465
Print Delivery Station Version	3.2.0.623
RenderPDF Engine Version	5.2.0.25
Java Version	1.8.0_51

Close

</div>

6.1.2 Exporting server and system information

You can export the system and server information displayed on the **Overview** tab to a text file that you can

To export system information:

1. In the Configuration Manager, click **Home** > **Overview**.
2. Locate the **System Health** panel, then click **Export System Information**. A text file with a summary of the content of this tab is created and displayed in your browser.

6.1.3 Creating a package of diagnostic information

In order to diagnose an issue with your PrinterOn Server, you may need to send PrinterOn Support the log files for all your server subcomponents. You can quickly create a package of this information from the **Overview** tab.

To create a package for PrinterOn support:

1. In the Configuration Manager, click **Home** > **Overview**.

2. Locate the **System Health** panel, then click **Download Support Package**. The Configuration creates a ZIP file with comprehensive server information and logs for all managed components.

6.2 Configuring general cross-component settings

The **General Settings** tab lets you configure some of the most common configuration values from a single location. The options in this section are applied to all components and servers.

To configure job management settings:

1. In the Configuration Manager, click **Home** > **General Settings**.

2. In the **Debug Logging** panel, specify the logging level to use across all components.

3. In the **Job Management** panel, set the cross-component storage and workflow options. These settings allow you configure how print data is stored and to set some general limits to control the impact of printing on your network bandwidth.

4. In the **Proxy Settings** panel, define the server proxy settings for the Central Print Services, if you are using a proxy server.

5. In the **Printer Synchronization Settings** panel (available in Advanced view only), specify how services and printers are synchronized.

6. In the **Advertised Capabilities** panel (available in Advanced view only), define which features your PrinterOn service supports. These values are then sent to client applications that want to print using the service, such as the PrinterOn Mobile App, to help them optimize their behavior.

7. Click **Apply Settings**.

6.2.1 Setting debug logging levels

The Debug Logging panel of the General tab lets you set cross-component logging levels. Higher levels of logging are most useful when troubleshooting.

Debug Logging		
Log Level	Information	▾

Note: The Logging level you define here is applied to all PrinterOn components, unless you specify a different logging level for a specific component.

To configure the logging level for a specific component:

1. In the Configuration Manager, click **Advanced** > **Components**, then click the **Configure** button adjacent to the component you want to set a different logging level for.

2. Click the **Logging** tab, and configure the logging level as necessary.

In general, to reduce the impact on server performance, you should set the logging to **Information** (the default) or lower, and adjust it only when necessary to troubleshoot an issue.

6.2.1.1 Logging levels

Log Level	Description
Off	All logging is disabled.
Fatal	Only records non-recoverable or fatal errors.
Error	Records all errors.
Warning	Records warning messages (recoverable errors or unexpected conditions).
Information	Records all informational messages (default).
Debug	Records detailed troubleshooting logs that are useful for debugging.
Trace	Records more detailed troubleshooting logs than Debug.
All	Records all log information, providing the most detailed logs.

6.2.2 Configuring Job Management settings

The **Job Management** panel of the General tab lets you set cross-component workflow options. These settings allow you to set some general limits to control the impact of printing on your network bandwidth.

Job Management		
Job Storage Settings	Configure	
Job Size Limit	50	MB
Pending Release Job Expiry (Print Delivery Station)	50	Hours
Pending Download Job Expiry (Print Delivery Hub)	72	Hours

6.2.2.1 Job Management settings

Setting	Description
Job Data Storage	Lets you choose the Storage type, and if necessary, configure storage location settings. Click **Configure** to modify the settings. For more information, see Configuring job storage.
Job Size Limit	The maximum size of a document that will be accepted by the server. Users are notified that their document is too large when submitting a document larger than the configured value.
Pending Release Job Expiry	The maximum length of time that a job is held by the PDS without being released before the PDS deletes the job.
Pending Download Job Expiry	The maximum length of time that a job is held by a PDH without being downloaded by a PDS before the PDH deletes the job. This setting only applies if you have deployed a Print Delivery Hub component along with your server.

6.2.3 Configuring proxy settings for the Central Print Services

The Proxy Settings panel of the General tab lets you define the server proxy settings, if you are using a proxy server.
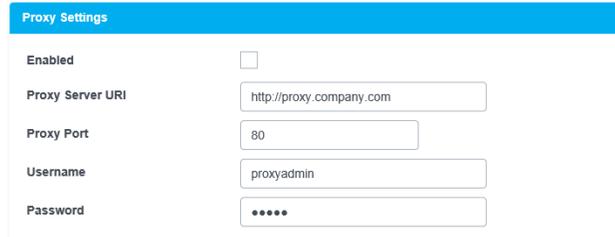
Proxy Settings	
Enabled	☐
Proxy Server URI	http://proxy.company.com
Proxy Port	80
Username	proxyadmin
Password	•••••

Note: The proxy settings you define here are only used by the CPS. In most deployments, this is sufficient, since all communication with the PrinterOn Directory flows through the CPS. However, there are cases where setting proxy settings for only the CPS is insufficient.

For more information about these scenarios and how to troubleshoot proxy communication issues, see Troubleshooting proxy issues.

6.2.3.1 Proxy Settings

Setting	Description
Enabled	When enabled, a proxy server is used.
Proxy Server URI	The URL or IP address of the proxy server with which to communicate.
Proxy Port	The network port number with which the proxy server has been configured to communicate.
Username	The user name required to authenticate against the proxy server, if required. **Note:** For NTLM Proxies, ensure that the Windows Domain name is added to the Username. This will automatically cause the server to use NTLM proxy options.
Password	The password required to authenticate against the proxy server, if required.

Managing your PrinterOn deployment

6.2.4 Configuring printer synchronization settings

The **Printer Synchronization Settings** panel of the General tab lets you specify how services and printers are synchronized.

> **Note:** To view the Printer Synchronization Settings panel, you need to turn on Advanced view.

6.2.4.1 Printer Synchronization Settings

Setting	Description
Synchronize By Default	When enabled, the component is updated when synchronizing printers with the PrinterOn Directory. Disable this setting only if you want to manually control synchronization with the PrinterOn Directory.
Automatic Printer Synchronization	When enabled, the component is automatically synchronized with the central printer list.
Synchronization Interval	The interval, in minutes, that the components is synchronized the central printer list.

6.2.5 Configuring service capabilities

The Advertised Capabilities panel of the General tab lets you advertise to client applications such as the PrinterOn Mobile App, what capabilities the service supports. The client app queries the PrinterOn Server to determine service capabilities and limitations and optimizes its behavior based on the response.

These settings are strictly informative, and are intended to provide a hint to client applications what they can expect from the PrinterOn service. However, advertising a capability does not guarantee that the feature is enabled in the relevant PrinterOn component. You should ensure that the values you configure here match the relevant feature configuration for your server.

> **Note:** To view the Advertised Capabilities panel, you need to turn on Advanced view.

6.2.5.1 Advertised Capabilities settings

Setting	Description
Preview Enabled	When checked, informs the client app that the PrinterOn Server provides print preview data. The PrinterOn mobile app is limited in what print preview data it van generate can only generate preview data for certain file formats (typically image formats and pdf). When server preview is available, the server provides preview data for other formats that the mobile app cannot generate locally. Currently, this setting is still in Beta and is disabled by default. Before enabling this setting, ensure that the Preview feature is properly configured in the PAS component settings: 1. Click **Advanced** > **Components**, then click the **Configure** button adjacent to the PrintAnywhere Server. 2. In the PAS configuration, click **Job Settings**, then locate the **Preview Settings** panel.
Secure Release Anywhere Enabled	When checked, informs the client app that the server supports Secure Release Anywhere feature, which allows users to print to a pool of printers and release the job to any of the printers in the pool. Secure Release Anywhere is an additional service that you can add to your PrinterOn service; it is not available by default. To enable Secure Release Anywhere for your service, contact PrinterOn.

Setting	Description
Directory Search Enabled	When checked, informs the client app that Directory Search is enabled on the server. Directory Search allows the mobile app to search your private PrinterOn Directory for printers on your network. This setting is enabled by default.
	Ensure that this **Directory Search Enabled** setting matches the value set in the CPS component settings:
	1. Click **Advanced** > **Components**, then click the **Configure** button adjacent to the Central Print Services.
	2. In the CPS component configuration, click **Basic**, then locate the **Directory Search Enabled** setting.
Doc API Enabled	When checked, informs the client app that the PrinterOn service supports Document API printing, which is used by the Mobile workflow, Google Cloud Print workflow, and iOS Native Print workflow. This setting is enabled by default.
	Although this setting indicates whether Document API printing is enabled for the PrinterOn service as a whole, Document API printing support is currently set on a per printer basis, as part of the Workflow options. If Document API printing is not set the same way across all printers, then you should set this setting to reflect the majority of your printers.
Company Name	Informs the client app of your company name.
Max File Size	Informs the client app what the maximum accepted file size is for a submitted print job, in MB. The default advertised maximum job size is 50 MB.
	Ensure that the file size you set matches the **Max Job File Size** defined in PAS component settings:
	1. Click **Advanced** > **Components**, then click the **Configure** button adjacent to the PrintAnywhere Server.
	2. In the PAS component configuration, click **Job Settings**, then locate the **Max Job File Size** setting in the **Incoming Job Settings** panel.
Deployment Mode	Informs the client app that the PrinterOn service is deployed in the selected mode.
	Ensure that the deployment mode you advertise matches the **Deployment Mode** defined in the Deployment Mode Configuration panel of the **Home** > **Licensing** tab.

6.3 Configuring job storage

By default, the PrinterOn Server is configured to used it's local database to store print and preview data. However, you can configure the server to use a third-party cloud solution instead. If you intend to use a third-party cloud solution, such as Amazon Web Services (AWS), to store your print data, you can configure a number of settings to optimize performance and limit the number of network requests that are made.

There are two types of data that might be stored:

Setting	Description
Print data	The data produced after rendering a document, and may include a number of PJL headers and other metadata used to convey information about the print data to the printer. The print data is generated by the PAS, and accessed by the PDH and PDS components which deliver the print data to the destination printer for printing.
Preview images	When server-side preview is enabled, the PAS renders the document and generates print preview images (one image for each page of the document) on behalf of the PrinterOn Mobile App. The previewing capabilities of the devices are very limited, so many document formats cannot be previewed, or the preview does not accurately reflect the appearance of the printed document. Server-side preview enables the PrinterOn Mobile App to display accurate previews for documents of any supported format. The preview images are stored separately from the print data. For more information on enabling server-side preview, see Enabling server-side print preview for the PrinterOn Mobile App.

You can configure the server to store print data and preview content in the same S3 instance and use the same access keys, or you can store them each in their own instance, with each instance requiring its own access keys.

To configure cloud-based job storage settings:
1. In the Configuration Manager, click **Home** > **General Settings**.
2. In the **Job Management** panel, click **Configure**. the Job Storage Settings page appears.
3. In the **Storage Configuration** panel, choose a **Storage Type** of **S3**. The page expands to display S3-specific settings.

4. In the **General S3 Settings** panel, configure the General S3 Settings as necessary.

The General S3 Settings panel lets you configure storage settings that apply to both print data and preview content.

Setting	Description
Access Key, Secret Key	The Access Key and Secret Key are part of the security credentials that are required to send requests to AWS. These keys are tied to your account. To allow the PrinterOn Server to communicate with your AWS account, you must supply these keys.
Endpoint	The entry point for AWS.
	There are a number of region-based end-points for Amazon S3 storage. However, to simplify the endpoint definition, Amazon is moving a virtual hosted model, in which the region is not specified in the URI. Endpoints that include the region will not be supported after September 30, 2020.
	To ensure that PDS and PDH are able to access print data from this location, the **Endpoint** value should be set to the following: https://s3.amazonaws.com
Bucket	The top-level location for your data within AWS. If sharing the same bucket, print data and preview content are stored in unique folders within the specified bucket.
Optimize Job Delivery	When selected, the PrinterOn Server only uploads ands stores a print job once, saving bandwidth and speeding up communication.

5. In the **Preview Settings** panel, configure the Preview storage information.

The Preview Settings let you configure how the server manages preview data generated by the PrintAnywhere Server (PAS).

Setting	Description
Same as Above	When checked, the Preview images are stored using the same account, endpoint and bucket that you defined in the General Settings panel.
	When unchecked, a number of fields are
Delete Preview Files After	Specifies the time, in minutes, that the preview images are stored before being deleted from the preview bucket.
Location Constraint	Specifies the region where the bucket is physically located.
Max Upload Threads	The maximum number of simultaneous connections the PrinterOn Server will create when communicating with the S3 service.
Publish Count	The number of retries the PAS will attempt to successfully publish the preview content to the AWS.
Publish Interval	The length of time before the PAS will attempt to republish the preview content after an unsuccessful attempt to publish.

6. In the **Print URI** panel, configure the Print data storage settings.

The Print URI settings let you configure how the server posts print data to the cloud storage service.

Setting	Description
Same as Above	The Access Key and Secret Key are part of the security credentials that are required to send requests to AWS. These keys are tied to your account. To allow the PrinterOn Server to communicate with your AWS account, you must supply these keys.
Location Constraint	Specifies the region where the bucket is physically located.
Publish Count	The number of retries the PAS will attempt to successfully publish the print data to the AWS.
Publish Interval	The length of time before the PAS will attempt to republish the print data after an unsuccessful attempt to publish.
URI Expires	The length of time that the URI is valid.

7. Click **Apply Settings**.

6.4 Enabling server-side print preview for the PrinterOn Mobile App

The Advertised Capabilities panel of the General tab lets you advertise to client applications such as the PrinterOn Mobile App, what capabilities the service supports. The client app queries the PrinterOn Server to determine service capabilities and limitations and optimizes its behavior based on the response.

When server-side preview is enabled, the PrintAnywhere Server renders the document and generates print preview images (one image for each page of the document) on behalf of the PrinterOn Mobile App.

By default, the PrinterOn Mobile App integrates with the mobile device's preview capabilities. However, the previewing capabilities of the devices are typically very limited, so many document formats cannot be previewed, or the preview does not accurately reflect the appearance of the printed document. Server-side preview enables the PrinterOn Mobile App to display accurate previews for documents of any supported format. The preview images are stored separately from the print data.

6.4.1 Server-side preview workflow

When the Mobile App user requests a preview of the document, the app submits the document to the server. The server then renders the app and then makes the preview images available to the device. To minimize network traffic, the PrinterOn Mobile App only downloads the preview images as they are displayed in the PrinterOn Mobile App.

> **Note:** There are known issues when using Libre Office to render documents with certain print options enabled. Currently, the orientation, paper size, and BW settings are ignored.

6.4.2 Server prerequisites

Server-side preview requires that Ghostscript be installed on the server. Ghostscript is a Postscript and PDF interpreter and rendering engine.

You can download Ghostscript at ghostscript.com/download/gsdnld.html.

6.4.3 Enabling server-side previews

To enable server-side preview:

1. In the Configuration Manager, make sure that Advanced view is on.
2. Click **Home** > **General Settings**, then locate the Advertised Capabilities panel at the bottom of the page.

3. In the Advertised Capabilities panel, check **Preview Enabled**.

6.5 Starting, stopping, or restarting the PrinterOn services

The **Services** tab allows you to quickly see the status of the component services installed with your PrinterOn Server.

To start, stop, or restart a PrinterOn service:

1. In the Configuration Manager, click **Home** > **Services**.

2. Click the appropriate button adjacent to the service that you want to start, stop, or restart.

6.6 Managing your PrinterOn license

From the **Licensing** tab, you can:

*   Update your PrinterOn Server license.
*   Download your PrinterOn Server license.
*   Download a custom license that you can use when installing a component on a remote server.
*   review your license information.
*   Modify your server deployment mode or set the internal Service URI.

6.6.1 Updating your PrinterOn license

The PrinterOn Server uses the information in your PrinterOn license file (PrinterOnConfig.txt) to determine what server features you can access. Your license will have a specified expiry date, after which you'll have no access to the PrinterOn service.

If you change the conditions of your license (for example, by adding additional printers, or extending the term of your existing license), you must update your license in the Configuration Manager before the changes take effect.

> **Note:** You MUST update your license before the term of the license expires to continue operation. The server will stop operation after the license expires.

To update your license file:

1. In the Configuration Manager, click **Home** > **Licensing**.
2. Locate the buttons at the bottom of the page.
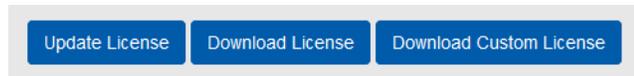
3. Click **Update License**. The Upload A New License dialog appears.

4. Enter the path to your updated license file, then click **Upload**.

6.6.2 Downloading your PrinterOn license

To download your license file:

1. In the Configuration Manager, click **Home** > **Licensing**.
2. Locate the buttons at the bottom of the page and click **Download License**.
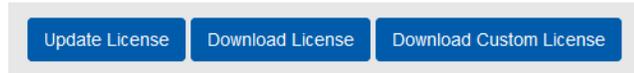
6.6.3 Downloading a custom PrinterOn license

If you intend to install a component such as a PDS on a remote server, you can simplify the set up by creating and downloading a custom license. A custom license lets you provide some additional details—such as a the parent server URI or a PDS serial number—that are not typically included in the license file.

With this information, the installer is able to pre-populate some configuration settings.

Before you download a custom PrinterOn license, you should complete steps 1-5 of the Before you begin section in Installing and configuring a remote PDS.

To update your license file:

1. In the Configuration Manager, click **Home** > **Licensing**.
2. Locate the buttons at the bottom of the page.
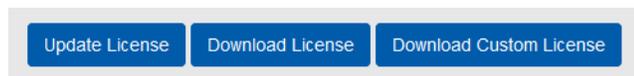
3. Click **Download Custom License**. The Select PDS Servers dialog appears.
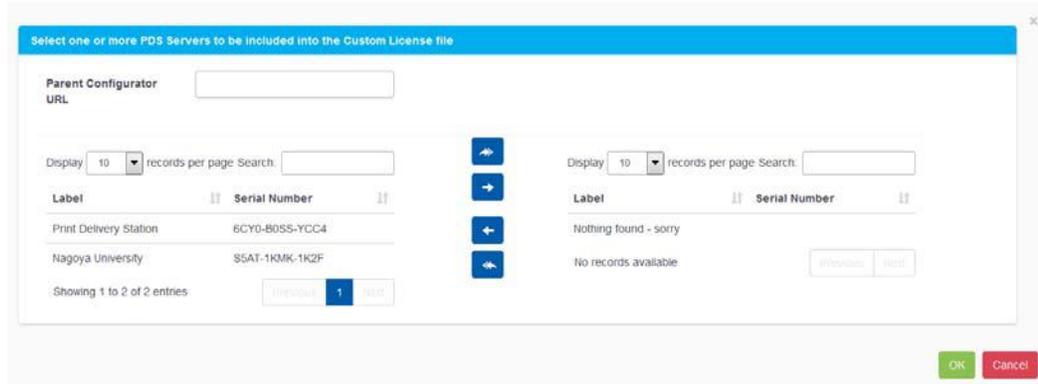
4. In the **Parent Configurator URI** field, enter the IP address and port of your central PrinterOn Server machine on which you manage all your PrinterOn services. The default port is 8057.

   This setting is optional:

   - If you provide a value for this setting, it is added to the custom license file and is used to automatically link the remote server to the parent upon installation, so you don't have to link to the Parent manually.

   - If you leave the setting blank, the remote server is not linked upon installation; however, you can link it manually at any time.

5. Choose one or more PDS serial numbers to include in the license by moving an available serial number on the left to the list on the right.

   Including multiple serial numbers allows you to use the same custom license for multiple remote installations.

6. Click **OK**.

7. Once downloaded, copy the license to the remote server(s) on which you intend to install a PDS instance. When prompted for the license file during the PDS installation, select this custom license file.

6.6.4 Viewing your license information

You can quickly review your current license information from the Configuration Manager.

To view license information:

1. In the Configuration Manager, click **Home** > **Licensing**.

2. Review the content in the following panels:

    • **License Details**: Provides information about what version and edition of the server you are permitted to install. This panel also specifies the expiry date of your license.

    • **License Features**: Provides information about which features of the PrinterOn Server you have permission to use.

6.6.4.1 License Details

Entry	Description
Version	The version of the server license. This value is **not** the version of the server software.
Edition	The edition of the PrinterOn Server that is associated with the license, for example, Express or Enterprise.
Start Date	The date on which your PrinterOn Server license was created.
End date	The date on which your PrinterOn Server license expires. You MUST update your license before the term of the license expires to continue operation. The server will stop operation after the license expires.
Site UID	A unique identifier used to set up your server. This ID is used during the installation to link your service to the PrinterOn Directory
Administrator Email	The email address of the administrator who created and manages the server license on the PrinterOn website.

6.6.5 Modifying the server deployment mode

By default, the PrinterOn Server supports several deployment modes.

To change the deployment mode for your PrinterOn services:

1. In the Configuration Manager, click **Home** > **Licensing**, and locate the **Deployment Mode Configuration** panel.
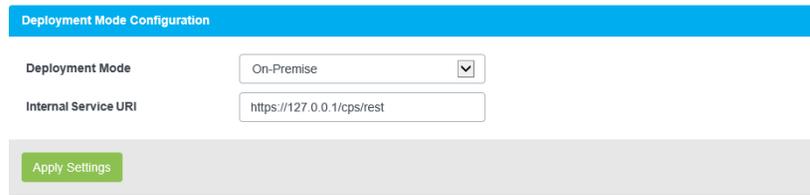
2. Choose the **Deployment Mode** from the drop-down. You can deploy the PrinterOn Server in one of the following modes:

    •   On-Premise

    •   On-Premise with Cloud Config

    •   Hybrid

    •   Hybrid Direct

    Click on a deployment for more information.

3. In the **Internal Service URI** field, specify the address used by the subcomponents to communicate with the Central Print Services in a distributed deployment. The Internal Service URI should be the following value:

    <PrinterOn_Server_IP>/cps/rest

4. Click **Apply Settings**.

6.6.5.1 On-Premise

The On-Premise deployment mode provides a fully isolated deployment with no external dependencies. All data is managed locally and all printer configuration is managed and stored in a local database.

Data Center
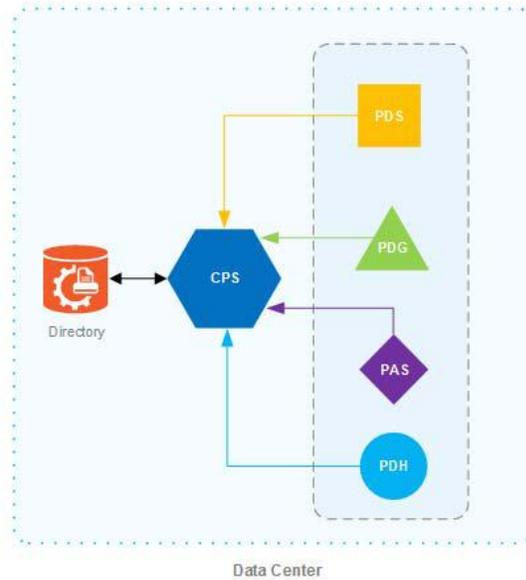
6.6.5.2 On-Premise with Cloud Config

The On-Premise with Cloud Config deployment mode provides a secure deployment that can operate with no persistent Internet connections. All data is managed locally, but printer configuration is managed using the PrinterOn Directory.

This deployment mode allows printers to be pre-configured and backed up using the PrinterOn Directory. No document data or job information is sent to the PrinterOn Directory; the Directory stores only printer information.

The On-Premise with Cloud Config deployment mode also supports PrinterOn's global driver distribution tools and automatic encryption key exchange between the Print Server and Release Stations.
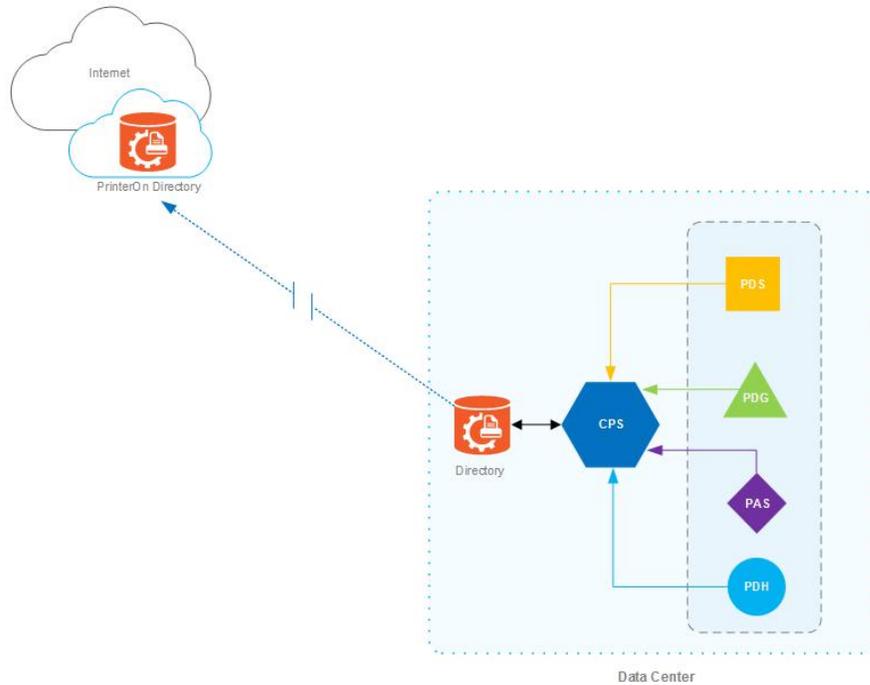
6.6.5.3 Hybrid

In a Hybrid deployment, all communication with the PrinterOn Directory is proxied through a single Central Print Services instance. Each subcomponent communicates with the address specified in the Services Manager URI.
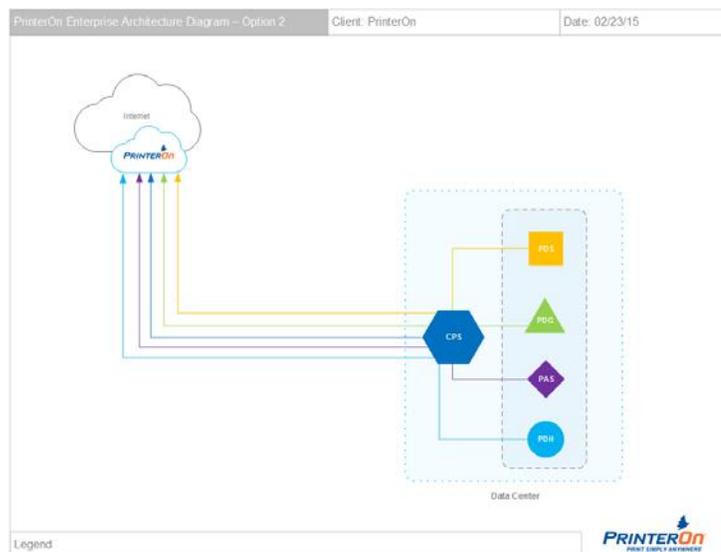
6.6.5.4 Hybrid Direct

In a Hybrid Direct deployment, all communication with the PrinterOn Directory occurs directly from the component to the PrinterOn Directory. This deployment mode is useful when using isolated components that cannot communicate with a single central server to be proxied.
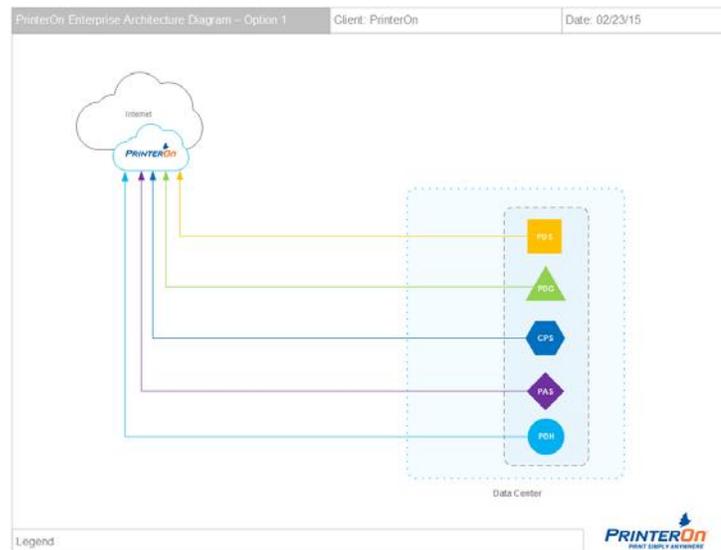
6.7 Managing components

The Serial Numbers tab lets you add new components and manage which components are active.

6.7.1 Adding component instances

Your PrinterOn service can have multiple instances of Print Delivery Stations (PDS), Print Delivery Hubs (PDH), and PrintAnywhere Servers. To identify each instance, PrinterOn uses serial numbers. Each time you create a PDS, PDH, or PrintAnywhere Server, it receives a unique serial number.

To add instances of a component:

1. Click **Home** > **Serial Numbers**.

2. Scroll to the bottom of the page and click the button for the component that you want to add.

3. In the Add dialog, enter the **Server Description** for the component. The server description is used to identify the component, so it should be meaningful.

4. Click **Add**.

6.7.2 Changing the serial number of an active component

To change the serial number of a component:

1. In the Configuration Manager, click **Home** > **Serial Numbers**, and locate the **Serial Numbers In Use** panel.
2. Locate the component you want to change, then click the adjacent **Change** button.
3. In the **Choose a New Serial Number** dialog, in the **Serial Number** drop-down, Choose a serial number of an inactive component, or select **New Serial Number** to create a new instance.
4. If you selected **New Serial Number**, specify a **Serial Number Label**.
5. Click **Apply Settings**.

6.7.3 Deleting unused serial numbers

Your PrinterOn license specifies how many instances of each component you are allowed to have. If you have an instance that is not in use, you can delete the component for that instance to free up the serial number so you can create a new instance.

To delete the serial number:

1. In the Configuration Manager, click **Home** > **Serial Numbers**, and locate the **Serial Numbers Not In Use** panel.

2. Locate the component you want to change, then click the adjacent **Delete** button.

7

Configuring authentication settings

The Authentication tab lets you specify the authentication method you want to use with your PrinterOn solution, and configure method-specific settings.

7.1 Supported authentication methods

PrinterOn supports a variety of authentication methods, giving you the flexibility to adapt the PrinterOn service to your organization's security model. You can also choose not to authenticate users at all, if necessary.

You can choose from the following authentication methods:

Authentication Method	Description
Inactive/None	No authentication is used. No login information is collected.
LDAP/AD	PrinterOn authenticates user credentials using Lightweight Directory Access Protocol (LDAP) to communicate with an Active Directory (AD).
Internal Users *(on-premise deployment mode only)*	PrinterOn authenticates user credentials against the internal PrinterOn user store.
Azure AD *(on-premise deployment mode only)*	PrinterOn authenticates user credentials against an Azure Active Directory, Microsoft's cloud-based identity and access management solution.

Authentication Method	Description
Third-Party Identity Management Service *(on-premise deployment mode only)*	PrinterOn authenticates user credentials against a cloud-based, third-party Identity Management Service (IdM), such as Ping Identity or Okta.
PrinterOn AAA Login (Custom)	PrinterOn authenticates user credentials against a designated web service to perform user authentication.
Web Print Only (SSO)	PrinterOn authenticates user credentials against a designated web server/service. **Note:** To use Remote Authentication/single sign on, your web server must authenticate the user and pass their identification to the PrinterOn Server with the **REMOTE-USER** HTTP header.
PrinterOn ACL *(hybrid deployment mode only)*	Authenticates the user's login information against PrinterOn's user database during printing.

7.2 Selecting your authentication method

To select the authentication method you want to use to manage access to the PrinterOn services:

1. In the Configuration Manager, click **Authentication**. The Authentication tab appears.
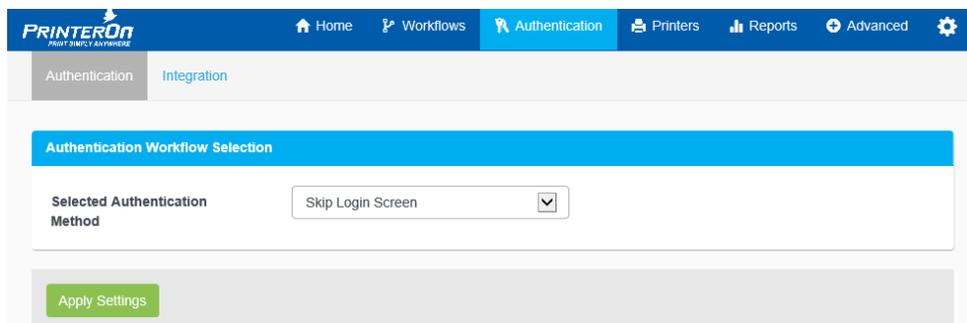
2. In the **Selected Authentication Method** drop down, select the authentication method that you want to implement.

3. Depending on the Authentication Method you choose, you may need to configure additional settings. Configure the settings specific to the selected authentication method as necessary:

   - Configuring PrinterOn to authenticate with LDAP/AD
   - Configuring PrinterOn to authenticate against the PrinterOn user store
   - Configuring PrinterOn to use Azure AD
   - Configuring PrinterOn to authenticate against a third-party Identity Management Service
   - Configuring PrinterOn to authenticate using AAA Login
   - Configuring PrinterOn to authenticate for Web Print workflow only
   - Configuring PrinterOn to authenticate using ACL

4. Click **Apply Settings**.

7.3 Configuring PrinterOn to authenticate with LDAP/AD

You can configure the PrinterOn Server to use the Lightweight Directory Access Protocol (LDAP) to communicate with an Active Directory (AD) or any other directory services to authenticate users. The LDAP/AD configuration allows you to use multiple LDAP servers for authentication, which provides redundancy if one of those servers is offline.

When multiple servers are used:

- The PrinterOn Server searches and validates user credentials by connecting to all configured LDAP simultaneously.
- The PrinterOn Server uses the results of the first successfully located/ authenticated user.

Each server is independently configured and managed. You must configure an LDAP/AD profile for each LDAP server you add. You can then select the profile to configure the server-specific authentication settings.

To configure the authentication behavior for an LDAP/AD server:

1. On the **Authentication** tab, select **LDAP/AD** as your Authentication method. The **LDAP/AD Settings** and **Authentication Behavior** panels appear.

2. In the **LPAD/AD Settings** panel, from the **LDAP/AD Server Profile** drop-down, choose which LDAP Server you want to configure.

   Note: You must configure a server profile for each LDAP server you add to your solution. For more information, see Creating and managing LDAP/AD profiles.

3. Define your **User Rules and Printer Access** logic. For more information, see Configuring LDAP/AD access control rules.

4. To require the PrinterOn Server to use LDAP/AD credentials for mobile app users, check **Web Authentication Enabled for Mobile (**Advanced view only).

   Note: You should typically check this option. You should only disable this option if web-based authentication is configured through PrinterOn's services to ensure that the mobile users are prompted to authenticate.

5. In the **Authentication Behavior** panel, configure the following settings as necessary:

   • **Guest Login Enabled**: When enabled, specifies that unauthenticated users are permitted to print. When guest login is enabled, you must also configure guest identification and designate one or more printers as guest printers. For more information, see Configuring guest printing.

   • **Trusted Application Behavior** (Advanced view only): Defines the minimum authentication requirements for users printing through the Print Delivery

Gateway (PDG) using the Google Cloud Print workflow. For more information, see Configuring authentication requirements for Google Cloud Print users.

6. Click **Apply Settings**.

7.3.1 Creating and managing LDAP/AD profiles

The PrinterOn Server supports configuring and using multiple LDAP/AD servers at the same time. Each server is independently configured and managed, which provides redundancy while authenticating the user if one of those servers is offline. You must configure an LDAP/AD profile for each LDAP server you add.

The **LDAP/AD Server Profiles** drop-down list provides access to all configured LDAP servers. The settings below the list apply to the selected server.

Servers are identified by their profile name, which you configure in the **LDAP/AD Profile Details** page. You should make sure each server has a unique name so you can easily identify which LDAP server you configuring.

7.3.1.1 Adding an LDAP/AD server profile

To add an LDAP/AD server profile:

1. In the **LDAP/AD Settings** panel, click **Add**. The LDAP/AD Profile Details page appears, with some default settings values provided.
2. Configure the LDAP server connection information as necessary.
3. Once you have confirmed the profile is correctly configured, click **Apply Settings**.

7.3.1.2 Deleting an LDAP/AD server profile

To delete an LDAP/AD server profile:

1. In the **LDAP/AD Settings** panel, select the server profile to remove from the **LDAP/AD Server Profiles** drop-down.
2. Click **Delete**.

7.3.1.3 Editing an LDAP/AD server profile

To edit an LDAP/AD server profile:

1. In the **LDAP/AD Settings** panel, select the server to modify from the **LDAP/AD Server Profiles** drop-down.

2. Click **Edit**. The LDAP/AD Profile Details page appears.

3. Configure the LDAP server connection information as necessary.

4. Once you have confirmed the profile is correctly configured, click **Apply Settings**.

7.3.2 Configuring LDAP/AD server profiles

LDAP/AD server profiles are configured on the LDAP/AD Profile Details page.

7.3.2.1 LDAP/AD Profile settings

Setting	Description
Active	When checked, enables the profile.
Name	A unique name for the configuration profile.
Mode (*Advanced view* only)	The mode of LDAP authentication. The mode can be one of: • **Advanced**: Validates the user's login and password against your LDAP server. This authentication method also allows the PrinterOn Server to look up other user attributes such as a user's email address, network login, or even a custom attribute field. The supplied Bind DN and Bind Password information is used to locate and authenticate users. • **Basic**: Validates that the user credentials exist and are valid against a given LDAP server. Instead of retrieving the user's email address from the LDAP server, it is composed using their login ID and a specified domain name. This authentication method binds the user to the LDAP server using simple authentication, and assumes that your LDAP server uses (or extends) the standard schema. If you have a custom LDAP deployment, this authentication may not work without further modification. **Note:** With Basic Authentication, User Lookup integration for email printing is not possible.
LDAP/AD Server URI	The IP address or DNS name of the LDAP/AD server to be used for authentication.
Enable SSL	When checked, the LDAP/AD server uses SSL. Enable this option if your LDAP server requires SSL connections. **Note:** If you check **Enable SSL**, you must also make sure that **LDAP/AD Server URI** specifies the ldaps:// protocol and SSL port (typically 636).
Search DN(s)	The distinguished names (DN) representing the branch from which the search for the users occurs. If you selected **Advanced** LDAP mode, searches look for users in this branch and below of the LDAP tree. This field supports multiple Search DNs. Separate multiple DNs with a semi-colon (for example, ou=OrganizationalUnit;dc=domain).

Setting	Description
Administrator Bind DN *(Advanced Mode Only)*	The distinguished name (DN) representing the login used to bind the LDAP server for searches. This option is used to search for users and user information in the LDAP/AD server. It can be represented in two ways: • server\username • cn=display name,ou=OrganizationalUnit,dc=domain
Administrator Password *(Advanced Mode Only)*	The password for the login given in **Administrator Bind DN** above.
Domain Name to Append to User ID *(Basic Mode Only)*	The domain name used in conjunction with the user's ID to create their email address. The domain name is appended to the user's ID to make a valid email address. For example, if the user ID is **jsmith** and you set the domain name to **myorganization.com**, then the email address is: jsmith@myorganization.com
Bind Users *(Advanced view only)*	When checked, users are authenticated and bound to the LDAP Server. Any requests received are not trusted and require full authentication. **Note:** There is a limitation when disabling this setting. If you have multiple LDAP instances configured, when using Web Print, the PrinterOn server only reads the configuration of the first LDAP instance. If you disable this setting on the first LDAP instance, that setting will be applied to all instances. Conversely, if you disable this setting on an instance other than the first instance, the setting will be ignored and the default setting (enabled) is applied to all instances.
Prepend Windows Domain Name to User UD	When checked, a domain name or other qualifier is prepended to the user ID when submitted with the print job. This user ID is transmitted throughout the workflow and communicated with any third-party print management systems to assist in reporting and user tracking.
Follow LDAP Referrals *(Advanced view only)*	When checked, LDAP referrals are followed when searching for users on an LDAP/AD server. This option should generally be checked, unless your LDAP/AD server specifically requires that referrals be ignored.
E-mail Address Wildcard Search *(Advanced view only)*	When checked, wild cards can be used in searching.

Setting	Description
Prepend "smtp:" to E-Mail Address Searching *(Advanced view only)*	When checked, smtp: is prepended to email addresses. Some LDAP/AD environments contain multiple user IDs for each user. When performing a user lookup using a supplied email address, prepending smtp: to the user ID assists in differentiating between users. This setting should be enabled when using user email in an AD environment.
Enable Configuration Manager Access *(Advanced view only)*	When checked, the LDAP/AD profile is used as a PrinterOn Administrator profile, allowing you to designate a set of users who can administer the PrinterOn Server. These users can log into Configuration Manager using their standard credentials, rather than logging in through the built-in Root user account. If you want to use LDAP/AD for authentication when logging into Configuration Manager, you **must** enable this setting. For more information about how to configure the Configuration Manager to authenticate against an LDAP/AD server, see Modifying the Configuration Manager Authentication mode.
User ID Attribute	The LDAP/AD server attribute field containing the user login IDs. This attribute is appended to the Base DN in order to do user lookup in the Directory. For example, given a **User ID Attribute** of **cn**, the PrinterOn Server attempts to validate users via the following path: cn=LoginName,ou=People,dc=ldapdomain.
User Email Attribute	The LDAP/AD server attribute field containing the user's email address. This attribute is appended to the Base DN in order to fetch the user's email address once they are validated against the Directory. For example, given a **User Email Attribute** of **mail**, the PrinterOn Server attempts to look up user's email addresses in the directory via the following path: mail,ou=People,dc=ldapdomain
User Display Name Attribute *(Advanced view only)*	The LDAP/AD server attribute filed containing the full display name.
User First Name Attribute *(Advanced view only)*	The LDAP/AD server attribute field containing the user's first name.
User Surname Attribute *(Advanced view only)*	The LDAP/AD server attribute field containing the user's surname or last name.

Setting	Description
User Phone Number Attribute(s) (*Advanced view* only)	The LDAP/AD server attribute field containing the user's phone number.

7.3.3 Configuring LDAP/AD access control rules

Access control rules allow you to control which users can access and discover printers. On your LDAP/AD server, you can organize your users in to Organizational Units (OUs) and Groups. You can then create rules that link those OUs or Groups to PrinterOn printer departments (logical groupings of PrinterOn Printers).

> **Note:** For more information about creating and managing Printer Departments, see Managing printer departments.

For example, you could organize all members of your Marketing team into the Marketing OU, then create a printer department called Marketing, which contains all marketing team's printers. You can then create an access control rule that limits access to the Marketing printer department to those users who are part of the Marketing OU. Every user who is part of the Marketing OU can access and print to the printers in the associated department.

Access control rules also impact the discovery and search capabilities from the various workflows, including the Web Print and Mobile workflows. When searching for printers using the PrinterOn mobile app, or automatically discovering devices using PrinterOn Discovery, users are only presented with those printers to which they have been granted access.

Access control rules also apply when using technologies such as Apple AirPrint devices. Due to its implementation constraints, the PrinterOn Server cannot limit what printers are visible to iOS devices. However, it can restrict a user's ability to print to only those printers to which they have access. Although users can see all the printers that have been enabled for iOS users, they can only submit print jobs after successfully authenticating.

7.3.3.1 Configuring access control

To configure access control:

1. In the **LDAP/AD Settings** panel, from the **User Rules and Printer Access** drop-down, select either **Organizational Unit** or **Group**.

> **Note:** Rules must be based on either Organizational Units (OUs) or Groups; there cannot be a mix of both.

2. Click **Manage User Rules**. The User Rule page appears.

3. In the **User Rule To Manage** panel, select the rule you want to modify, or select **Create New Rule** to create a new one.

4. In the **Rule Settings** panel, define the **Rule Name**. You can modify the value to change the name of an existing rule.

   - If you are creating a rule for an Organizational Unit, configure the following settings.

Setting	Description
Organization Unit (OU)	A list of the automatically located OUs in the currently active LDAP configuration. You can use an existing OU to quickly configure a rule, or you can manually enter a fully qualified OU.

Setting	Description
Recursive	When checked, CPS traverses the OU tree to match users that may be in sub-units of the parent OU as well.
	In the example below, if MainDept is configured, only *User1* and *User2* will be valid if Recursive is not checked. *User3* and *User4* will be valid if Recursive is enabled.

	• MainDept
	   • User1
	   • User2
	   • SubDept
	      • User3
	      • User4

• If you are creating a rule for a Group, configure the following settings.

Setting	Description
Group	A list of the automatically located Groups in the currently active LDAP configuration. You can use an existing Group to quickly configure a rule, or you can manually enter a fully qualified Group/CN.

5. In the **Linked Printer Departments** panel, check the printer department(s) that you want to link to the rule.

> **Note:**
>
> • You must select at least one check box. You will not be permitted to apply the settings if you haven't selected a **Linked Printer Department** option.
>
> • If you select **No Departments**, users will only be able to access those printers that are not a member of any printer departments.

For more information about creating and adding printers to printer departments, see Managing printer departments.

6. Click **Apply Settings**.

7.4 Configuring PrinterOn to authenticate against the PrinterOn user store

PrinterOn includes its own user store that you can use as for identity management and access control. The PrinterOn user store lets you manage users, organize them into groups, and create access control rules to manage access to PrinterOn resources. You can manage the PrinterOn user store from the Users tab in the Configuration Manager.

The **Internal Users** authentication method relies exclusively on the internal user store for authentication and access control. After selecting and configuring this authentication method, you must create user accounts, user groups, and access control rules in the PrinterOn user store.

To configure PrinterOn to authenticate against the PrinterOn User Store:

1. On the **Authentication** tab, select **Internal Users** as your Authentication method. The **Authentication Behavior** panel appears.

2. In the **Authentication Behavior** panel, configure the following settings as necessary:

   • **Guest Login Enabled**: When enabled, specifies that unauthenticated users are permitted to print. When guest login is enabled, you must also configure guest identification and designate one or more printers as guest printers. For more information, see Configuring guest printing.

   • **Trusted Application Behavior** (Advanced view only): Defines the minimum authentication requirements for users printing through the Print Delivery Gateway (PDG) using the Google Cloud Print workflow. For more information, see Configuring authentication requirements for Google Cloud Print users.

3. Click **Apply Settings**.

You can now access the **Users** tab to populate the PrinterOn user store and create access control rules. For more information, see Managing the PrinterOn user store.

7.5 Configuring PrinterOn to use Azure AD

PrinterOn supports using Azure Active Directory, Microsoft's cloud-based Identity Management Service, as the authenticator for your PrinterOn service. Azure AD sits in the cloud, external to the PrinterOn service. As a result, when a user must authenticate, the PrinterOn Server redirects them to an external URL hosted by Azure AD where the user can supply their credentials.

If the user is successfully authenticated, Azure AD creates a user token that PrinterOn uses as confirmation that the user is authorized to access the PrinterOn service. Each subsequent time the user attempts to use a protected printer, PrinterOn checks with Azure AD to determine whether the user token is still valid. If so, the user remains authenticated. Otherwise, the user must re-authenticate.

User credentials are submitted to Azure AD. PrinterOn never requests the user's credentials directly.

When using Azure AD for authentication, the PrinterOn Server uses its internal user store to control access to PrinterOn resources. PrinterOn downloads user and/or group data from the Azure AD user store to the PrinterOn user store, where you can create access control rules.

The PrinterOn Server lets you configure how data is synchronized; you can pro-actively download the contents of the Azure AD user store, or you can populate the PrinterOn user store as each user logs in for the first time. You can control synchronization of user data and group data separately, allowing you to pre-populate the PrinterOn user store with the Azure AD groups but populate each user only when they log in for the first time, for example.

To configure PrinterOn to use Azure AD, you'll need to complete the following tasks:

1. Register your PrinterOn service with your Azure AD service. This registration creates a bond of trust between the PrinterOn server and your Azure AD service. You also need to configure the Graph API permissions to specify what Azure AD data PrinterOn can access.

2. Supply the PrinterOn Server with your Azure AD communication information. To allow PrinterOn to successfully redirect users and to synchronize data from the Azure AD user store, you need to provide PrinterOn with your Azure AD network and security information.

3. Configure the PrinterOn user store to create user groups and Access Control Rules as necessary.

7.5.1 Configuring the Azure AD communication settings

To configure PrinterOn to authenticate against your Azure AD:

1. On the **Authentication** tab, select **Azure AD** as your Authentication method. The **Azure AD Settings** and **Authentication Behavior** panels appear.

Authentication Workflow Selection

Selected Authentication Method	Azure AD ▼

Azure AD

OAuth 2.0 Authorization Endpoint	
OAuth 2.0 Token Endpoint	
Microsoft Azure AD Graph API Endpoint	
Use OIDC UserInfo API	☐
Application ID	
Application Key	
Preferred User ID Claim	
Prompt	
Enable Group Sync	☐
Enable User Sync	☐
Enable Configuration Manager Access	☐

Authentication Behavior

Guest Login Enabled	☑	Manage Guest Settings
Trusted Application Behavior ❓	Authenticated and Guest ▼	

Apply Settings

2. In the **Azure AD** panel, provide the connection information required for the PrinterOn server to communicate with your Azure AD service:

Setting	Description
OAuth 2.0 Authorization Endpoint	The URL hosted by Azure AD where PrinterOn redirects the user when they attempt to sign in to use the service.
OAuth 2.0 Token Endpoint	The URL where the PrinterOn server requests Access, ID, and Refresh tokens. The PrinterOn Server uses these tokens to determine the authentication status of the user. If the credentials have expired, the user is forced to re-authenticate.
Microsoft Azure AD Graph API Endpoint	The Azure AD Graph API endpoint. The Graph API allows PrinterOn to synchronize data between the Azure AD and PrinterOn user stores.
Prefer UserInfo API over Graph API (*Advanced view* only)	When selected, indicates that PrinterOn retrieves user information from the UserInfo API instead of the Graph API endpoint that PrinterOn typically uses to acquire this information. This setting should only be enabled in those rare instances when the Graph API does not provide the information necessary to authorize users, but the UserInfo.
Application ID	The unique ID of the PrinterOn service, generated when you registered PrinterOn with Azure AD. The PrinterOn Server requires this value to authenticate with Azure AD.
Application Key	The unique client secret key for your PrinterOn service. You must generate this key in Azure AD and copy the value immediately. The PrinterOn Server requires this value to authenticate with Azure AD.
Preferred User ID Claim (*Advanced view* only)	The identifying information that PrinterOn requires from the user when authenticating against Azure AD. This value is optional. If you define a value for this field (for example email address), then users would be required to supply that value to be authenticated. If you leave this field blank, by default PrinterOn requires the Preferred Username claim from the user to authenticate them.

Setting	Description
Prompt (*Advanced view* only)	The message PrinterOn displays to the user to allow them to grant permission for PrinterOn to authenticate them. Some Authentication services require a user's consent to allow PrinterOn access to the service on their behalf. The message you provide here will be used to prompt the user for confirmation when necessary.
Enable Group Sync	When enabled, indicates that PrinterOn will synchronize user group information between the PrinterOn user store and the Azure AD user store. The **Group Sync Interval** setting appears, letting you set how often, in minutes, PrinterOn synchronizes the group data. For more information, see How synchronization settings affect PrinterOn behavior.
Enable User Sync	When enabled, indicates that PrinterOn will synchronize user information in the PrinterOn user store with the Azure AD user store. The **User Sync Interval** setting appears, letting you set how often, in minutes, PrinterOn synchronizes the user data. For more information, see How synchronization settings affect PrinterOn behavior.
Enable Configuration Manager Access	When enabled, allows users to log into configuration manager by authenticating against the Azure AD service.

3. In the **Authentication Behavior** panel, configure the following settings as necessary:

    *   **Guest Login Enabled**: When enabled, specifies that unauthenticated users are permitted to print. When guest login is enabled, you must also configure guest identification and designate one or more printers as guest printers. For more information, see Configuring guest printing.

    *   **Trusted Application Behavior** (Advanced view only): Defines the minimum authentication requirements for users printing through the Print Delivery Gateway (PDG) using the Google Cloud Print workflow. For more information, see Configuring authentication requirements for Google Cloud Print users.

4. Click **Apply Settings**.

7.5.1.1 How synchronization settings affect PrinterOn behavior

When using Azure AD for authentication, the PrinterOn Server uses its internal user store to control access to PrinterOn resources. As a result, PrinterOn needs to populate its internal user store with data from the Azure AD user store. Two settings let you control how data from your Azure AD user store is synchronized with the PrinterOn user store:

- **Enable Group Sync**: Lets you control how PrinterOn synchronizes user group information between the PrinterOn user store and the Azure AD user store.
- **Enable User Sync**: Let's you control how PrinterOn will synchronize user information in the PrinterOn user store with the Azure AD user store.

How you configure each of these settings in combination affect the behavior of PrinterOn. The following table illustrates how the PrinterOn behavior changes based on how you configure these settings.

Group Sync	User Sync	PrinterOn Behavior
Enabled	Enabled	PrinterOn automatically downloads all user data and group data from the Azure AD user store.
		Users do **not** need to authenticate before using Web Print or Email Print workflows. Users must authenticate before using other print workflows.
Disabled	Disabled	PrinterOn uses Just-in-Time provisioning to populate the user store; when a user logs in for the first time, their user data is added to the PrinterOn user store.
		Group data is never added to the user store. As a result, access control rules can only be applied to individual users, not groups.
		Because Google Cloud Print and Email User Lookup have no means of asking for credentials, the user must log in once before these features will work.
Enabled	Disabled	PrinterOn automatically downloads only group data from the Azure AD user store. User data is populated as each user logs in for the first time.
		Because Google Cloud Print and Email User Lookup have no means of asking for credentials, the user must log in once before these features will work.

Group Sync	User Sync	PrinterOn Behavior
Disabled	Enabled	PrinterOn automatically downloads only group data from the Azure AD user store. User data is populated as each user logs in for the first time. Group data is never added to the user store. As a result, access control rules can only be applied to individual users, not groups. Because Google Cloud Print and Email User Lookup have no means of asking for credentials, the user must log in once before these features will work.

7.6 Configuring PrinterOn to authenticate against a third-party Identity Management Service

You can configure PrinterOn to use a third-party Identity Management Service (IDM), such as Ping Identity, Okta, or iWelcome, as the authenticator for your PrinterOn service. Third-party IDMs sit in the cloud, external to the PrinterOn service. As a result, when a user must authenticate, the PrinterOn Server redirects them to an external URL—hosted by the IDM—where the user can supply their credentials.

If the user is successfully authenticated, the IDM creates a user token that PrinterOn uses as confirmation that the user is authorized to access the PrinterOn service. Each subsequent time the user attempts to use a protected printer, PrinterOn checks with the IDM to determine whether the user token is still valid. If so, the user remains authenticated. Otherwise, the user must re-authenticate.

User credentials are submitted to the IDM. PrinterOn never requests the user's credentials directly.

When using a third-party IDM for authentication, the PrinterOn Server uses its internal user store to control access to PrinterOn resources. User data is downloaded from the IDM to the PrinterOn user store, where you can create access control rules.

With most IDMs, PrinterOn uses Just-In-Time provisioning; the first time users authenticate against your identity management service to use the PrinterOn service, a copy of their user details are provisioned to the PrinterOn user store. Group data is not downloaded. You'll need to manually create groups in the PrinterOn user store.

To configure PrinterOn to use a third-party IDM, you'll need to complete the following tasks:

1. Register your PrinterOn service with your IDM service. This registration creates a bond of trust between the PrinterOn server and your service.

2. Supply the PrinterOn Server with your IDM communication information. To allow PrinterOn to successfully redirect users and to synchronize data from the Azure AD user store, you need to provide PrinterOn with your IDM network and security information.

3. Configure the PrinterOn user store to create user groups and Access Control Rules as necessary.

7.6.1 Configuring the Identity Management Service communication settings

To configure the communication settings to allows PrinterOn to authenticate against your third-party identity management service:

1. On the **Authentication** tab, select **Third-Party Identity Management Service** as your Authentication method. The **Third-Party Identity Management Service** panels appear.

2. In the **Third-Party Identity Management Service** panel, configure the communication settings as necessary.

Setting	Description
Service Type	Specify the specific OpenID variant used by the IDM. • For most IDMs, you should select **Generic OpenID Connect**. • If you are using Google Identity Platform, select **Google OpenID Connect**. **Note:** Google Identity Platform is not a fully supported IDM; however, it is currently in Beta.
Authentication Endpoint	The URL hosted by the Identity Management Service to which the PrinterOn server redirects user for authentication. If the user is successfully authenticated, the Identity Management Service returns an authorization code to PrinterOn, which informs the PrinterOn service that the user has successfully authenticated and is authorized to access the PrinterOn service.
Token Endpoint	The URL hosted by the IDM from which the PrinterOn server requests Access, ID, and Refresh tokens. The PrinterOn Server uses these tokens to determine the authentication status of the user. If the credentials have expired, the user is forced to re-authenticate.
User Information Endpoint	The URL where PrinterOn can access user profile information, such as their email address. PrinterOn downloads this user data to the PrinterOn user store the first time a user logs in.
Client ID	The unique ID of the PrinterOn service, generated when you registered PrinterOn with your IDM. Depending on the service you are using, this value may be automatically generated by the IDM, or you may enter your own Client ID value. The PrinterOn Server requires this value to authenticate with the IDM.
Client Secret	The unique client secret key for your PrinterOn service. You must generate this key in your IDM and copy the value to this field. The PrinterOn Server requires this value to authenticate with the IDM.

Setting	Description
Preferred User ID Claim *(Advanced view only)*	The identifying information that PrinterOn requires from the user when authenticating against the IDM. This value is optional. If you define a value for this field (for example email address), then users would be required to supply that value to be authenticated. If you leave this field blank, by default PrinterOn requires the Preferred Username claim from the user to authenticate them.
Scope	The scope of information collected about a user during authentication, such as their email, username, and so on. In almost all cases, you should set **Scope** to a value of **openid email profile offline_access**. This value permits PrinterOn to collect only the minimum necessary user information required.
Suppress Scope for Code Flow	When checked, the scope is not passed on when the PrinterOn server requests a refresh token for the user. Because the user has previously been authorized with a specified scope, the scope is unnecessary for the IDM to issue a refresh token. Most IDMs simply ignore the scope in any refresh request. However, some IDMs will reject a refresh request if it includes scope values, essentially revoking authorization for the user. In these cases, you can enable this setting to prevent the PrinterOn server from including the scope in the refresh request.
Echo Refresh Token for Clients *(Advanced view only)*	When checked, the PrinterOn server returns the refresh token that was included in a refresh request. Before performing a time-intensive task, the PrinterOn server preemptively submits a refresh request, to ensure that the user's authorization remains valid for the duration of the task. In most cases, IDMs either issues a new refresh token to the PrinterOn server, or it returns a the same refresh token. The PrinterOn server then returns the response to the client app that made the request. However, some IDMs do not return any token if the provided refresh token is still valid. This can cause issues for some client apps, since the apps may expect a refresh token in the response. To mitigate any issues that may occur in such a scenario, you can check this setting to ensure that the client app receives the expected token in the response.

Setting	Description
Prompt *(Advanced view only)*	A message PrinterOn displays to the user to allow them to grant permission for PrinterOn to authenticate them. Some Authentication services require a user's consent to allow PrinterOn access to the service on their behalf. This message will be used to prompt the user for confirmation when necessary.
Resource *(Advanced view only)*	The resources or APIs that are being authorized for use. Typically, this field can be left blank.
Resource Owner Password Flow Supported	When checked, the IDM allows PrinterOn to collect the user password and pass it on to the Identity Management Service, instead of redirecting the user to the Authentication URL to supply their credentials.
Enable Configuration Manager Access	When enabled, allows users to log into configuration manager by authenticating against the Identity Management Service.

3. In the **Authentication Behavior** panel, configure the following settings as necessary:

    - **Guest Login Enabled**: When enabled, specifies that unauthenticated users are permitted to print. When guest login is enabled, you must also configure guest identification and designate one or more printers as guest printers. For more information, see Configuring guest printing.

    - **Trusted Application Behavior** (Advanced view only): Defines the minimum authentication requirements for users printing through the Print Delivery Gateway (PDG) using the Google Cloud Print workflow. For more information, see Configuring authentication requirements for Google Cloud Print users.

4. Click **Apply Settings**.

You can now access the Users tab to create user groups and Access Control Rules. For more information, see Managing the PrinterOn user store.

7.7 Configuring PrinterOn to authenticate using AAA Login

The PrinterOn AAA Login authentication method uses a designated web service to perform user authentication. When enabled, all other authentication methods are deactivated.

> **Note:**
>
> • To use this authentication method, you must integrate with PrinterOn's Job Accounting API.
>
> • When using AAA Login authentication, the authentication service must not reside on a host that resolves to an IPv6 address. PrinterOn does not yet support IPv6 for this feature.

To configure the authentication behavior for an AAA Login:

1. On the **Authentication tab**, select **AAA Login (Custom)** as your Authentication method. The **Custom User Authentication Settings** panel appears.

2. In the **User Authentication URI** field, specify the URL of the web service performing the authentication. The PrinterOn Server redirects users to this URL during login.

> **Note:**
>
> • This authentication scheme must be configured in conjunction with PrinterOn's hosted configuration interface.
>
> • PrinterOn does not support IPv6 for this field. The authentication service must not reside on a host that resolves to an IPv6 address.

3. In the **Authentication Behavior** panel (visible only when Advanced Settings is enabled), configure the following settings as necessary:

   • **Guest Login Enabled**: When enabled, specifies that unauthenticated users are permitted to print. When guest login is enabled, you must also configure

guest identification and designate one or more printers as guest printers. For more information, see Configuring guest printing.

- **Trusted Application Behavior** (Advanced view only): Defines the minimum authentication requirements for users printing through the Print Delivery Gateway (PDG) using the Google Cloud Print workflow. For more information, see Configuring authentication requirements for Google Cloud Print users.

4. Click **Apply Settings**.

7.8 Configuring PrinterOn to authenticate for Web Print workflow only

If users will only be printing using the Web Print workflow, you can configure your PrinterOn server to use web-based, single sign-on authentication.

To configure PrinterOn to web-based single sign-on for authentication:

1. On the **Authentication** tab, select **Web Print Only - Single Sign-on** as your Authentication method. The **Authentication Behavior** panel appears.

2. In the **Authentication Behavior** panel, configure the following settings as necessary:

- **Guest Login Enabled**: When enabled, specifies that unauthenticated users are permitted to print. When guest login is enabled, you must also configure guest identification and designate one or more printers as guest printers. For more information, see Configuring guest printing.

- **Trusted Application Behavior** (Advanced view only): Defines the minimum authentication requirements for users printing through the Print Delivery Gateway (PDG) using the Google Cloud Print workflow. For more information, see Configuring authentication requirements for Google Cloud Print users.

3. Click **Apply Settings**.

7.9 Configuring PrinterOn to authenticate using ACL

The PrinterOn Access Control Login (ACL) authentication method authenticates the user's login information against PrinterOn's user database during printing. You can manage users in the PrinterOn user database at the PrinterOn.com web admin portal at www.printeron.com/administrators.

> **Note:** The PrinterOn Access Control Login (ACL) authentication method is only available when you have deployed PrinterOn in Hybrid mode.

When enabled, all other authentication methods are deactivated.

To configure the authentication behavior for PrinterOn ACL Login:

1. On the **Authentication** tab, select **PrinterOn ACL** as your Authentication method. The **PrinterOn Access Control Settings** panel appears.

2. In the **Authentication Behavior** panel, configure the following settings as necessary:

   • **Guest Login Enabled**: When enabled, specifies that unauthenticated users are permitted to print. When guest login is enabled, you must also configure guest identification and designate one or more printers as guest printers. For more information, see Configuring guest printing.

   • **Trusted Application Behavior** (Advanced view only): Defines the minimum authentication requirements for users printing through the Print Delivery Gateway (PDG) using the Google Cloud Print workflow. For more information, see Configuring authentication requirements for Google Cloud Print users.

3. Click **Apply Settings**.

7.9.1 Managing PrinterOn user accounts on the web portal

If you have installed PrinterOn in a hybrid deployment, in which some components are installed within your organization and others are hosted externally, the PrinterOn ACL authentication method is available.

This authentication method allows you to control access to printers by creating Access Control Lists (ACLs) on the PrinterOn admin web portal, then attaching printers and adding users to that ACL. Users added to the ACL are granted permission to access any of the printers attached to that ACL.

To manage user accounts:

1. Log in to the PrinterOn.com web portal at www.printeron.com/administrators.
2. On the Home page, choose **Manage Access Control Lists**. The Access Control Lists page appears.

3. In the **New ACL Name** field, specify the name of your Access Control list, then click **New ACL**. The ACL is added to the list above.

    Each printer can have a unique list of users. Users can be repeated to allow access to multiple printers, or you can choose to group printers by departments.

4. Select your ACL in the list, then click **Manage Printers**. The Manage Printers page appears.

Name: Reception

Messages:

Available Printers	Attached Printers
company-sales	company-reception

Add >>

<<Remove

Cancel   Save

5. Attach printers to the ACL by moving them from the Available Printers list to the Attached Printers list. All users added to the ACL will have access to the attached printers.

6. Click **Save**.

7. Select your ACL in the list, then click **Manage Users**. The Manage Users page appears.

Name: Reception

Messages:

Attached Users
sales@company.com
reception@company.com

Remove

info@company.com   Add User

Add a Filter   Add Filter

Cancel   Save

8. Click **Add User** to and add individual user email addresses. When users are added, they receive an automated message requesting them to create a password with PrinterOn. This password is used to authenticate print requests.

    > **Note:** Print jobs submitted via email must be sent from the address specified here.

    Messages:

Access Control Lists		
Name	# of Users	# of Printers
Sales Dept.	3	1
Reception	2	1

    New ACL Name   **+   New ACL**

    Manage Users   Manage Printers   **−   Delete ACL**

9. Click **Save**.

7.10 Configuring guest printing

For whichever authentication method you configure PrinterOn to use, you can also enable guest login, which permits unauthenticated users access to some printing services.

Configuring guest printing is a two-part process:

1. Configure the guest login settings by enabling guest login for your selected authentication method and configuring how guest users are identified for reporting and tracking purposes.

2. Designate printers as guest printers that can accept print requests form guests.

7.10.1 Configuring guest login settings

The PrinterOn Server can control how guest users (that is, users who have not unauthenticated) are identified when reporting and integration with output/print management solutions.

To configure the guest workflow:

1. In the Configuration Manager, click **Authentication**. The Authentication tab appears, displaying the configuration for your selected authentication method.

2. In the **Authentication Behavior** panel, check **Guest Login Enabled**.

3. Click **Manage Guest Settings**. The Guest Settings dialog appears.

4. In the Guest Settings dialog, specify the **Guest Behavior**. You can choose one of the following behaviors:

    *   **Do Nothing**: The job owner name for all guest jobs is set to GuestUser.

    *   **Default User ID**: The job owner name for all guest job submissions is set to the value you specify in the **Guest User ID** field. The Guest User ID is used for all Guest Users and is the same for all workflows. This value is also delivered to third-party solutions, and appears in the PrinterOn Reports.

    *   **Prompt**: The user is prompted to supply the name to use as the job owner. When you select **Prompt**, you can define the following settings:

Setting	Description
Prepend Guest User ID	All guest jobs are prepended by the value set in this field. If left blank, nothing is perpended to the ID that the user defines.
Ensure User ID is unique	When checked, the PrinterOn Server verifies that the username supplied by the guest user does not match any existing usernames within the LDAP/AD structure.

5. Click **Apply Settings** to close the Guest Settings dialog.

6. Click **Apply Settings**.

7.10.2 Designating a printer as a guest printer

You can configure which of your printers are classified as Guest printers.

> **Note:** Before you can designate a printer as a guest printer, you must first complete the steps in Configuring guest login settings.

To designate a printer as a guest printer:

1. In the Configuration Manager, click **Printers**. The Printers tab appears.

2. Enable guest printing for a printer by toggling the setting in the **Guest** column from a ⊗ to a ✓.

> **Note:** The **Guest** column only appears in the Printers List if you have enabled the **Guest Login Enabled** setting for your Authentication method. For more information, see Configuring guest login settings.

7.11 Configuring authentication requirements for Google Cloud Print users

For users printing through Google Cloud Print, you can control the minimum access rights required for the print job to be accepted.

The Trust Application Behavior setting, available in Advanced view,

1. In the Configuration Manager, make sure that Advanced view is on.

2. Click **Authentication**. The Authentication tab appears, displaying the configuration for your selected authentication method.

3. In the **Authentication Behavior** panel, from the **Trusted Application Behavior** drop-down, choose how you want the PrinterOn Server to handle print jobs

submitted using the Google Cloud Print workflow. You can choose from the following values:

Value	Description
Allow All	Accepts all print requests from the Google infrastructure.
	Identified users and unidentified users can access both Guest and non-Guest printers without restriction. Any configured access rules are ignored.
Reject All	Rejects all print requests. Disables submission of print jobs through the Google infrastructure to PrinterOn printers.
Authenticated	Accepts print requests submitted by identified users who can be authenticated against the selected authentication method. If the user store includes information pertaining to Google Cloud Accounts, then the administrator can control access to printers.
	Any configured LDAP/AD access rules or PrinterOn access rules are respected.
	Unidentified users are not permitted to print, even to Guest printers.
Authenticated and Guest	Accepts print requests submitted by identified users who can be authenticated against the selected authentication method, as well as those who are unidentified users in the context of PrinterOn printers.
	Any configured access rules are respected.

4. Click **Apply Settings**.

8

Managing the PrinterOn user store

PrinterOn includes its own user store that you can use as for identity management and access control. The PrinterOn user store lets you manage users, organize them into groups, and create access control rules to manage access to PrinterOn resources. You can manage the PrinterOn user store from the Users tab in the Configuration Manager.

The PrinterOn user store is used to store user data in conjunction with the **Internal Users**, **Azure AD**, and **Third-Party Identity Management Service** authentication methods. The Users tab is only accessible when one of these authentication methods is selected on the Authentication tab. For more information on configuring these authentication methods, see Configuring authentication settings.

- For **Internal Users** authentication, the PrinterOn user store is the sole repository for user information; you must create the user accounts, user groups, and access rules yourself.

  > **Note:** PrinterOn supports the bulk import of users into the PrinterOn user store. For information on importing, see Importing users into the PrinterOn user store.

- For **Azure AD** and all **Third-Party Identity Management Services** (IDM), user accounts are created in your IDM's user store, and then provisioned to the PrinterOn user store. PrinterOn synchronizes its user store with the IDM's user store at regular intervals.

  All authentication is performed against the IDM's user store. The PrinterOn user store is only used for controlling access to PrinterOn resources; you'll need to create access control rules and, if necessary, user groups, in the PrinterOn user store.

To access the PrinterOn user store:

1. In the Configuration Manager, click **Users**. The Users tab appears.
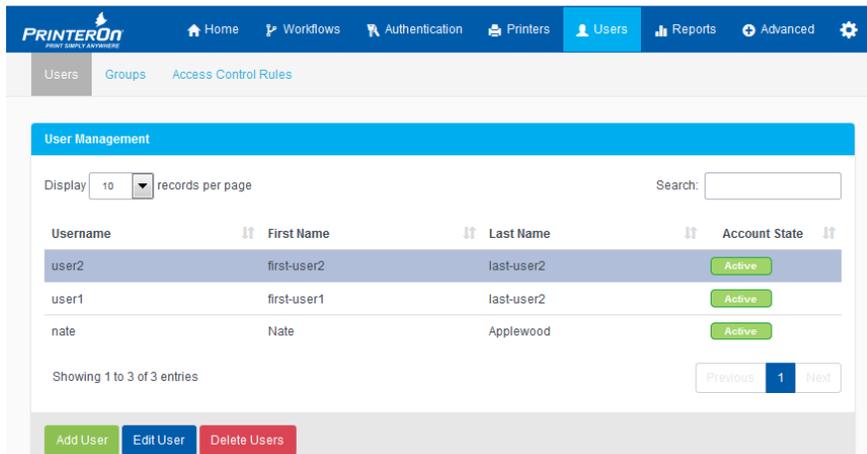
2. Create and manage the user store data as necessary.

    • Creating and managing user accounts.

    • Creating and managing PrinterOn groups.

    • Creating and managing PrinterOn Access Control Rules.

8.1 About the PrinterOn user store

The PrinterOn user store is used to store login and access information about users of the PrinterOn service. The user store stores three types of data:

Data type	Description
User	An individual who administers or uses the PrinterOn service. A user can be added to one or more user groups and assigned to one or more access control rules. For more information on managing users, see Creating and managing user accounts.For information on importing multiple users into the PrinterOn User Store, see Importing users into the PrinterOn user store.

Data type	Description
User Group	A collection of users. You can group users in any logical way; for example, by department, by geographic location, or some other criteria.
	You can assign a group to one ore more access control rules.
	For more information on managing user groups, see Creating and managing PrinterOn groups.
Access Control Rule	A set of privileges that you can grant to a user or user group for a specific object (for example, a printer or printer department) to define what parts of the PrinterOn service the user or group can access.
	Privileges are granted by assigning a role to the user or user group for a particular object (for example, a printer, or printer group).
	For more information on managing access control rules, see Creating and managing PrinterOn Access Control Rules.

8.2 Creating and managing user accounts

The Users tab lets you add, view, or modify the accounts of users with access to the PrinterOn service.

The PrinterOn user store is also used if you are using LDAP/AD, Azure AD or another third-party identity management service. The first time users access the PrinterOn service by authenticating against your identity management service, a PrinterOn account is created for them in the PrinterOn user store and a copy of their user details are provisioned to it.

Note: You can also choose to pre-emptively bulk import the data of all your users into the PrinterOn user store without requiring them to log into the service by using a CSV file. For more information, see Importing users into the PrinterOn user store.

Once a user is added to the PrinterOn user store, you can create a printer policy for them, add them to groups or assign access control rules to manage their access to the PrinterOn service.

To manage user accounts:

1. In the Configuration Manager, click **Users**. The Users tab appears.
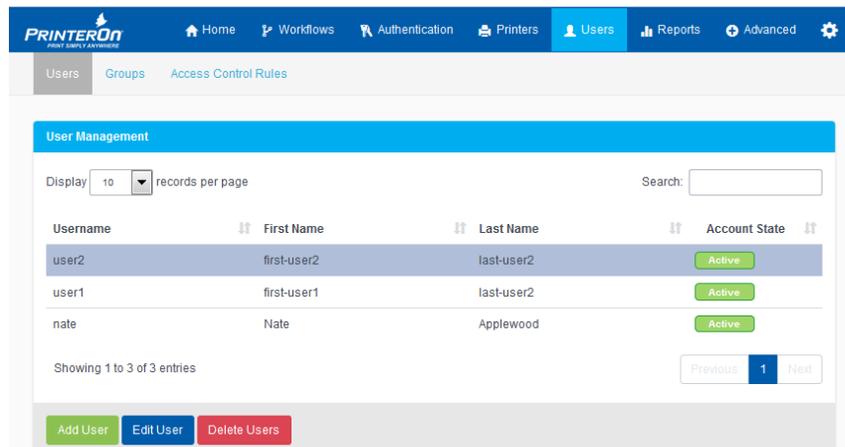
2. Perform one of the following tasks:

   • Add a new user account.

   • Edit an existing user account.

   • Create a printer policy for the user.

   • Delete a user account.

8.2.1 Adding PrinterOn user accounts

If you are using the PrinterOn Internal Users authentication method, you'll need to create PrinterOn accounts for each user who will be accessing the PrinterOn service.

Note: If you are using Azure AD or another third-party IDM service, user account information is provisioned to the PrinterOn user store when a user authenticates to use the service for the first time. You don't need to manually add or import users.

You can also import multiple users into the PrinterOn user store at once using a CSV file. For more information, see Importing users into the PrinterOn user store.

To add new PrinterOn user accounts to your service:

1. In the Configuration Manager, click **Users**. The Users tab appears.

2. Click **Add User**. The Add User dialog appears.

3. Define the following settings for the user as necessary:

Setting	Description
User Name	The name with which the user signs into PrinterOn service. If the user is an administrator, this is also the name with which they sign into the Configuration Manager.
Password, Confirm Password	The password the user uses to sign into the PrinterOn service.
First Name, Last Name	The name of the user.
Alias	An alternate name for the user.
Expiry Date	The date on which the user's access permissions expire.
Emails	The email address associated with this user account. Click + to display additional fields so you can associate multiple email addresses with the account.
Description	An optional description of the user.

4. If you choose, create a printer policy for the user.
5. Click **Save**.

8.2.2 Editing user account information

You may need to modify an existing account on occasion, for example, to reactivate a disabled account, or change other user information.

To edit a user account:

1. In the Configuration Manager, click **Users**. The Users tab appears.
2. In the User Management panel, select the user account that you need to modify, then click the adjacent **Edit** button.

> **Hint:** To filter the list of users, begin typing the user's alias, first name, or last name in the **Search** field.

3. The Edit User panel appears.
4. Modify the settings as necessary:

Setting	Description
User Name	The name with which the user signs into PrinterOn service. If the user is an administrator, this is also the name with which they sign into the Configuration Manager.
Password, Confirm Password	The password the user uses to sign into the PrinterOn service.
First Name, Last Name	The name of the user.
Expiry Date	The date on which the user's access permissions expire.
Emails	The email address associated with this user account. Click + to display additional fields so you can associate multiple email addresses with the account.
Description	An optional description of the user.

5. If you choose, create or modify the printer policy for the user.
6. Click **Save**.

8.2.3 Creating a printer policy for a user

A printer policy allows you to define some user-specific default values for commonly set print options that override the default value assigned to the printer. You can assign a printer policy for any user who is likely to commonly select the same setting values for their print jobs, preventing them from having to change the printer default each time they print.

For example, to reduce paper usage, you may configure your organization's printer to print double-sided by default. However, you may have a user whose printing needs are predominantly for printing labels, which need to be printed single-sided since they are affixed to a package. To prevent that user from having to change the duplex setting every time they print, you can create a printer policy for them to set their personal default duplex value to single-sided.

To create a printer policy:

1. Add or edit a user as necessary.
2. In the Add or Edit User dialog, expand the Printer Policy panel to display the printer policy options.
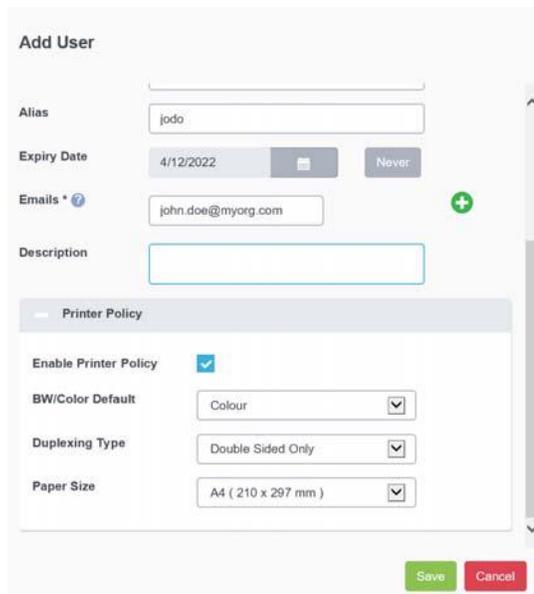
3. To enable the policy for the user, check **Enable Printer Policy**.

4. Define a default value for the user for one or more of the following printer output settings:

- B&W/Color Default: Choose between **B&W** or **Color**. If the printer does not support the selected value, the printer's default value is used.

- Duplex Type: Choose a duplex option, or select Not managed to use the printer's default duplex type.

- Paper Size: Choose a paper size. If the printer does not support the selected paper size, the printer's default paper size is used.

5. Click **Save**.

8.2.4 Deleting a user account

To delete a user account:

1. In the Configuration Manager, click **Users**. The Users tab appears.

2. In the User Management panel, select the user account that you need to modify, then click the adjacent **Delete** button.

> **Hint:** To filter the list of users, begin typing the user's alias, first name, or last name in the **Search** field.

8.3 Creating and managing PrinterOn groups

A group is a collection of users. You can group users in any logical way; for example, by department, by geographic location, or some other criteria.

The PrinterOn user store is also used if you are using Azure AD or another third-party identity management service. When users authenticate against your identity management service, a copy of their user details are provisioned to the PrinterOn user store.

Once a user is added to the PrinterOn user store, you can add them to groups or assign access control rules to manage their access to the PrinterOn service.

To manage user accounts:

1. In the Configuration Manager, click **Users**. The Users tab appears.
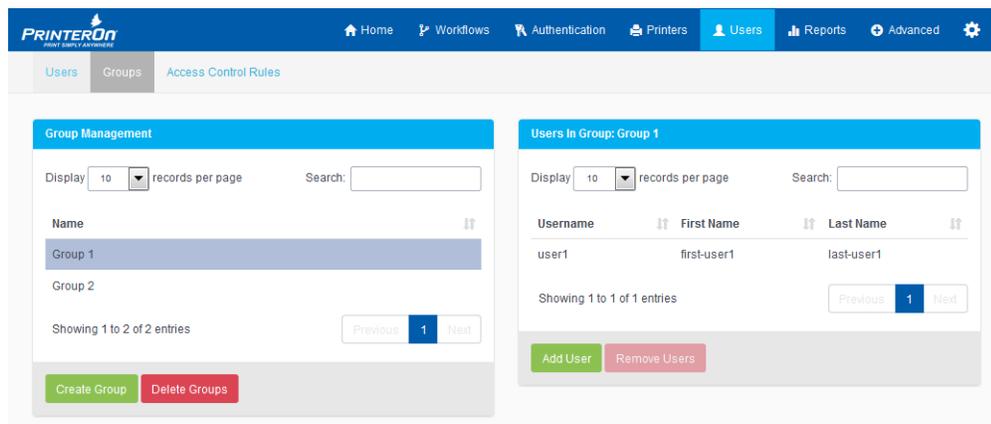
2. Perform one of the following tasks:

   • Add a new PrinterOn user group.

   • Modifying the users assigned to a group.

   • Delete a user group.

8.3.1 Adding a user group

To add a new PrinterOn user group to your service:

1. In the Configuration Manager, click **Users > Groups**. The User Groups tab appears.
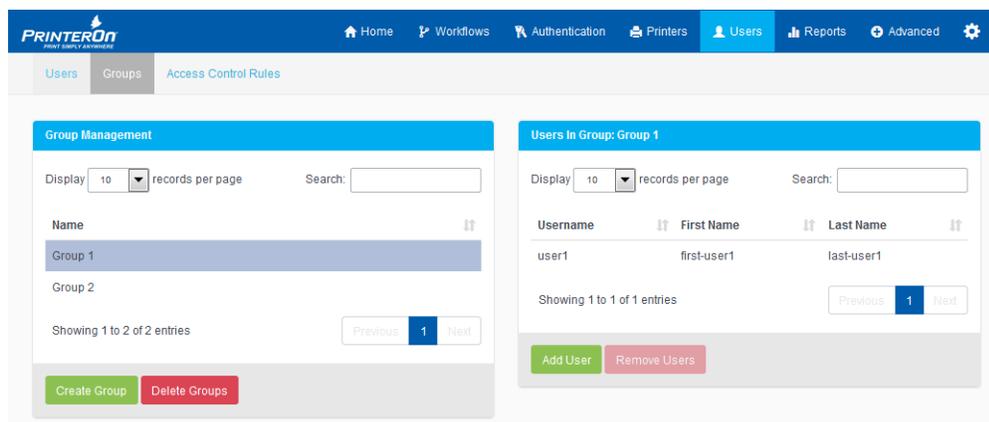
2. In the Group Management panel, click **Create Group**. The Create Group dialog appears.
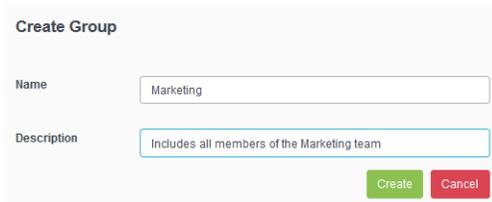
3. Specify a **Name** and **Description** for the user group
4. Click **Save**.
5. Configure which users are assigned to the group as necessary.

8.3.2 Managing the list of users in a user group

You can modify which users are in a user group at any time.

To modify the list of users in a group:

1. In the Configuration Manager, click **Users** > **User Groups**.
2. In the Group Management panel, select the group that you want to add users to. The Users in Group panel appears.

> **Hint:** To filter the list of groups, begin typing the group name in the **Search** field.

3. To add users:

    a) In the Users in Group panel, click **Add User**. The Add User to Group dialog appears, containing a list of all available users not already added to the group.
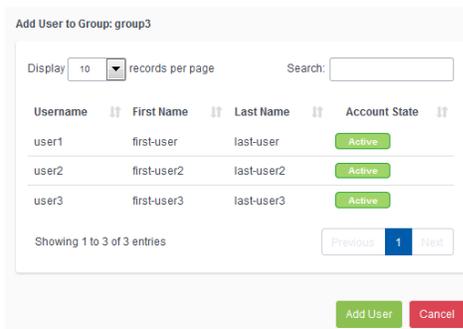
b) Select the group user(s) that you want to add to the group.

> **Hint:** To filter the list of users, begin typing the username in the **Search** field.

- Press **Ctrl** to select multiple users.
- Press **Shift** to select multiple sequential users.

c) Click **Add User**.

4. To remove users:

a) In the Users in Group panel, select the user(s) you want to remove from the group.

> **Hint:** To filter the list of users, begin typing the username in the **Search** field.

- Press **Ctrl** to select multiple users.
- Press **Shift** to select multiple sequential users.

b) Click **Remove Users**.

8.3.3 Deleting groups

To delete groups:

1. In the Configuration Manager, click **Users**. The Users tab appears.
2. In the User Management panel, select the group(s) that you want to delete.
   - Press **Ctrl** to select multiple users.
   - Press **Shift** to select multiple sequential users.
3. Click the **Delete Groups** button.

8.4 Creating and managing PrinterOn Access Control Rules

Access control rules allow you to control the level of access a user or group of users has to the PrinterOn service. Access is controlled by assigning a role (that is, a set of privileges), to a user or user group, for a particular component object of the PrinterOn service (for example, a printer or printer department).

Privileges are granted by assigning the user or group to one of the following roles:

- **User**: Permits use-only access to an object. For example, a user can print to a printer.

- **Administrator**: Permits full administrative access to Configuration Manager.
- **Printer Admin**: Limits administrative access to Configuration Manager to the configuration and management of printers.
- **Report Admin**: Limits administrative access to Configuration Manager to the generation of reports and audit trail management.
- **User Admin**: Limits administrative access to Configuration Manager to the creation and management of PrinterOn user accounts, groups, and access control rules.

> If a user is part of two or more access control rules that grant different levels of access for the same object, the rule that grants them the most privileges takes precedence.

If you are using the Internal Users, Azure AD, or some other third-party identity management service, you'll need to manually define Access Control Rules for your users.

By default, with no access control rules set up, all users are granted User privileges to all printers.

8.4.1 Defining an Access Control Rule

To define an Access Control Rule:

1. In the Configuration Manager, click **Users > Access Control Rules**. The Access Control Rules tab appears.
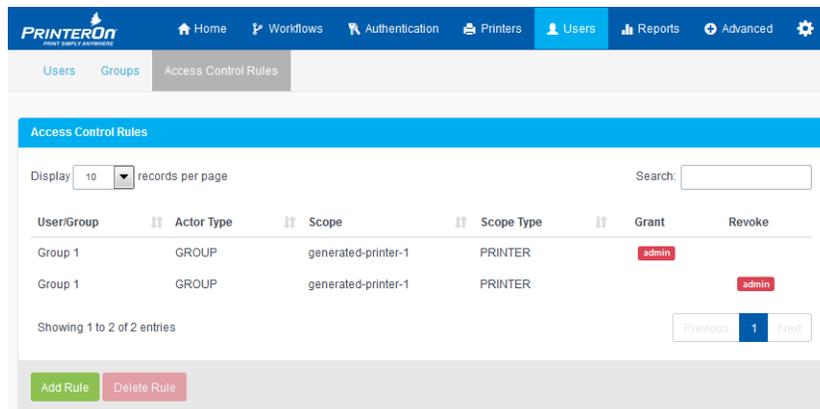
2. Click **Add Rule**. The Add Rule dialog appears.
3. In the Add Rule dialog, provide a **Name** for the new rule.

4. In the **Assign this Role** field, choose one of the following roles:

Role	Description
Administrator	Administers the entire PrinterOn configuration. This role can access all features and capabilities of the Configuration Manager, with no limitations or restrictions.
Printer Admin	Administers PrinterOn printers. This role can perform any task related to a printer, for example, changing the printer configuration or adding the printer to a department.
Reports Admin	Administers reporting functionality within the system. This role can generate reports and manage audit trail data for the service.
User Admin	Administers user accounts in the PrinterOn user store. This role can add or remove user accounts, add accounts to groups and create access control rules and assign them to users and groups.
User	A printing-specific role that can be assigned to any user to allow them to print using the PrinterOn service.

5. In the **To this User/User Group** field, choose which user or user group you want to assign the selected role to.

6. In the **For this Object** field, choose which object you want to give the user or user group access to.

7. Click **Save**.

8.4.2 Deleting Access Control Rules

To delete an Access Control Rule:

1. In the Configuration Manager, click **Users** > **Access Control Rules**. The Access Control Rules tab appears.

2. Select the rule(s) that you want to delete.

    *   Press **Ctrl** to select multiple rules.

    *   Press **Shift** to select multiple sequential rules.

3. Click the **Delete Rule** button.

9

Integrating user lookup extensions

The Integration tab contains advanced integration capabilities that you can configure to allow PrintAnywhere Server to identify users. You can choose between the following integration extensions:

- **User Lookup**: The PrintAnywhere server uses the user's email address to query an identity management service (IDM) to determine the user's domain account user ID. The IDM can be local (an LDAP/AD server or the PrinterOn User Store) or a third-party identity management service (Microsoft Azure, Ping)

  If you select **User Lookup**, you'll need to configure the lookup rules for both identified and unidentified users. For more information, see Configuring User Lookup integration.

- **User ID from Email Address**: The PrintAnywhere server extracts the user ID from the user's email address. No additional configuration is required.

9.1 Configuring User Lookup integration

User Lookup integration is typically used when also integrating your service with a third-party print management server. With User Lookup integration, the PrintAnywhere server searches for user account information in the identity management service you have configured to authenticate and authorize users.

When a user (typically an email print user) submits a job to PrintAnywhere, the PrintAnywhere server uses the user's email address to query the IDM to locate the user's

domain account name. The PrintAnywhere server then associates the print job with the domain account.

This information also allows you to define behavior for identified and unidentified users.

To configure user lookup integration:

1. In the Configuration Manager, click **Authentication** > **Integration**.
2. In the **Integration Type** drop-down, select **User Lookup**. The User Lookup and User Lookup Rules panels appear.
3. Configure the User Lookup settings.
4. Configure the User Lookup Rules. You can define different user lookup rules for each type of user to specify how the PrintAnywhere processes jobs in each case.
5. Click **Apply Settings**.

9.1.1 Configuring the User Lookup settings

To configure the User Lookup Settings:

1. In the User Lookup panel, select **Enable User Lookup**.
2. Click **Edit** to define the Service API configuration. The User Lookup Settings dialog appears.
3. Configure the following settings:

Setting	Description
Domain Filter	A semicolon-separated list of email domain(s) for which the PrintAnywhere server will search the IDM service. For example: printer.com;printeron.net Users submitting jobs from email addresses from the specified email address domains are looked up in the IDM, and if found, treated as iIdentified users. Users whose email domains are not included in the list are treated as Unidentified users.
API Lookup URL	The URL of the server that is hosting the user lookup API. Typically this is the CPS server installed with your PrinterOn Server. The default URL is: http://localhost/cps/cpsapi

Setting	Description
API Username	A valid username configured in the CPS server for use with the API. The **username** must be configured on your CPS server prior to using the API.
API Password	A valid password associated with a username configured in the CPS server for use with the API. The **password** must be configured on your CPS server prior to using the API.
API Key	A valid API key created in the CPS server for use with the API. The combination of the **username**, **password**, and **API key** is used to ensure that only valid and authorized clients can use the API.
Email Address	An email address to validate the lookup configuration. Enter an email address and an optional printer, then click **Test** to see whether a successful connection was established and whether the email address was located.
Printer (Optional)	A printer ID to validate the lookup configuration. Enter an email address and the name or number of a printer, then click **Test** to see whether a successful connection was established and whether the printer was located.

4. Click **Test** to test the configuration.

5. When you have confirmed the lookup settings are correctly configured, click **Apply Settings**.

9.1.2 Configuring the behavior for identified and unidentified users

Users may be classified as either Identified or Unidentified:

- An *Identified User* is one that can be located using the User Lookup API. To be classified as an Identified User, the API must successfully respond and provide a valid username for the user. When a user is identified, the job owner information for the print job is set to the retrieved username.

  > **Note:** Typically, identified users can only print to non-guest printers.

- An *Unidentified User* is any user for which the server cannot locate a username associated with the user's email address.

  > **Note:** Typically, unidentified users can only print to guest printers.

> **Note:** When using Google Cloud Print or PQMS, and the **Trusted Application Behavior** setting can override the typical behavior for identified and unidentified users. If **Trusted Application Behavior** is set to **Allow All**, any user type can access any printer type. See Configuring authentication requirements for Google Cloud Print users for more information.

You can define different user lookup rules for each type of user to specify how the PrintAnywhere processes jobs in each case.

When configuring behavior for a type of user, you can also configure behavior specific to either Guest printers or non-Guest printers. For example, you may choose to reject jobs submitted by identified users to Guest printers, but to accept jobs submitted by unidentified users.

To configure the processing behavior for each user type:

1. In the **User Lookup Rules** panel, click the **Identified Users** sub panel. The panel expands to display the **Non-Guest Printers** panel.

2. In the Non-Guest Printers panel, from the **Release Action Mode** drop-down, specify how the server processes jobs from identified users to non-Guest printers.

   > **Note:** When configuring job release behavior, you must ensure your Print Delivery Station is capable and configured to handle managed job behavior.

You can specify one the following behaviors:

Release Action Mode	Description
Default	No overriding action is taken for jobs submitted for this user type; jobs are processed and released as configured for the specific printer. No authentication is performed. **Note:** This option disables Web-Based authentication, if enabled in CPS or PrinterOn's Administration Web Dashboard.
Automatic Release (Override)	Jobs are automatically released from the Print Delivery Station to the configured Print queue. This is the most common configuration when integrating with a third-party print management solution.
Hold in PDS (Override)	Jobs are held by the Print Delivery Station. Users must use a PrinterOn job release solution to access the print jobs.
Reject Jobs	Jobs will be rejected by the server if they are from the specified user type. **Note:** For Unidentified Users, you should choose this setting if you only wish to access jobs from users in your IdM service.
Default – Enable Web Authentication	No overriding action is taken for jobs submitted for this user type; jobs are processed and released as configured for the specific printer. However, users must authenticate themselves before the job is printed. Users will receive an email with a link to the Authentication Server to allow them to provide their credentials.

3. Specify additional behavior for identified users:

   - Whether to return a Release Code to the user.

   - Whether to set the job owner to the PrinterOn generated Privacy Release Code.

4. Click the **Identified Users** sub panel. The panel expands to display the **Guest Printers** panel.

5. Repeat Steps 2-3 to define behavior for unidentified users to Guest printers.

6. In the **Default Failure Action Mode**, specify the behavior of the PrintAnywhere server if it is unable to communicate with the lookup service. If you specify a value of **Off**, all print jobs are rejected.

7. Click **Apply Settings**.

10

Advanced clustering and document processing scalability

You can improve your PrinterOn service's performance and resilience by adding additional PrintAnywhere Processing Server or Status Server components to your deployment and configuring them as clusters. Enabling and configuring basic clustering with the PrinterOn server is simple and can be completed with minimal effort and time. The solution has been designed to minimize configuration and maintenance.

Note: Advanced clustering of PrintAnywhere servers is only available for PrinterOn Enterprise Edition.

Creating a server cluster for document processing provides the following benefits
- Provides additional server capacity and performance.
- Optimizes server utilization by distributing documents across multiple PrintAnywhere components.
- Provides additional redundancy.
- Simplifies maintenance.

10.1 PrintAnywhere Server clustering overview

The PrinterOn Server offers two forms of clustering depending on your deployment needs and requirements:

- Document processor clustering, which increases job processing capacity.
- Advanced redundancy clustering, which provides backup service that helps to simplify service upgrades and to maintain service continuity should issues occur with physical hardware.

10.1.1 Document processor clustering

Basic clustering involves attaching a second PrintAnywhere Processing Server to the primary server's Status Server. The Processing Server is responsible for converting/rendering documents supplied by the user. The Status Server is responsible for distributing jobs across available Processing Servers.

10.1.2 Server redundancy clustering

Server Redundancy Clustering involves installing and associating a second PrintAnywhere Status Server to the primary PrintAnywhere Server's Status Server. The Status Server is responsible for managing incoming job requests and distributing jobs across available Processing Servers to be printed.

10.1.3 Clustering requirements

PrinterOn supports deploying the necessary Document Processing Clustering components on the same physical server as your primary PrinterOn Server using separate virtual machines. This approach allows the deployment to minimize additional costs and yet can still provide the same performance as a separate physical server.

To deploy a cluster, you'll need to meet the following requirements:

- You must have an additional virtual machine prepared with the necessary applications for processing documents.
- The host physical server must have sufficient memory to allocate the minimum recommended memory to each virtual machine.

- Each virtual machine must be addressable on the network, since the Status Server must be able to respond and communicate with each Processing Server and the Processing Server must be able to independently resolve and communicate with the Status Server.

10.1.4 Print job processing in a clustered deployment

When configuring your service for clustering or diagnosing issues, it is useful to understand the behavior of the servers. The following provides a brief overview of the clustering behavior.

- The Status Server delivers jobs to Processing Servers in the order they appear in the Configuration Utility.

- The Status Server delivers new jobs to the least busy server each time a new job arrives. As a result, in a low volume deployment with clustering enabled, the first Processing Server in the list will receive the bulk of the jobs.

- The Processing Server reports its capabilities to the Status Server during a synchronization process. This process:

  - Informs the Status Server which applications and formats are supported by each configured Processing Server.

  - Allows the Status Server to determine whether a Processing Server is running.

  - Occurs every 2 minutes, allowing the Status Server to update its state information when idle.

- Each time a job is submitted or completed, the Processing Server informs the Status Server of its current state, allowing the Status Server to maintain an up to date state of all Processing Servers.

- If a configured Processing Server is not available when the Status Server is started, the Status Server continues to check its status every 2 minutes. When the Processing Server starts, the Status Server automatically detects it and starts delivering print jobs to that server.

- If all Processing Servers in a cluster are unavailable, the Status Server rejects incoming jobs.

10.2 Creating and configuring a server cluster

To create a PrintAnywhere server cluster, you'll need to complete the following tasks:

1. Add a new PrintAnywhere Server instance to your PrinterOn server for each new PrintAnywhere component you intend to install. Adding a new instance creates a new PrintAnywhere serial number. When you install a PrintAnywhere component on a remote server, you'll choose a serial number to assign to that component.

2. Install each new PrintAnywhere Server component on a remote server. Each time you install a PrintAnywhere Server, you'll connect it to one of the serial numbers you received when adding a new instance to your PrinterOn service.

3. Add your PrintAnywhere servers to a cluster.

> **Note:** Because each PrintAnywhere Server is installed on a remote server, you must also ensure that the Internal Service URI value is correctly configured. The Internal Service URI is used by the subcomponents to communicate with the Central Print Services in a distributed deployment.

10.2.1 Adding a new PrintAnywhere Server to your PrinterOn service

To set up a cluster of PrintAnywhere servers, you must have multiple PrintAnywhere servers. Each PrintAnywhere server you deploy must have a unique serial number. You can add a new PrintAnywhere Server to your service and receive the serial number you need.

Once you have a serial number for each PrintAnywhere Server instance you intend to deploy, you can copy the updated license file to your remote servers, install the PrintAnywhere component software on each server, and then configure your server cluster(s).

To add a PrintAnywhere Server instance:

1. Click **Home** > **Serial Numbers**.

2. Scroll to the bottom of the page and click **Add PrintAnywhere Server**.

3. In the Add PrintAnywhere Server dialog, enter the **Server Description**. The server description is used to identify the PrintAnywhere Server, so it should be meaningful.

Add PrintAnywhere Server

Server Description   Remote PrintAnywhere Server 1

Add   Cancel
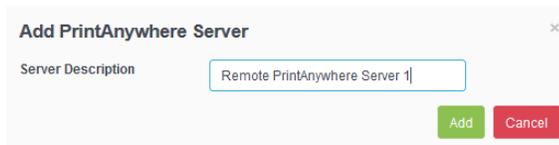
4. Click **Add**. The PrinterOn Server generates a new serial number for an additional PrintAnywhere Server instance.

   Each time you add a new PrintAnywhere instance, the PrinterOn Server adds the new serial number to your license file. When complete, download your updated license and copy it to each server you intend to install a PrintAnywhere Server on.

10.2.2 Installing the PrintAnywhere component on the remote server(s)

Note: Before you install the PrintAnywhere software on a remote server, ensure that you have downloaded your license file on the parent PrinterOn server and copied it to the server on which you are installing the PrintAnywhere component. The installer needs the license files to allow you to associate the installed software with one of your PrintAnywhere Server serial numbers.

To install a PrintAnywhere component:

1. Run **PSIM.exe** to launch the PrinterOn Installation Wizard. The wizard guides you through the installation of the PrinterOn software.

2. Click **Next** at the Welcome screen, then accept the License Agreement to proceed with the installation.

3. On the License Summary File screen, browse to your PrinterOn license file and select it, then click **Next**.

   Note: Ensure that your license file contains multiple PrintAnywhere serial numbers.
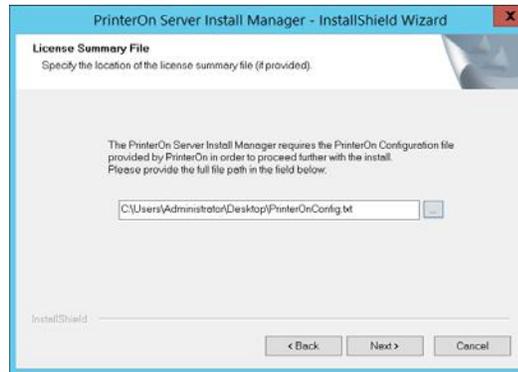
4. On the Setup Type screen, choose **Custom**, then click **Next**.
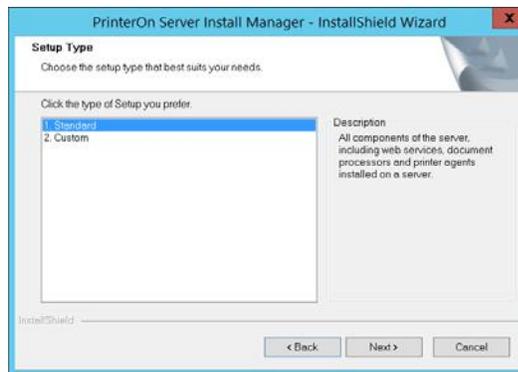
5. In the Select Features screen, select only **PrintAnywhere**, then click **Next**.
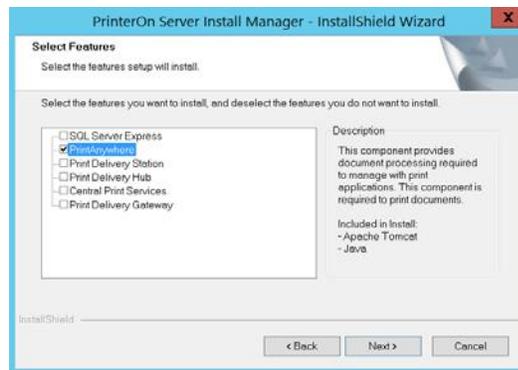
6. Follow the installation wizard until you get to the Serial Numbers screen.

7. On the Serial Numbers screen, select the serial number for the PrintAnywhere instance you are installing on the remote host, then click **Next** to install the PrintAnywhere Server.
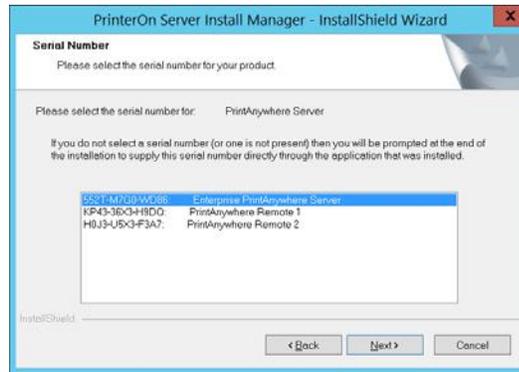
8. When the installation is complete, click **Finish**, and then reboot the computer.

9. If you choose, you can connect this server to a parent configuration server. For more information, see Connecting remote servers to a parent Configuration Manager.

10.2.3 Adding servers to a cluster

To connect servers:

1. In the Configuration Manager, click **Advanced** > **Clustering**.

2. From the **Select A Server** drop-down, select a server to configure. The drop-down lists all connected servers.

10.2.3.1 Adding Processing Servers

Processing servers increase the capacity of the solution. By default, the local Processing Server should be connected.

To add a processing server:

1. In the Configuration Manager, click **Advanced** > **Clustering**.
2. Click **Add Processing Server**. The Processing Server Information dialog appears.
3. To add a Processing Server that is already managed by the Configuration Manager:

   a) In the **Select A Server** drop-down, select a known server from the list.

   ```
   Processing Server Information                                    ✕

   Select A Server          WIN-VE3SO2P5HA9 - 127.0.0.1          ⬍

   Use Host Name ❔          ☐
   Reciprocate Connection   ☐

                                                    Add   Cancel
   ```

   b) Configure the following settings:

Setting	Description
Use Host Name	When checked, the server's hostname is used for communication. Otherwise, the IP address is used. **Note:** When operating, the server performs a reverse DNS lookup to validate the IP address provided. You should ensure that the IP address is valid and routable between servers.
Reciprocate Connection	Copies this configuration to all other Processing Servers managed by the Configuration Manager.

4. To add a Status server that is not managed by the Configuration Manager:

    a) In the **Select A Server** drop-down, select **Manual Entry**.

    b) Configure the following settings:

Setting	Description
Enabled	When checked, the server is enabled.
Machine Host Name	The network hostname or IP address of the server running the Processing Server that you are adding to the cluster.
Request Port	The network port number on which the Processing Server listens for requests.
Server Serial Number	The serial number of the Processing Server that is being connected to the Status Server. Each Server should have a unique serial number; this value must match the value on the destination server. For information on acquiring additional PrintAnywhere Serial numbers, see Creating and configuring a server cluster.

5. Click **Add**.

10.2.3.2 Adding Status Servers

Status Servers increase add redundancy to the solution as well as capacity. The local Status Server is NOT added to the list. Status Servers share job information during job processing. Add incoming jobs are received by a Status Server before being directed to the least busy Processing Server.

To add a Status Server:

1. In the Configuration Manager, click **Advanced** > **Clustering**.

2. Click **Add Status Server**. The Status Server Information dialog appears.

3. To add a Status Server that is already managed by the Configuration Manager:

    a) In the **Select A Server** drop-down, select a known server from the list.

    b) Configure the following settings:

Setting	Description
Use Host Name	When checked, the server's hostname is used for communication. Otherwise, the IP address is used. **Note:** When operating, the server performs a reverse DNS lookup to validate the IP address provided. You should ensure that the IP address is valid and routable between servers.
Reciprocate Connection	Copies this configuration to all other Status Servers managed by the Configuration Manager.

4. To add a Status server that is not managed by the Configuration Manager:

    a) In the **Select A Server** drop-down, select **Manual Entry**.

    b) Configure the following settings:

Setting	Description
Enabled	When checked, the server is enabled.
Machine Host Name	The network hostname or IP address of the server running the Status Server that you are adding to the cluster.
Request Port	The network port number on which the Status Server listens for requests.
Server Serial Number	The serial number of the Status Server that is being connected to the Processing Server. Each Server should have a unique serial number; this value must match the value on the destination server. For information on acquiring additional PrintAnywhere Serial numbers, see Creating and configuring a server cluster.

5. Click **Add**.

11

Adding a Print Delivery Hub

PrinterOn's Print Delivery Hub (PDH) is intended to provide a simple and reliable solution to deliver print jobs to printers and MFPs that are distributed across numerous disparate and isolated networks. The PDH acts as a centralized distribution server, coordinating the delivery of print jobs between PrinterOn's print servers and clients and PrinterOn's print release station software.

> **Note:** The Print Delivery Hub component is only available for PrinterOn Enterprise Edition.

When deploying a cloud printing solution, printers and MFPs can be distributed globally. However, users still want access these devices much like any other local device. The PDH offers a solution for enabling these print devices without the need for significant network reconfiguration. The Print Delivery Hub provides access to these devices while maintaining a high degree of security.

The PDH server accepts and holds print jobs generated and transmitted by PrinterOn's clients until they are retrieved for downloading and release by PrinterOn's Print Deliver Station (PDS) component. The PDS software initiates the communication from within the network and behind the firewall. The PDS can also be configured to communicate using commonly available ports such as 80 and 443. This combination minimizes the network configuration required to deliver print jobs from one network to another.

The PDH is based on the industry standard Internet Printing Protocol (IPP). PrinterOn has extended and enhanced the protocol with a number of PrinterOn extensions for improved print job data security (encryption), data compression, and collection of print job

metadata that is used for print job tracking and integration with print management and other cost recovery solutions.

11.1 System capacity

A single PDH can handle up to 5,000 PDS servers concurrently and at least 100,000 print jobs per day. Please note that one PDS may provide access to multiple printers or MFPs.

Increasing the number of PDH servers used (either in a single cluster or in a two cluster setup) allows for a larger number of PDSs to be handled concurrently.

11.2 Network layout

Without using any PDH servers, the PrinterOn system sends print jobs directly to a PDS. Print jobs can also be sent through PrinterOn's hosted PDH service, which is typically used with PrinterOn hosted and managed services.

For On-Premise deployments that require print jobs to be delivered to printers installed in disparate networks (that is, network segments in separate physical locations, possibly different cities, states, or countries), it may not be possible for the PrinterOn server or the PrintWhere driver to deliver print jobs directly to the PDS. In these cases, you can deploy a PDH service to provide simplified access to remote printers and MFPs connected to PDS servers. In this arrangement, print jobs are delivered to the PDH. PDS servers communicate with the PDH to detect and download the print jobs.

The PDH service can be installed in a central network operating center and must be accessible over the network to the PrintAnywhere Server, desktop PrintWhere clients, and PDS servers. Because the PDH is the only service in this network configuration that requires incoming network traffic access, changes to the network should be minimal.

11.3 Common deployment scenarios

The PDH can be deployed as a single server, or within a cluster of PDH servers. Deploying multiple PDH instances in either a one-cluster or two-cluster configuration can increase the availability of the printing service, increase overall capacity, and allow for part of the system to be disabled for maintenance purposes.

Note that clients such as PrintAnywhere and the PrintWhere Universal Print Driver can be configured to communicate with a PDH server and also configured to communicate directly to a PDS. This configuration option is managed on a per-printer basis. The software first attempts to communicate directly to PDS (which provides a performance advantage). If the software is unable to contact the PDS, it uses the configured PDH as an alternate route to deliver print jobs.

11.3.1 Single server deployment

The simplest way to enable printers and MFPs in separate networks is to deploy a single dedicated PDH. The server is deployed and configured so that it is accessible by both the PrinterOn Enterprise server and the remote print locations.

Each PrinterOn virtual printer is configured to deliver print jobs to the Print Delivery Hub and each Print Delivery Station will be configured to download print jobs from the PDH.
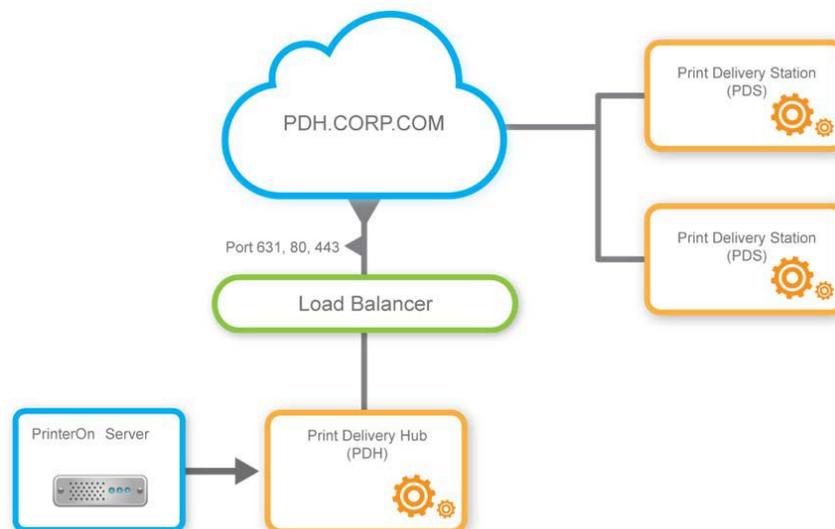
11.3.2 Two node redundant deployment

In this example, two PDH servers are configured to operate as a single system. This deployment allows for future growth by adding additional nodes to either server to expand the number of peers in the cluster. In this configuration, print jobs are duplicated on each server. By replicating the servers, the overall service is more resilient to hardware failures that may occur on either server.

Please note that both PDH servers must be configured to ensure the cluster is addressable via a single DNS entry. A load balancer must also be configured to distribute network traffic between the servers. The load balancer distributing traffic to the PDH nodes would have to direct traffic away from the node being taken down for maintenance and redirect that traffic to the remaining nodes.
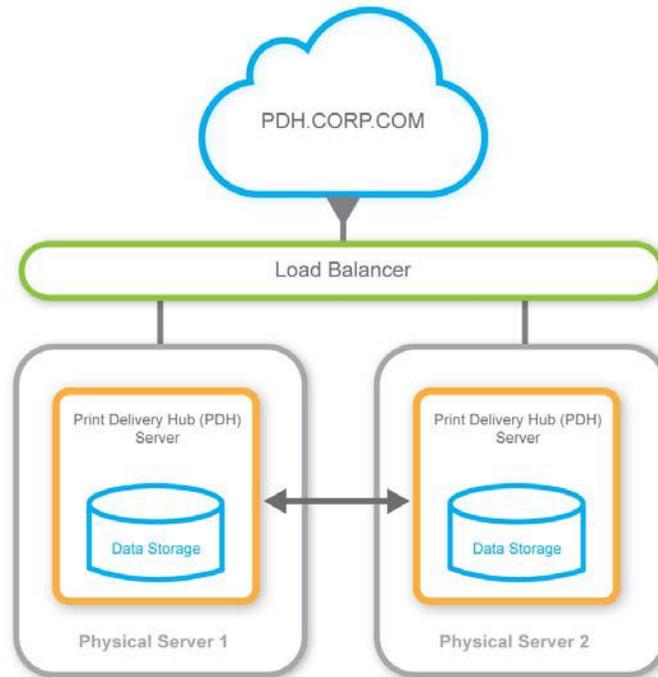
11.3.3 Multiple redundant PDH clusters

This configuration is an expansion of the previous example. Additional PDH cluster peers can be added to each PDH cluster to increase overall capacity. Each cluster peer shares a common storage subsystem where print job data and metadata files are stored. The common storage subsystem is typically a network shared file system.

Each peer in the cluster can be deployed either on a distinct virtual machine on a single physical server or on a separate physical server.
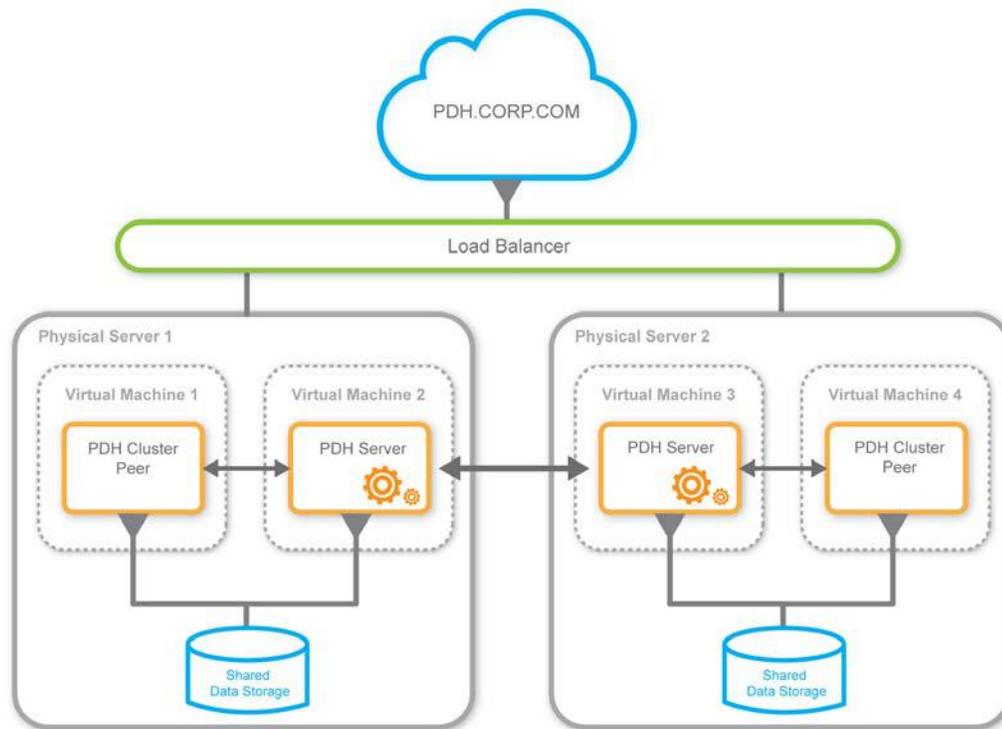
11.4 Configuring Internet communications

The **Internet Communication** tab contains the main settings controlling incoming and outgoing communications used by the PDH software.

To configure Internet communication for a PDH:

1. In the Configuration Manager, click **Advanced** > **Components**.
2. Click the **Configure** button adjacent the **Print Delivery Hub** component. The PDH component configuration appears.
3. Click **Internet Communication**.

4. Configure the settings in the following panels:

    - Licensing

    - Web Services Manager

    - Network and Broadcast Settings

    - Thread Pool

    - Print Delivery Station Communication

    - XMPP Notifications

5. Click **Apply Settings**.

11.4.1 Network Identification and Access

PrinterOn print clients, such as PrintAnywhere and PrintWhere, and PDS deployments are designed to access the PDH service as a single entity. As a result, when deploying a multi-node setup, care must be taken to ensure the cluster is addressable via a single DNS entry and that load balancers accept traffic for that name and forward the traffic appropriately to each PDH server in the cluster.

11.4.2 Configuring PDH licensing and the Web Services Manager

The **Licensing** and **Web Services Manager** panels allow you to specify the PDH serial number required to activate the PDH, and the URL or the Web Services Manager connection information.

Licensing		
Serial Number ❓	5005-52NB-AP3H	✅

Web Services Manager	
Services Manager URL	https://127.0.0.1/cps/rest/

11.4.2.1 Licensing and Web Services Manager settings

Setting	Description
Serial Number	This is the serial number of PDH license and can be obtained from PrinterOn under the Software tab once you log in as an administrator. This is required to activate the Print Delivery Hub.

Setting	Description
Services Manager URL	The URL of the Web Services Manager. The Services Manager controls how the components of the server communicate to retrieve printer information and license information.

11.4.3 Configuring Network and Broadcast Settings

The **Network and Broadcast Settings** panel defines the ports used by the PDH. The PDH listens on the configured ports for requests from Print Delivery Stations. You can set up to three ports, and specify whether which ports are enabled, and which ports are configured to use SSL.

By default, the **Default IPP Port** is configured to be port 631, which is the port typically assigned to the Internet Printing Protocol (IPP).

Often, Print Delivery Stations are deployed in locations whose networks may offer limited or controlled access to the Internet. To provide reliable communication, you can configure and enable up to two additional ports.

Typical installations use port 80 and port 443, as these are the most commonly accessible. Port 443 is usually configured to use SSL. Enabling ports 80 and 443 provides the highest accessibility for remote PDS deployments.

If you check **SSL** for a port, you must also configure the PDH SSL tab. For more information, see Configuring SSL settings for your PDH.

11.4.4 Configuring Thread Pool settings

The **Thread Pool** panel shows the configuration parameters for the worker thread pool used by PDH for handling incoming communication traffic.

Thread Pool (per Communication Port)	
Min Threads	5
Max Threads	50
Socket Backlog	50
Socket Shutdown Delay (ms)	0
Idle Time (ms)	5000

Note: Only administrators who have a good understanding of networking and server management should modify the settings in this panel. PrinterOn has chosen default values that should satisfy the requirements of most installations.

The **Min Threads** and **Max Threads** settings control the size of the thread pool used for each of the communication ports enabled in the Network and Broadcast panel. A connection is used while print client software such as PrintAnywhere queries for printer status and availability and while a print job is being transmitted. These worker threads are also used between PDHs in peer and cluster communications.

Threads are returned to the pool when the operations are complete. The default values should satisfy most installation requirements. Installations that handle a heavy traffic load may benefit from increasing the Max Threads setting.

11.4.4.1 Thread Pool settings

Setting	Description
Min Threads	The initial number of threads allocated by the software. This setting helps prevent thread starvation at startup time.
Max Threads	The upper limit to the number of simultaneous connections each port can accommodate.

Setting	Description
Socket Backlog	The number of "half-open" sockets each port can support. Half-open sockets are those that are in the first stages of establishing a communication channel between the print client and the PDH server.
	The default value of 50 should be suitable for most installations. Network setups that experience large latencies (100 ms or more) between PDH and print clients might benefit from a larger **Socket Backlog** value, such as 100.
Socket Shutdown Delay	The amount of time the PDH server keeps the socket open after transmitting the final data and before fully closing the socket. The delay period helps to ensure an orderly teardown of the socket.
	As with the Socket Backlog parameter, setups that experience large latencies (100 ms or more) might benefit from a larger Socket Shutdown Delay. If print clients are experiencing errors such as unexpected socket termination, increasing this value to 500 ms might improve the communication process.
Idle Time	The socket timeout period used by the threads in the thread pool.
	While waiting for a response from the IPP client software, if no data packet is received for this amount of time, it is assumed that the client has disconnected ungracefully. In that case, the socket is closed and the worker thread is recycled back into the thread pool, ready to service another communication request.

11.4.5 Configuring Print Delivery Station Communication settings

The **Print Delivery Station Communication** panel provides additional configuration and control over how Print Delivery Stations (PDS) and other printer agents access and communicate with a Print Delivery Hub (PDH).

11.4.5.1 Print Delivery Station Communication settings

Setting	Description
Enhanced Client Authentication Policy	The type of authentication required in order to connect to PDH and download print jobs. The available options are **Always**, **Optional**, and **Never**.

Setting	Description
Password	Applicable only to on-premise deployments of PrinterOn. A password that ensures communication between Print Delivery Hub and Print Delivery Station is secure. The **Password** value entered in PDH must be entered into the corresponding **Password** field in the Print Delivery Station Configuration Settings. Beginning with version 4.2.4, the PrinterOn Enterprise Managed Cloud service uses PDS-specific passwords, in which each PDS agent has its own unique password that it uses to connect to the PDH. Therefore, the PDH **Password** setting has no function in Managed Cloud deployments, and any value in this field is ignored.
JWT-Based User Authorization (*Advanced view* only)	When set to **Required**, a JSON Web Token (JWT) must be included in a request when the user attempts to access a list of their print jobs for release. The JWT adds an additional layer of security. When a user successfully logs into the PrinterOn service, a JWT is returned to the user by the authentication service. This token can then be included in subsequent requests on behalf of the user to provide authorization to access other resources. When a user makes a request for their list of print jobs, the PDH validates the token signature. JWTs are also used in place of release codes, which are inherently less secure. Print jobs can only be released to the printer by the authorized user, whose identity is verified by the token. Other options for this setting include: • **Disabled**: JWTs are not supported and can not be included in the request for authorization. This is the default. • **Optional**: JWTs can be included in the request, but are not required for authorization; the PDH will validate the token if it is present and JWT validation is enabled, but will still pass on the request the token is omitted. If this value is set to **Required**, then you must disable the Support Release Code Job Access setting on the Job Settings tab.
Allowed JWT Issuer suffixes (*Advanced view* only)	A semi-colon-separated list of URLs from which JWTs may be issued for the purposes of authorizing access to the PDH.
JWKS End Point (*Advanced view* only)	The location from which the PDH retrieves public key information in the JSON Web Key format.

Setting	Description
JWT Signature Validation (*Advanced view* only)	When enabled, the PrinterOn server attempts to verify the signature of the JWT.
	By default, this setting is enabled. If you are using JWT-based user authorization, it is recommended that you leave this setting enabled, unless you have a compelling reason to disable it.
Enhanced Request Security	When set to **Required**, the PDH requires that any requests from a user to access a list of their print jobs must include a Signature Key.
	The Signature Key adds an additional layer of security; when a user makes a request, if the Signature Key is included, it allows the PDH to confirm who sent the request and ensure that only that person can retrieve and release the request.
	Other options for this setting include:
	• **Disabled**: Signature Keys are not supported and can not be included in the request. This is the default.
	• **Optional**: Signature Keys can be included in the request, but are not required; the PDH will validate the signature if it is present, but will still pass on the requested print jobs if the signature is omitted.
	If this value is set to **Required**, then you must disable the Support Release Code Job Access setting on the Job Settings tab.
Accept Jobs For Any Print Delivery Station	When checked, the PDH accepts any print jobs destined for any Print Delivery Station. Having this option enabled is the simplest method to deploy a PrinterOn Service.
	When unchecked, each agent must register their PrinterOn printers with the PDH server. The PDS and PDH software performs the registration automatically when configured to do so; the PDS registers its associated printers when it checks for pending jobs to download. The PDH server rejects any jobs destined for a printer that is not registered with the server.
	It is generally recommended to enable this option when initially deploying your service to simplify the configuration and management process.
Enable Advanced Job Validation	When enabled, PDS performs an additional round of job validation to ensure that
	This setting should only be enabled if no authentication is used. Enabling this setting results in increased network load and can reduce performance.

Setting	Description
Enable HTTP Keep-Alive	When enabled, the PDS holds a persistent connection with the PDH. Enabling this setting minimizes the network overhead associated with establishing a network connection. You should only change this setting as directed by PrinterOn Support.
Minimum Client Notification Timeout (ms)	The minimum amount of time that PDS will hold a connection. You should only change this setting as directed by PrinterOn Support.
Default Client Notification Timeout (ms)	The default amount of time that PDS holds a connection if no notification timeout is set. This setting is only used in conjunction with some legacy embedded agents that don't support notification timeout. You should only change this setting as directed by PrinterOn Support.
Enable Client Notification Registration	When enabled, turns on long polling notifications. You should only change this setting as directed by PrinterOn Support.
Enable Client Notification De-Registration	When enabled, disables part of long polling notification. This setting is only used in conjunction with some legacy embedded agents that don't support notifications. You should only change this setting as directed by PrinterOn Support.
Enable PerPdsPdh Password (*Advanced view* only)	When enabled, each PDS that attempts to communicate with the PDH must have its own unique password for the PDH. The PDH retrieves the passwords for a PDS from the location specified in the **PDH Password Endpoint** field.
PDH Password Endpoint (*Advanced view* only)	The location from which the PDH retrieves PDS passwords. When contacted by a PDS, the PDH retrieves the password for that PDS from the specified location and compares it to the password included in the PDS request. If they match, access is granted.
CPS Signing URL (*Advanced view* only)	The location from which the PDH retrieves a signing token.
JWKS URL (*Advanced view* only)	The location from which the PDH retrieves the public key's information in the JWKS format.

11.4.6 XMPP notifications

The **XMPP** panel controls settings pertaining to the optional XMPP Server integration feature. When enabled, this feature causes PDH to connect to an XMPP Server—using the connection details specified in panel—to publish print job availability information.

Installation, configuration and administration of the XMPP Server are beyond the scope of this document. Corresponding XMPP Notification settings must be entered into the Agent.

11.5 Configuring PDH job settings

The **Job Settings** tab contains the settings controlling how print job files are processed and certain rules for accepting print jobs and purging them if they have been abandoned.

To configure job storage settings for a PDH:

1. Log in to the Configuration Manager.
2. Click **Advanced** > **Components**.
3. Click the **Configure** button adjacent the **Print Delivery Hub** component. The PDH component configuration appears.
4. Click **Job Settings**.
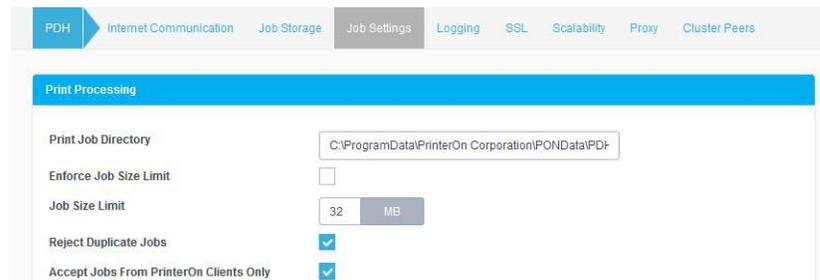
5. Configure the settings in the following panels:
   - Print Processing
   - Unclaimed job Handling
   - Advanced Network Settings
6. Click **Apply Settings**.

11.5.1 Configuring Print Processing settings

The **Print Processing** panel controls settings regarding job data storage and rules used to determine whether to access or reject new jobs.
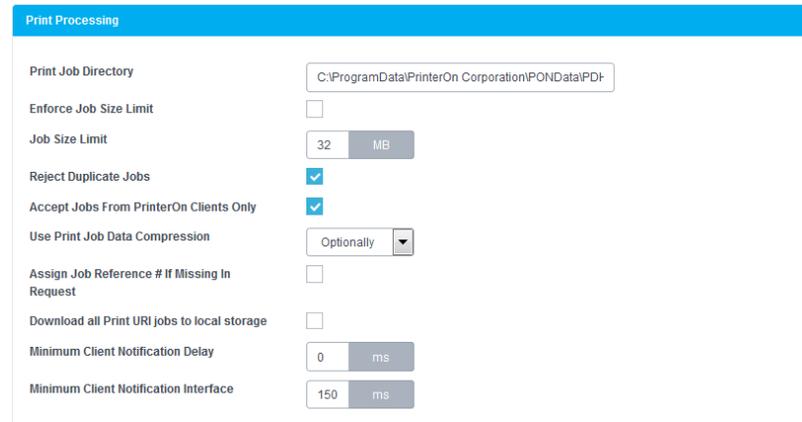
Print Processing	
Print Job Directory	C:\ProgramData\PrinterOn Corporation\PONData\PDH
Enforce Job Size Limit	☐
Job Size Limit	32 MB
Reject Duplicate Jobs	☑
Accept Jobs From PrinterOn Clients Only	☑
Use Print Job Data Compression	Optionally ▼
Assign Job Reference # If Missing In Request	☐
Download all Print URI jobs to local storage	☐
Minimum Client Notification Delay	0 ms
Minimum Client Notification Interface	150 ms

11.5.1.1 Print Processing settings

Setting	Description
Print Job Directory	Where the print job data and metadata files are stored. When implementing a PDH cluster this storage location must be available to all PDH peers. This is typically a network storage location accessible to all nodes in a cluster.
Enforce Job Size Limit	When checked, the **Job Size Limit** is enforced and applied to new jobs.
Support Release Code Job Access	When checked, users can use release codes to access and release the print jobs. If you have set one or both of the JWT-Based User Authorization or Enhanced Request Security settings to **Required**, you must disable this setting.
Job Size Limit	When **Enforce Job Size Limit** is enabled, PDH rejects incoming print jobs whose size exceeds the specified limit.
Reject Duplicate Jobs	When checked, duplicate print jobs are immediately rejected by the system. Print jobs are identified by Job ID number (as defined by the Internet Printing Protocol (IPP) RFC.) The cause of duplicate print jobs is usually an unreliable network connection that causes the software that transmitted the print job to miss the acknowledgment that the print job had been received properly. When that happens, the print client software can re-transmit the print job.

Setting	Description
Accept Jobs from PrinterOn Clients Only	When checked, incoming print jobs from non-PrinterOn Clients are not accepted. Otherwise, the PDH server will accept IPP compliant print jobs from any IPP print client.
Use Print Job Data Compression	How print job data compressions is managed by PDH. There are three options:
	• **Optionally:** Indicates that the PDH supports compression and the submitting client can optionally compress new prints jobs prior to submitting to PDH. Release station clients, such as PDS, can choose to download the print data in a compressed or uncompressed state depending on the capabilities of the print device.
	• **Never:** PDH reports to the sending client that compression is not supported. Release station software, such as PDS, will receive all jobs in an uncompressed state when downloading jobs.
	• **Always:** PDH reports to the sending client that compression is supported. Release station software, such as PDS, will receive all jobs in a compressed state when downloading jobs.
	For best compatibility, this setting should be set to **Optionally**.
Assign Job Reference # If Missing In Request	When checked, the PDH assigns a job reference number if none exists in the request. This scenario is extremely rare. As a result, this setting is used primarily for troubleshooting; you should only change this setting as directed by PrinterOn Support.
Download all Print URI jobs to local storage	This setting is for future support of cloud storage. It is not currently used.
Minimum Client Notification Delay	The length of time, in milliseconds that the PDH waits before notifying the PDS that a job is available. By default, there is no delay.
	Increasing the delay can be useful if your system handles a high number of batch jobs, or emails with multiple attachments to be printed. In these cases, having a delay allows the PDH to receive all the documents before sending out notifications to the PDS. PDH can send out a single notification for multiple received documents, minimizing the amount of communication between components, and thereby reducing network use.
Minimum Client Notification Interval	The minimum length of time PDH waits after sending PDS a notification before sending another notification.

11.5.2 Configuring Unclaimed Job Handling settings

The **Unclaimed Job Handling** panel controls the feature whereby unclaimed print jobs are automatically purged from PDH if they have remained on the server beyond the specified interval.

Unclaimed Job Handling	
Enable Abandoned Job Purge	✓
Purge Abandoned Job Interval (Hours)	50

11.5.2.1 Unclaimed Job Handling settings

Setting	Description
Purge Unclaimed Jobs	When checked, PDH automatically deletes jobs that have not been downloaded by a PDS client.
Job Retention Period	The length of time that the PDH server stores print jobs before it deletes them.

11.5.3 Advanced Network Settings

The **Advanced Network Settings** panel provides additional advanced network configuration options, generally intended for an advanced or customized deployment.

Advanced Network Settings	
Server Download Buffer Size (MB)	0
Enable Download Pacing Feature	✓

11.5.3.1 Advanced Network settings

Setting	Description
Server Download Buffer Size	The size of the download buffer. This setting correlates to the TCP Window Size, and is provided to help address network scenarios, such as high bandwidth and also high latency. Too high a value here wastes memory and can decrease throughput if the network suffers too many packets that need to be retransmitted.
Enable Download Pacing Feature	When checked, the PDH monitors the amount of data waiting in its (internal) transmit buffer. When the transmit buffer gets 75% full, PDH slows the rate at which more data is loaded into the buffer.
	When the transmit buffer goes back below the configured threshold, the PDH increases the rate at which data is provided to the buffer. The goal is to prevent PDH from buffering the entire print job data payload in memory, reducing memory usage by PDH.
	The Download Pacing Feature is enabled by default and is expected to be useful in nearly every situation. To allow the PDH Admin to troubleshoot situations where print job data download speeds appear to be highly variable, the feature can be disabled as a diagnostic aid.

11.6 Logging

The **Logging** tab contains the settings pertaining to application and debug logging. Log files are created as required and are automatically deleted. The PDH server will automatically delete older log files to ensure the total size of all log files stays within the **Total Size Limit** setting.

When a new log file is created, the log file name is created using the time the file was created as a unique filename. Log file names take the form:

ListeneryyyyMMddhhmmss.sss.log

where:

- **Listener**: the base name for all PDH log files
- **yyyy**: year
- **MM**: month (January = 01)
- **dd**: day (first of the month = 01)
- **hh**: hour (24-hour clock)
- **mm**: minute

- **ss.sss**: second (including milliseconds)

To configure logging settings for a PDH:

1. Log in to the Configuration Manager.

2. Click **Advanced** > **Components**.

3. Click the **Configure** button adjacent the **Print Delivery Hub** component. The PDH component configuration appears.

4. Click **Logging**.

5. Configure the Debug Logging settings:

Setting	Directory
Log Level	The level of detail to use for logging across all components. Higher levels of logging are most useful when troubleshooting.
Output Directory	The folder where the log files are written.
Maximum File Size	The maximum file size of an individual log file. When a log file's size reaches the Maximum File Size value a new log file will be automatically created.
Total Size Limit	The total size of all the log files that can exist at any one time. If creating a new log file causes the total storage used by the system to exceed this limit, the oldest log file is automatically deleted.

6. Click **Apply Settings**.

11.7 Configuring SSL settings for your PDH

The **SSL** tab allows you to configure the PDH to support SSL. Enabling SSL for your PDH server provides additional security for print jobs delivered through the server. When SSL is enabled and configured for the PDH, clients submitting print jobs to the PDH server use a secure SSL channel. Print Delivery Station deployments downloading print jobs to be printed also use SSL.

To configure SSL settings for a PDH:

1. Log in to the Configuration Manager.
2. Click **Advanced** > **Components**.
3. Click the **Configure** button adjacent the **Print Delivery Hub** component. The PDH component configuration appears.
4. Click **SSL**.

5. Configure the settings in the following panels:
   • SSL Certificate Keystore
   • Enter SSL Information
6. Click **Apply Settings**.

11.7.1 SSL Certificate Keystore

If any port is configured to use SSL, the SSL Certificate Keystore panel becomes active, allowing you to set details for the SSL Certificate.

PDH uses a standard format file for storing SSL Certificates, known as a keystore. As defined by Oracle (Sun), the keystore file can contain multiple certificates.

SSL Certificate KeyStore	
KeyStore File	NONE
KeyStore Passphrase	••••••••
Key Name	focus
Key Passphrase	••••••••

11.7.1.1 SSL Certificate Keystore settings

Setting	Description
Keystore File	The full path and file name for the keystore file used to store the SSL Certificate. • Click the Browse button (...) to select an existing file. • Click **Create** to create a new keystore file or a new key within an existing keystore file. It is recommended that the PDH SSL Certificate be stored in its own keystore file, not the cacerts file in the underlying JRE installation. When you click **Create**, a dialog box appears prompting you for required and optional data used when generating an SSL Certificate.
Keystore Passphrase	The passphrase (or password) for the overall keystore file. The default value is password. If using an existing keystore file, you must specify the correct passphrase here.
Key Name	The key (or certificate) name used to identify the certificate that PDH is to use.
Key Passphrase	The passphrase (or password) for the certificate that PDH is to use. The default value is password.

11.7.2 Entering SSL Information

The **Enter SSL Information** panel lets you provide the information associated with your certificate.

Enter SSL information

Common Name (CN)

Organization Unit (OU)

Organization Name (O)

Locality Name (L)

State Name (ST)

Country (C)   AD

11.8 Configuring scalability behavior

The **Scalability** tab lets you configure the behavior of PDH to use clustering to deploy a system that is both fault-tolerant and scalable. The **Scalability** settings only come into effect when you create a PDH cluster. To create a cluster, you must add peer nodes on the **Cluster Peers** tab. For more information, see Adding Cluster Peers. By default, PDH is configured to operate as a standalone server.

Cluster Peers are PDH nodes that share a common storage subsystem where print job data and metadata files are stored. The common storage subsystem is typically a network shared file system. Each peer can create, read, write, or delete any print job on the common storage subsystem when accepting print jobs from print clients and making them available for download by Print Delivery Station deployments. When a PDH node creates, updates, or deletes a job, that PDH node sends each configured peer a message detailing the update. The messages between Cluster Peers are called Peer Notification messages.

A maximum of two PDH clusters can be defined for a particular PDH installation. When Remote Hub Replication is enabled, print jobs are automatically copied between PDH clusters. The PDH node that receives the print job from the print client transmits a message to the Remote Hub alerting that cluster of the newly received print job. The PDH node that received this update copies the print job to its own Print Request Directory (which may be shared with other Cluster Peers.) Update messages between PDH clusters are called Replicate Job messages.

The maximum number of PDH nodes comprising a PDH setup is limited to nine. Take care to ensure that each PDH node is assigned a unique Peer ID number.

At software startup and, optionally, at configurable intervals thereafter, the software ensures the entire job list is fully synchronized between all active PDH nodes.

To configure Scalability settings for a PDH:

1. Log in to the Configuration Manager.

2. Click **Advanced** > **Components**.

3. Click the **Configure** button adjacent the **Print Delivery Hub** component. The PDH component configuration appears.

4. Click **Scalability**.

5. Configure the settings in the following panels:

    • Cluster Security

    • Cluster Configuration

    • Remote Hub Replication

    • Remote Hub Synchronization

6. Click **Apply Settings**.

11.8.1 Configuring Cluster Security and Cluster Configuration

11.8.1.1 Cluster Security and Cluster Configuration settings

Setting	Description
Enhanced Cluster Authentication Policy	How cluster authentication is enforced. This setting has the following possible values: • **Never** – Authentication between cluster peers is not enforced. • **Optional** – Authentication between cluster peers is validated if a password is supplied. • **Always** – Authentication between cluster peers is always validated.
Cluster Communication Password	The password that should be used when cluster peers communicate. Each cluster peer should have the same password configured.
Peer ID For This Computer	The PDH node number for this instance of the software. You must ensure that each PDH instance is assigned a unique ID number.

11.8.2 Configuring Remote Hub Replication

When Remote Hub Replication is enabled, print jobs are automatically copied between PDH clusters. The PDH node that receives the print job from the print client transmits a message to the Remote Hub alerting that cluster of the newly received print job. The PDH node that received this update copies the print job to its own Print Request Directory (which may be shared with other Cluster Peers.) Update messages between PDH clusters are called Replicate Job messages.

11.8.2.1 Remote Hub Replication settings.

Settings	Description
Enable	When checked, Remote Hub Replication is enabled.
Pacing Delay	The amount of time to wait between Replicate Job messages during software startup or during cluster resynchronization, when enabled. This delay interval helps prevent network saturation between PDH nodes. The default value of 50 ms is usually sufficient for most environments. If your service experiences significant load, and print jobs between PDH clusters are significantly different, increasing this value to 75 or 100 is recommended.
Remote Hub URI	The address of the remote PDH cluster as specified via the Scheme, Address and Port fields.

11.8.3 Configuring Remote Hub Resynchronization

When enabled, this feature causes the entire job list held in memory to be replicated with the other PDH Cluster. During normal operation, a PDH cluster will automatically inform its paired cluster that jobs have arrived, been downloaded, or deleted. Resynchronization occurs at a set time interval to ensure that both clusters are mirrored and compensate for any variations.

11.8.3.1 Remote Hub Resynchronization settings

Setting	Description
Enable	When checked, Remote Hub Synchronization is enabled.
Resynchronization Interval	The amount of time between resynchronization events. The timer starts after the software has started running. Decreasing the time frame between resynchronization will require additional network resources.
Use One-Shot Resynchronization	When checked, a single resynchronization message is used to update the other PDH Cluster regarding the entire list of jobs known to this PDH node. Otherwise a separate Replicate Job message is transmitted for each job known to this PDH node. One-shot synchronization sends a single, large update message to a paired cluster. A large message is more susceptible to transmission failure on a congested network segment, but is generally faster than using separate Replicate Job messages for each known job. Smaller update messages are more reliably transmitted and received, but have a higher overhead due to establishing a new connection for each update. This means the resynchronization process takes longer to complete. If the network between PDH clusters is high quality and high performance, enabling this option is recommended.

11.8.4 Adding Cluster Peers

The **Cluster Peers** tab lets you add Peer PDH nodes to your cluster. to your configure network settings for communicating with PDH Peer instances.

A cluster peer, also referred to as a node, is a fully functional Print Delivery Hub Server. A PDH Peer is intended to provide increased reliability, maintainability and performance. For a multi-node setup, care must be taken to ensure the cluster is addressable via a single DNS entry and that load balancers accept traffic for that name and forward the traffic appropriately to each and any PDH server in the cluster.

Having more than one node in a single cluster has a few benefits:
- It allows the cluster to handle more simultaneous connections (from PrinterOn Print Delivery Station software).
- It makes the cluster more resilient to failure of an individual node due to system failures.

- It also allows an administrator remove, disable, or update individual nodes without impacting the overall cluster.

To add a cluster peer:

1. Log in to the Configuration Manager.

2. Click **Advanced** > **Components**.

3. Click the **Configure** button adjacent the **Print Delivery Hub** component. The PDH component configuration appears.

4. Click **Cluster Peer**. The Cluster Peers tab displays a list of all the peers in the cluster. By default, there are no peer nodes, since the PDH is configured to operate as a standalone server.
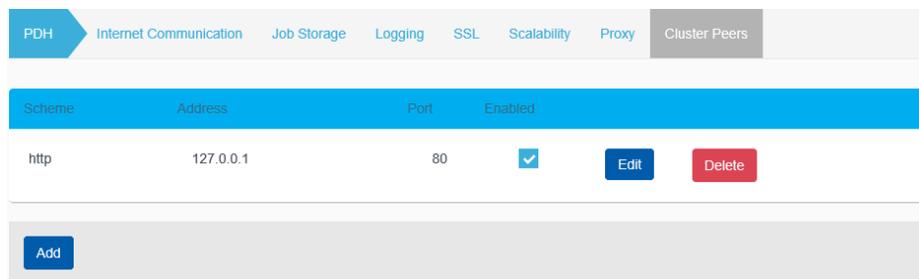
5. Click Add. The **Add Cluster Peer** panel appears.
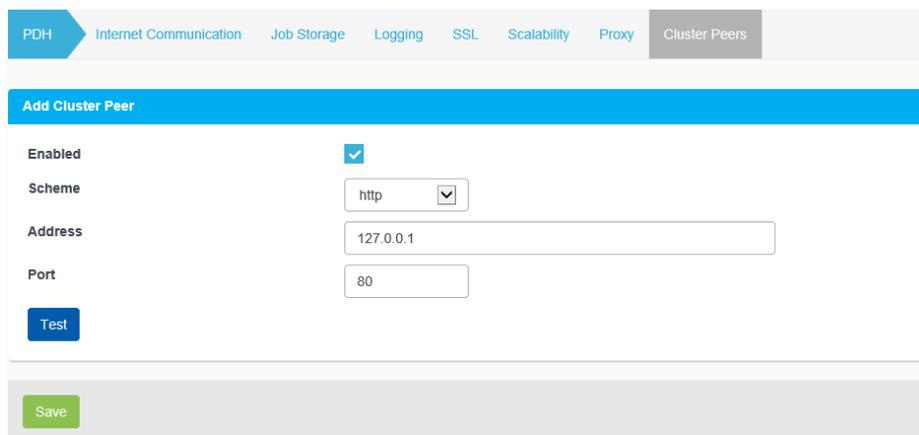
6. Configure the following settings:

Setting	Description
Enabled	Allows you to enable or disable communication to the Peer.
Scheme	Allows you to specify http:// or https://.

Setting	Description
Address	Allows you to configure the address of the Peer. You can use a DNS name or an IPv4 Address.
Port	Allows you to specify the port number. Note that the port number specified is used to notify Cluster Peers of updated job information. Port 631 is recommended, as it is required in each PDH deployment.

7. To test the connection to the peer node, click **Test**.

8. Click **Save**.

11.9 Proxy Configuration

The **Proxy** tab allows you to configure HTTP Proxy settings.

To configure logging settings for a PDH:

1. Log in to the Configuration Manager.

2. Click **Advanced** > **Components**.

3. Click the **Configure** button adjacent the **Print Delivery Hub** component. The PDH component configuration appears.

4. Click **Proxy**.

5. Configure the Proxy settings:

Setting	Description
Proxy Enabled	When checked, the use of an HTTP Proxy is enabled.
Proxy Address	Specify the DNS name or IPv4 address of your proxy server.
Proxy Port	Specify the port number that should be used to communicate with the proxy.
User Name	The login/username to use when authenticating against the proxy server.---If your proxy does not require Authentication parameters, you can enter any values here and they will be ignored. PDH supports Basic Authentication and NTLM Authentication. For NTLM Authentication, the User Name usually includes a Domain followed by a User ID, as in domain\userID. (Note the single backslash.)
Password	The password to use when authenticating against the proxy server.

6. Click **Apply Settings**.

12

Configuring your mail server for PrinterOn email printing

The PrinterOn server has been designed to provide email-based printing capabilities as part of an overall Enterprise printing platform. PrinterOn recognizes that deployment and configurations within an organization may vary significantly and has developed a solution that is flexible and adaptable to your specific requirements.

In addition, the PrinterOn server has been designed to be as unobtrusive as possible, allowing for a deployment that requires minimal changes to your existing installation. This chapter outlines a number of deployment options to let select the deployment that best suits your needs.

12.1 Maintaining email security

The PrinterOn Server only performs basic validation of the email address and domain. It is typically the responsibility of the upstream email server and configured SPAM software to ensure the validity of the incoming email addresses prior to being delivered to the PrinterOn server.

The PrinterOn server integration for email printing is one where the Enterprise Server simply acts as a mail client, much like Outlook or any other mail client. Like these clients, they assume the mail server is providing a level of security prior to delivering the messages. This approach allows the PrinterOn server to be flexible while using existing SPAM or virus investments.

12.2 Recommended message routing configurations

The PrinterOn server monitors a single mailbox to receive and process email print requests. To facilitate receiving email print requests, different routing configurations are available depending on the number of printers supported within your installation.

The simplest deployment option is to create a mailbox on your existing mail server to receive print email print requests. In this deployment scenario, the PrinterOn server will act as a simple mail client and monitor for new email messages in the mailbox.

However, the recommended scenario is to separate email printing and the PrinterOn server from your corporate mail server. In this scenario, you install a mail server, such as the free Windows based hMailServer (www.hmailserver.com) directly on the PrinterOn server.
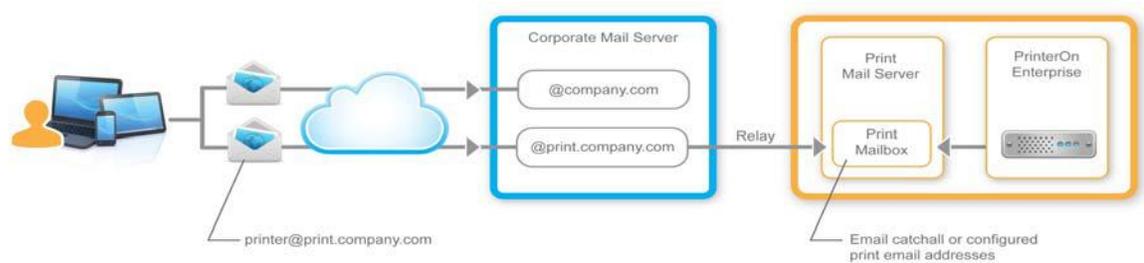
This mail server is dedicated for receiving and processing all email print requests. All email print messages are routed directly to this mail server to be processed by the PrinterOn server. If your organization uses Microsoft Exchange, you may consider configuring an Internal Relay Domain to direct messages to a subdomain such as print.company.com.

12.2.1 Configuring a printing-specific email subdomain

Regardless of where the mail server is located, it is typically beneficial to segregate email print jobs from other email traffic within your network. In addition to making it easier for users to identify print locations, segregating email traffic offers additional flexibility in how and where your email print jobs are processed.

PrinterOn recommends that you configure a subdomain within your existing domain structure to support email printing. For example, if your company domain is www.companyxyz.com, you might set up your email printing subdomain as

@print.companyxyz.com. By adding this subdomain for printing, you also have the option of deploying a separate email server dedicated to email printing.

For example, your primary corporate email may be managed by a server for all messages routed to @companyxzy.com. You may then install a dedicated mail server (possibly a low-cost or free alternative such as hMailserver) on the PrintAnywhere server itself.

Mail received at the @print.companyxyz.com subdomain can be routed to this mail server for handling only email print jobs. This approach also aligns with the use of email server catch-alls, as emails received by the mail server should be intended for email printing.

12.3 Creating a printing-dedicated mailbox

To allow seamless emailing printing, the PrinterOn server establishes a connection to the internal mail server using standard connection protocols (IMAP4, EWS, and Notes Domino). With this type of integration, the PrinterOn server uses a single mailbox on the mail server to scan for new email print jobs to be printed.

When email printing is enabled on multiple printers, only one mailbox on the mail server is scanned for new mail. This means you need to configure a way for all the emails to all printers to be delivered to that mailbox without changing the email address associated with each printer. You can do this mailbox configuration in several ways, depending on the specific environment:

- In non-ActiveSync environments with small numbers of printers, you can create aliases on a single mailbox.
- When creating aliases is not possible or inconvenient, such as in Microsoft Exchange ActiveSync environments and non-ActiveSync environments with many printers, you can:
    - create a distribution group for each printer, and add the mobile print mailbox to it.
    - set up automatic email forwarding to the mobile print mailbox.

12.3.1 Setting up a mailbox alias in non-ActiveSync environments

When supporting a small number of printers, the simplest configuration option is to associate multiple email addresses with a single mailbox on your mail server. This option involves the least amount of configuration for the mail server administrator.

PrinterOn provides two email addresses for every PrinterOn enabled printer. The first is a 12-digit numeric email address such as 300234123432@company.com. The other is a configurable alpha-numeric address such as boardroom-printer@company.com. The numeric address is guaranteed to be unique and will never change throughout the lifespan of the printer listing in the PrinterOn database. The alpha-numeric address is configurable in the Configuration Manager and may be modified in the future.

When configuring a small number of printers, you can retrieve the address from PrinterOn's web admin portal site and add these as optional addresses for your email print mailbox. Users can then submit print jobs to these addresses and all emails will be routed to the common mailbox.
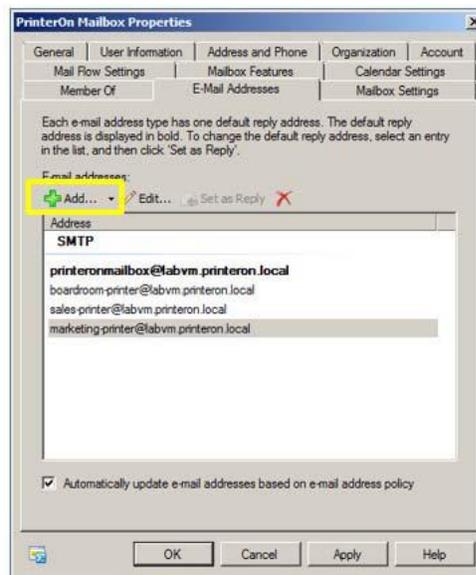
12.3.2 Creating a mailbox when aliases cannot be used

If you are enabling email printing and also using Microsoft's ActiveSync to allow mobile devices to connect to your Exchange server, the email alias deployment option described above may not meet all your requirements. Microsoft's ActiveSync does not support the same capabilities when connecting with some iOS and Android devices. In these cases, all emails are delivered to the default email address configured for the mailbox, as opposed to the address entered by the user. The **Hide from Exchange Address lists** option is ignored.

There are two ways to workaround this issue:
- Create a distribution group for each printer, and add the mobile print mailbox to it.
- Set up automatic email forwarding to the mobile print mailbox.

PrinterOn Enterprise v4.3.9 Configuration Guide | 259

These mailbox configurations are supported for both ActiveSync and non-ActiveSync environments.

12.3.2.1 Creating distribution groups and lists

To create a distribution group in Microsoft Exchange:

1. Create one main mobile print mailbox. This mailbox can be named anything, for example, printeronmailbox@mycompany.com.
2. Ensure this mailbox is completely created by logging in to the mailbox at least once using the Outlook client or OWA access.
3. For each printer email address, create a new distribution group in the Exchange server.
4. Each Alias should reflect the printer name as created at PrinterOn.com.

    For example, boardroom-printer@company.com
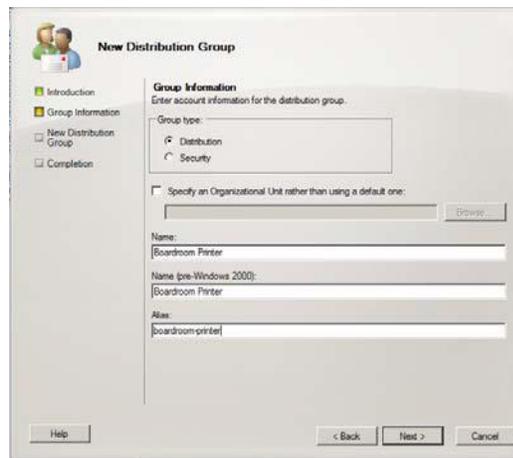
5. Once the group is created, modify the Distribution Group properties as necessary.
6. Go to the **Members** tab and click **Add**.

7. Select the main mobile print mailbox that was created in Step 1.
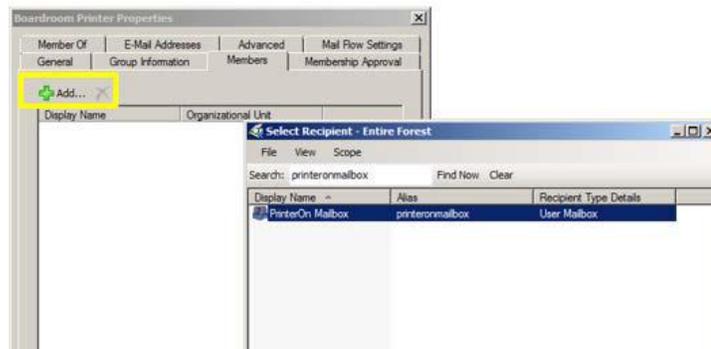
When completed, email messages are copied to the main print mailbox while the original recipient and sender information remain unchanged.

12.3.2.2 Setting up mail forwarding rules

To configure automatic mail forwarding:

1. Create individual user mailboxes for each printer and one for a main mobile print mailbox.

   This main mobile print mailbox can be named anything, for example printeronmailbox@mycompany.com.

2. Ensure each mailbox is completely created by logging in to the mailbox at least once using a service like Outlook.

3. For each mailbox, on the Exchange server, access the **Delivery Options**.
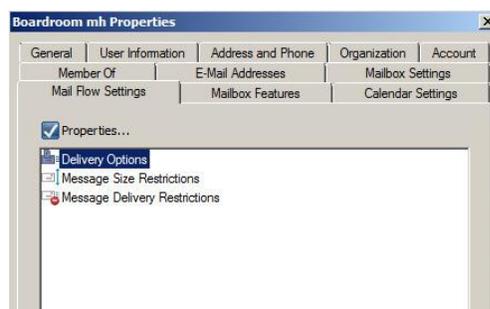
a) In the Delivery Options, check **Forward to:**, then browse for the central PrinterOn mailbox created in Step 1.
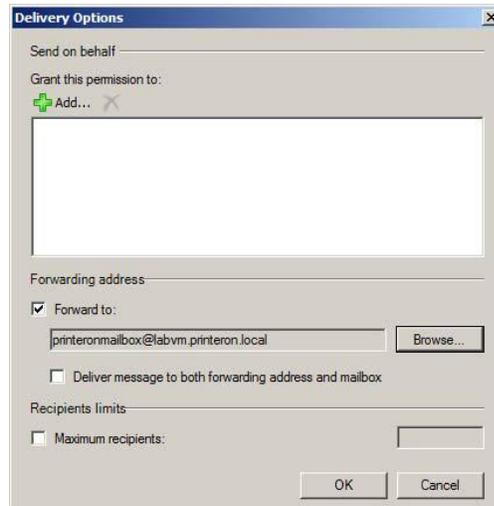
b) Leave the option **Deliver message to both forwarding address and mailbox** unchecked.

When completed, messages are copied to the main print mailbox and the original recipient and sender information is preserved.

12.4 Configuring email catch-alls

Email catch-alls are an important part of the PrinterOn email printing solution. The PrinterOn email plugin monitors a single mail folder for incoming messages. By using the mail server's catch-all capabilities, users can simply forward emails to the mail server using the printer's name in the email address. The catch-all directs all unknown emails to the mailbox monitored by the PrinterOn server.

How you configure an email server's catch-all feature varies from server to server.

12.4.1 Setting up a catch-all in Exchange 2010

For information about setting up a catch-all in Microsoft Exchange 2010, see the Knowledge Base article at the following location:

http://technet.microsoft.com/en-us/library/bb691132.aspx

12.4.2 Setting up a catch-all in hMailServer

The hMailServer (http://www.hmailserver.com) provides a simple configuration to support catch-alls. To configure catch-alls with the hMailServer review the following steps.

> **Note:** Before setting up the catch-all, you must first configure the PrinterOn server email print mailbox.

To set up a catch-all in hMailServer:

1. Launch the hMailServer administrator interface.
2. Click **Domains**, then click the domain configured for email printing.
3. Click **Advanced**.
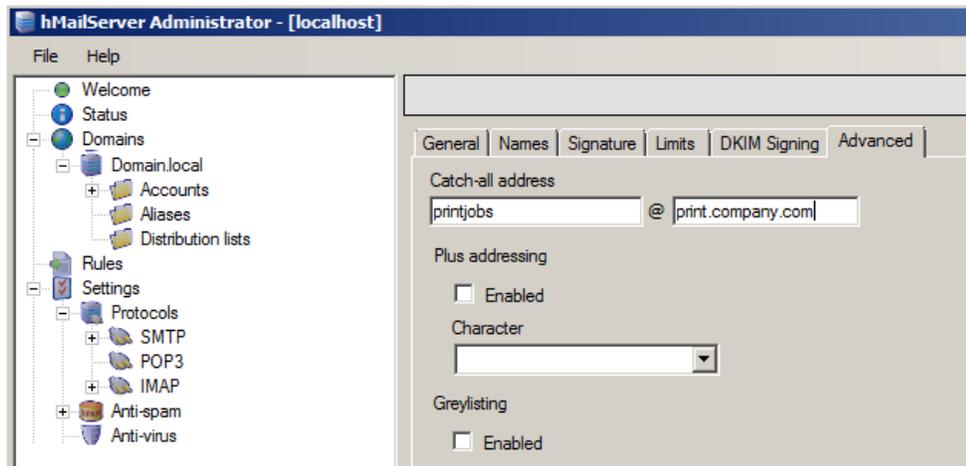
4. In the **Catch-all address** fields, enter the email address and domain of the PrinterOn mailbox.
5. Click **Save**.

12.4.3 Setting up a catch-all in Lotus Domino

The Lotus Domino server provides a simple configuration to support catch-all using the **Group** feature. When you create a new Group in the Domino Directory, you can specify the

registered users to be added to the group. There is no limit to the number of Domino user accounts that you can attach to a group.

> **Notes:**
>
> - Make sure that you have Editor or Author access with **GroupCreator** privileges.
> - Before setting up the catch-all, you must first configure the PrinterOn server email print mailbox.

To set up a catch-all in Lotus Domino:

1. From the Domino Administrator or Web Administrator, click **People & Groups**.
2. Select **Domino Directories > Groups**, then click **Add Group**.
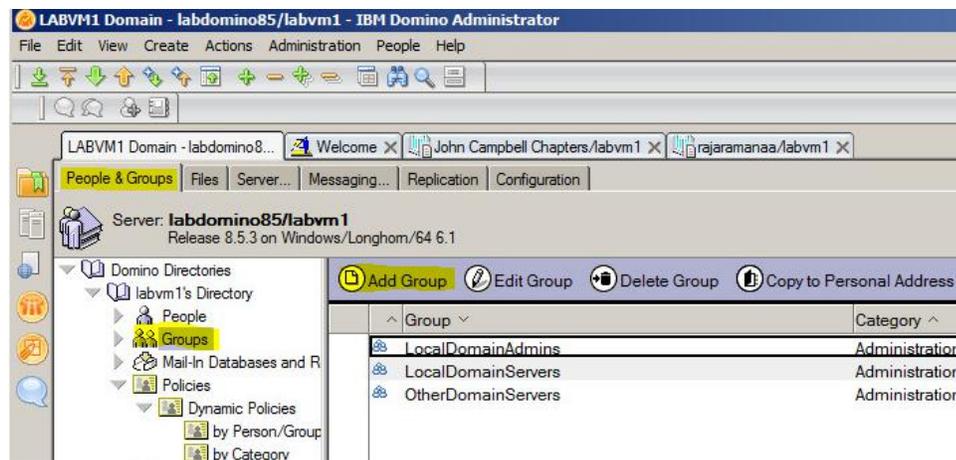
3. On the **Basics** tab, configure the following settings:

Setting	Description
Group Name	A descriptive name for the group.
Group Type	The type of group. Set to **Mail Only** to define the group as a mailing list.
Mail Domain	The Domino domain associated with the group's email address.
Internet Address	The email address for the group. This should be the printer's email address as defined on the PrinterOn.com PrintSpot; each printer must have a mail account created.
Members	The users of the mailing list. The PrinterOn mailbox must be added as a member.
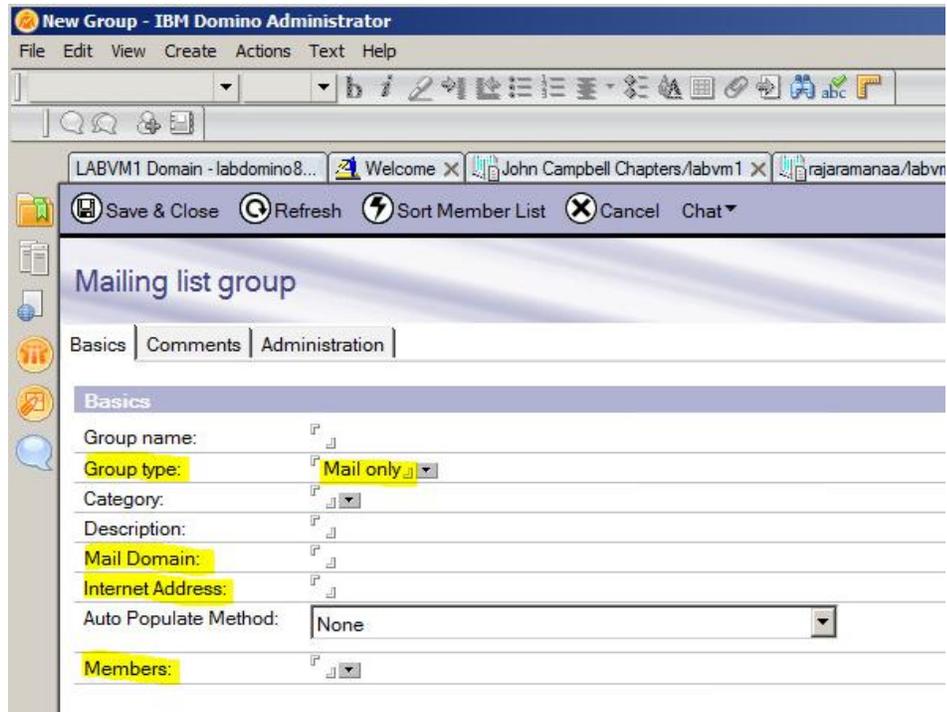
Note:

• **Internet Address** must be the printer's email address as defined on the PrinterOn.com PrintSpot. Each printer must have a mail account.

• The **Members** list must include the mailbox to be monitored by the PrinterOn server.

13

Reviewing service activity

In addition to service configuration functionality, the PrinterOn Configuration Manager Lets you generate a number of reports that you can use to monitor your PrinterOn service.

From the Reports tab of the Configuration Manager, you can view a wide range of activity information for your service. You can generate a single activity report for all printers attached to your service, or create a report for a specific printer.

You can export any report you generate to a CSV file so you can archive or present the data as necessary.

The Reports tab includes four subtabs:

Tab	Description
Summary	Generates a site summary report, providing high-level usage information for your PrinterOn service.
Printer	Generates a report of the activity for a single printer attached to your PrinterOn service.
Audit Trail	Generates an report of configuration activity for your PrinterOn service.
Advanced	Generates a variety of filtered activity reports for your service.

13.1 Creating a Site Summary report

The Summary tab lets you generate a site summary report for your PrinterOn service. A site summary report presents a three-month snapshot of usage statistics.

To create a site summary report:

1. In the Configuration Manager, click **Reports** > **Summary**. The server generates and displays the report.

2. To export the data, click **Export as CSV**.

13.2 Creating a printer activity report

The Printer Activity tab lets create a printer activity report, which outlines the activity of a single printer over a specified period of time.

To generate a printer activity report:

1. In the Configuration Manager, click **Reports** > **Printer Activity**. The Printer Activity panel appears.
2. From the **Printer** drop-down, choose which printer you want to generate a report for.
3. From the **Time Range** drop-downs, choose the start date and end date for the report.

4. Click **Generate Report**. The report is generated and data presented in a series of additional panels.

- The **Detailed Report** panel contains information about each job that was sent to the selected printer: when it was submitted, who submitted it, page and impression counts, whether it was printer in color, whether it was duplexed, and so on.

- The **Job Count** and **Impression Count** panels display graphs that illustrate various stats.
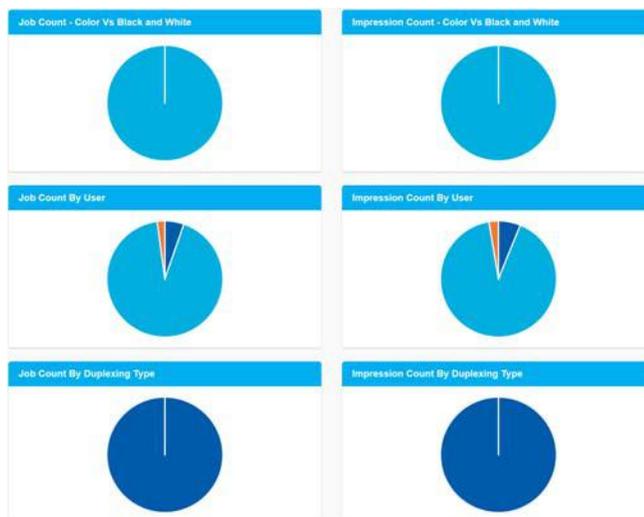
5. To export the data, click **Export as CSV**.

13.3 Creating an Audit Trail report

The Audit Trail tab lets you audit the configuration activity for your PrinterOn service. The Configuration Manager logs all changes made to the service settings, such as changing a printer configuration, adding user accounts, or disabling a workflow. An audit trail report lets you review those changes, and can help you to troubleshoot performance issues and to maintain the integrity and security of the service.

Audit trail reports are customizable; you can specify the type of data included in the report

To generate an audit trail report:

1. In the Configuration Manager, click **Reports** > **Audit Trail**. The Audit Trail tab appears.

2. In the Audit Trail Filter panel, constrain the content of the audit report by specifying filter criteria:

Criteria	
Resource Type	Returns audit data only for the specified resource type.
Affected Resource ID	Returns audit data only for the specified resource ID.
Performed By	Returns audit data only for the specified user(s).
Time Range	Returns audit data logged within the specified start date and end date.

3. Click **Generate Report**. The report is generated and presented in a table.

4. To export the data, click **Export as CSV**.

13.3.1 Managing audit trail data

As administrators modify the configuration of your PrinterOn service, the Configuration Manager audit trail data continues to accrue. Over time, older data may no longer need to be saved. The Audit Trail tab allows you to clear your oldest records.

To purge obsolete audit trail data:

1. In the Configuration Manager, click **Reports** > **Audit Trail**. The Audit Trail tab appears.

2. Locate the **Clear Old Records** panel.

3. Choose how you'd like to identify which records to clear:

    •   **Remove audit trail before**: Removes all audit trail entries that occurred before the specified date.

    •   **Remove Oldest**: Removes the oldest specified number of entries.

4. Click **Delete**.

13.4 Creating advanced reports

The Advanced tab lets you create of predefined reports, which distill the data and filter it to display more focused usage reports that provide additional insight into how the service is being used, who is using it, and what issues they are encountering.

The Configuration Manager provides six different predefined reports:

- **Top 5 most used printers**: Displays which were the most active printers over the specified time period.
- **Job count by user type**: Displays the most common types of users using the service over the specified time period.
- **Top 5 most active departments**: Shows which departments submitted the most print jobs over the specified time period.
- **Top 10 most common errors**: Shows which errors were encountered most over the specified time period.
- **Job count - Color vs black and white**: Shows the frequency of jobs submitted as color print jobs versus those submitted as black and white over the specified time period.
- **Top 5 most used applications**: Shows the applications most commonly used to create the documents submitted for printing over the specified time period.

To generate an advanced report:

1. In the Configuration Manager, click **Reports** > **Advanced**. The Advanced tab appears.
2. For one of the report types, from the **Time Range** drop-downs, specify a start data and end date.
3. Click **Generate Report**. The report is generated and presented in a chart.
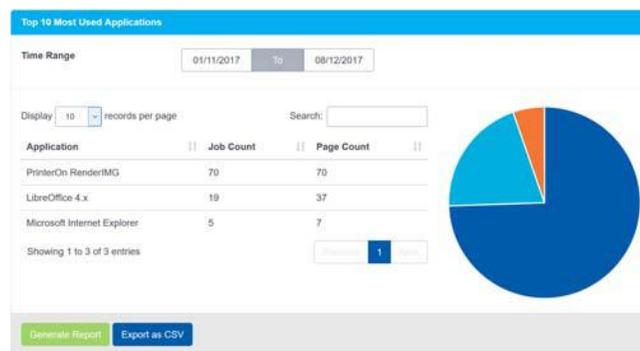
4. To export the data, click **Export as CSV**.

5. Repeat Steps 2-4 for any other advanced report type you want to create.

14

Recommendations for service monitoring

Many administrators and service providers leverage centralized notification and monitoring tools. PrinterOn's own Public Cloud services leverage monitoring tools such as Nagios, which is configured to monitor key metrics for a variety of systems. These tools provide notifications to IT support based on configured thresholds and service metrics.

The following information is provided as a reference only; each implementation and service design inherits certain custom characteristics. The following should be used as a guideline for your own monitoring service and should be adapted to your specific needs.

The tables below describe certain thresholds that may be used to initiate an automated notification to support staff. The values provided do not always indicate a problem or fault; they are sometimes indicative of possible future problems or may simply indicate that the server status or logs should be reviewed manually.

14.1 PrintAnywhere Status Server

Monitoring Metric	Thresholds and Action(s)	Frequency recommendation
Memory	• > 100MB Allocated • Clear PrintAnywhere JobRecords Folder • Restart Service	• Check 5 min interval • Memory consistent across 2 intervals
CPU	• > 50% utilization • Restart Service	• Check 5 min interval • Memory consistent across 2 intervals
Process Failure	• Allow Auto-restart up to 2 times • Subsequent failures require service cleanup and log review	

14.2 PrintAnywhere Processing Server

Monitoring Metric	Thresholds and Action(s)	Frequency recommendation
Memory	• > 250MB Allocated • Clear PrintAnywhereStorage Folder • Restart Service • Restart Server	• Check 5 min interval • Memory consistent across 2 intervals
CPU	• > 50% utilization • Restart Service • Clear PrintWhere Spool Directory • Restart Server	• Check 5 min interval • Consistent CPU usage across 2 checkpoints • CPU spikes for up to 4 minutes generally accepted

Monitoring Metric	Thresholds and Action(s)	Frequency recommendation
Process Failure	• Allow Auto-restart up to 1 time The Processing Server contains complex server management tools to attempt to self-heal the print subsystem. If the Processing Server cannot fix itself, the Print Subsystem it will shut itself off. • After auto-shutoff review logs for re-registration notifications • Restart Server and re-install PrintWhere	

14.3 PrintAnywhere PASPort Server

Monitoring Metric	Thresholds and Action(s)	Frequency recommendation
Memory	• > 100MB Allocated • Restart Service • Restart Server	• Check 5 min interval • Memory consistent across 2 intervals
CPU	• > 50% utilization • Restart Service • Restart Server • > 5 messages pending in the managed mailbox inbox • Restart Service • Clear Monitored Mailbox of messages.	• Check 5 min interval • Consistent CPU usage across 2 checkpoints • CPU spikes for up to 4 minutes generally accepted
Process Failure	• Allow Auto-restart up to 1 time • After auto-shutoff review logs for re-registration notifications	

14.4 CPS Tomcat

Monitoring Metric	Thresholds and Action(s)	Frequency recommendation
Memory	• > 200MB Allocated • Restart Service	• Check 5 min interval • Memory consistent across 2 intervals
CPU	• 50% utilization • Restart Service	• Check 5 min interval • Memory consistent across 2 intervals
Process Failure	• Allow Auto-restart up to 2 times • Subsequent failures require service cleanup and log review	

14.5 PWCRoute.exe

Monitoring Metric	Thresholds and Action(s)	Frequency recommendation
Memory	• > 250MB Allocated • Restart Processing Server Service • Clear PrintWhere Spool Directory • Restart Sever	• Check 5 min interval • Memory consistent across 2 intervals
CPU	• > 50% utilization • Restart Service	• Check 5 min interval • Memory consistent across 2 intervals
Process Failure	N/A	

14.6 Windows Print Spooler

Monitoring Metric	Thresholds and Action(s)	Frequency recommendation
Memory	• > 768MB Allocated • Restart Service • Restart Server	• Check 5 min interval • Memory consistent across 2 intervals
CPU	• > 50% utilization • Restart Service	• Check 5 min interval • Memory consistent across 2 intervals
Process Failure	• Allow Auto-restart up to 2 times • Subsequent failures require service cleanup and log review	

15

Troubleshooting problems

To address an unexpected issue with the Enterprise server, determining where and what component is at fault is a critical part of the process. The following is intended to provide assistance with this process. The process will involve investigating major components or the communication between them.

15.1 High Level Overview

A few key symptoms and information may assist in reducing the problem space significantly. The Enterprise system may be divided into 3 primary divisions:

- **Submission & Job Reception**: Includes API clients, CPS and PrintAnywhere Status Server.
- **Job Processing/Printing**: Includes primarily the PrintAnywhere server, and may be impacted by access to end point printers or services.
- **Job Delivery**: Includes PDS, PDH and HotSpot printers. Impacts submission from the PrintAnywhere Server.

In addition to these 3 items the overall configuration may be the cause of an issue. That overall configuration and the information that binds the systems together will also be discussed below.

15.2 Key Troubleshooting Data Points

Two key data points may be used to help assist and rapidly divide the problem space into smaller pieces:

- Job Reference ID
- User Messages

These do not always identify the root cause of the issue but do aid with a rapid assessment of where to review.

15.2.1 Job Reference ID

Once a job has been accepted by the PrintAnywhere Server, a Job Reference ID is attached to the job, specifically the Status Server subcomponent. The presence or absence of a Job Reference ID provides a major clue where to start investigating issues.

If a Job Reference ID...	It is highly likely that...	Troubleshooting should focus on...
was not returned	- The job did not get submitted to the Status Server - The problem resides in CPS - The problem resides in the data submitted with the request including: - Missing required parameters - Missing or corrupt data file - Invalid API format	- CPS & Tomcat logs - Status Server logs
was returned	- The job was received by the PrintAnywhere Server - The problem resides within the PrintAnywhere Server - The problems may include: - Invalid printer information - Communication issues amongst PrintAnywhere components - Issues printing specific documents	- Status Server logs - Processing Server logs

15.2.2 User Messages

Once a job has been accepted by the service, specifically PrintAnywhere, all messages will be returned with a code prefix that helps identify the component that reported the message.

For Example:

- PAS0108 – Returned from PrintAnywhere
- PWC0100 – Returned from PrintWhere

This information can be used to quickly isolate whether the issue was caused by PrintAnywhere, PrintWhere communication, or other components.

Generally, the User Message contains the message ID from the component that originated the message. For example, an issue may originate in communication between PrintWhere and the destination device, or in PrintAnywhere when handling a document. The message prefix will help isolate this information. For example:

- PAS0002: The job has been processed.
- PWC4510: Unable to contact the printer.

Messaging Prefix	Base reporting component
PAS	PrintAnywhere
PWC	PrintWhere
PTS	Configuration and Licensing
FCS	Print Delivery Station

16

Adding printers in hybrid deployments

If you have a hybrid deployment and wish to add more devices or additional print management queues, you can do so from the PrinterOn web admin portal. Your ability to add new printers to your deployment is determined by your license. From the homepage of the PrinterOn web administration portal, you can confirm how many printer listings are currently added, as well as the total permitted by your license.

PrintSpot Summary ❓ About your PrintSpot Summary

Printspot Name:	
PrintSpot Type:	PrintSpot Enterprise
Service URL	
Service ID :	
Annual Renewal Date:	
Production Status:	
PrintSpot Language:	English [Change]
Show/Hide your PrintSpot in searches	Shown [Change]
License Information	Manage License
Annual Renewal Date:	
Checked License On:	
Number of Printers:	2
Number of Printers Licensed:	3

Manage Access Control Lists

Create a new PrintSpot under a new group

Create User Account

Change Group

☒ Delete this PrintSpot

16.1 Adding printers

To add more printers or additional print management queues in a hybrid deployment:

1. Log in to the PrinterOn.com web admin portal at www.printeron.com/administrators.

2. Click the **Printers** icon ![icon].

3. Click **Add a Printer to your PrintSpot**.

Manage your Printers for Infinite Lighting Corporate

Here you will find the printers associated with your PrintSpot, listed as they would appear t availability of each printer. To change your printer settings, click the link in the printer sumr

Add a printer to your Printspot

> **Note:** If this link is not displayed, please review your license information. If you have already reached your permitted number of printers, you can not add any more without changing the terms of your license agreement.

The Printer Configuration page appears. In most cases, the default settings should be sufficient, but you should review the settings to confirm.

4. Click the **Required Settings** tab and configure the required settings as necessary.

5. Click the **Optional Settings** tab and configure the optional settings as necessary.

6. Click the **Payment &Authorization** tab and configure the payment and authorization settings as necessary.

7. Click **Save**.

16.1.1 Configuring required settings

Required Settings are divided into the following groups:

*   Basic printer configuration settings
*   Web, PrintWhere, and Email Print settings

16.1.1.1 Basic printer configuration settings

Setting	Description
Print driver	The printer driver used to process any jobs sent to the printer. By default, a Generic PCL6 driver is specified. If your device does not support the default print driver, choose an alternate driver from the drop-downs. Printer drivers are sorted by manufacturer. First, select the printer driver manufacturer from the upper list, then select the printer driver from the lower list. If your specific printer model is not available, please choose an appropriate universal driver from your manufacturer. When sending print jobs to a managed pull queue, ensure that all devices within the pull group support the driver.
Manufacturer	The manufacturer of the printer, as shown to the user.
Model	Printer driver information that is presented to the user when viewing printer details. This value does not need to match the actual printer model.
Printer Model Name	The printer model name. This field is only used when you specified Samsung as the Printer Driver manufacturer and Samsung Universal EMU V2 as the printer driver, and allows the PrinterOn to optimize output for specific Samsung printer models. If you don't know the specific model, select **UnsupportedMono** or **UnsupportedColor**.
Descriptive Printer Label	A descriptive label that describes the printer to users. The value should be unique and descriptive. **Note:** PrinterOn does not enforce uniqueness on this value, but recommends that you set this value to a simple and easy-to-understand label for the printer.
External ID	The external ID for this printer.

16.1.1.2 Web, PrintWhere, and Email Print settings

Setting	Description
PrinterOn Name	A unique printer queue name used throughout the software to both identify and organize printers. This value is combined with the email domain to create the email address for the printer, to which users can email print jobs. For example: warehouse-printer-1@emailprint.com PrinterOn recommends using your internal naming convention when available.
Department	The Printer Department to which the printer belongs. The drop-down list only lists existing departments.
Default Printer Language	The default language for the printer, which the server uses to respond to email print jobs.
PrinterID	A unique QR code for the printer. Click the **QR Code** button to generate the QR code.
PrintWhere	When checked, workflows including mobile apps, GCP and iOS Native Print are allowed to be submitted to the printer.
Document API	When checked, the Document API URI is the URL returned by the server to the Mobile Apps when searching for printers. It is used by the App to submit documents to the server. By enabling this option, you can provide a value in the Document API URI.
Doc API URL	Specifies a Document API URI that is used when you enable the **Document API** setting. This value overrides the value configured on the PrinterOn Directory.
Email Domain	The email domain that should be appended to the printer name when advertising email print addresses to users.
Email Printing	When checked, email print is enabled for this queue. If disabled, users receive a message indicating the service is disabled. **Print Body of Email**: When checked, the body of an email is printed when receiving email print jobs. If disabled, only attachments are printed.

16.1.2 Configuring optional settings

Required Settings are divided into the following groups of settings:

- Job and User Information settings
- Release settings and Advanced Integration Options
- Output Options
- Print Delivery Station settings

16.1.2.1 Job and User Information settings

Setting	Description
User Identifier	Specifies whether the user is asked to provide Job Owner information that will be included with a print job. If you select **Optional** or **Required**, in the adjacent text box, specify the text displayed to request the user's name. If authentication will be used, you should enable this setting.
Computer Name	Specified whether the computer name is submitted with the request.
Client UID	Used in combination with custom integrations of third-party solutions to request user information. If you select **Optional** or **Required**, in the adjacent text box, specify the text displayed to request the Client UID. When the adjacent **Secured** check box is enabled, the server does not save the Client UID.
Session Meta Data	Used in combination with custom integrations of third-party solutions to request user information. If you select **Optional** or **Required**, in the adjacent text box, specify the text displayed to request the session metadata. When the adjacent **Secured** check box is enabled, the server does not save the session metadata.

Setting	Description
Anonymity Level	Defines what information is reported from PDS to the reporting server. Typically, reported information includes print job results and some page metrics, such as page counts and formats.
	Select one of the following values:
	• **None**: No anonymity is applied.
	• **Optional**: The PDS uses the Anonymity Level configured for the printer in the PrinterOn Directory. No local overriding rules are applied.
	• **Anonymous**: Suppresses Job Name and Job Owner.
	• **Minimal**: Includes basic job details, such as page count and job size.
	• **Anonymous + Minimal**: Combines options from both Anonymous and Minimal.

16.1.2.2 Release settings and Advanced Integration Options

Setting	Description
Privacy Release Code	Indicates if users must provide a release code to retrieve their print jobs. You should typically set this value to **Required** or **Optional** when using a PrinterOn Print Valet or embedded agent that supports entering a release code.
Releasing Print Jobs	How print jobs are released. There are two options:
	• **Automatically when they arrive**: When selected, print jobs are automatically released to the printer or print queues without being held.
	When integrating with most print/output management solutions, you should select this option.
	• **Using a PrinterOn Solution or HotSpot printer**: Print jobs are released using a PrinterOn solution. Users must supply a Release Code or other identifying information to access their print jobs.
	If jobs are to be held for secure release through a PrinterOn agent, you should select this option.
Enable 3rd Part Integration	When checked, lets you set the following settings to define release settings for your third-party Print Management Integrations:

Setting	Description
Inject a PJL Header container if none exists	When checked, the PrinterOn Server injects a PJL header into the print job. Many printers and print/output management solutions use PJL headers to collect job information. Some print drivers do not automatically include these PJL headers. If you encounter issues with your integration, enabling this option may be required.
Manage PJL headers for Passthrough Jobs	When checked, the PrinterOn Server modifies PJL headers. PrinterOn is able deliver print jobs from 3rd party systems through the print service. In some cases, those jobs may be pre-rendered data that contains PJL headers. This setting allows the PrinterOn server to process and modify these headers as necessary to prevent jobs from failing.
Inject PJL Based Copies	When checked, the PrinterOn Sever injects PJL-based copies. Some printers and MFPs support managing print copies though PJL headers instead of in the print data stream itself. If the printer connected to the queue supports PJL-based copies, enabling this option may reduce print data size when multiple copies are printed.

16.1.2.3 Output Options

Setting	Description
Cover Pages	When checked, a cover page is added to each print job, identifying the sender and the time the job was submitted.
Color printing	Defines whether color printing is supported. This setting allows users searching for printers to limit their search to those printers that support color. If you have a color printer but wish to discourage users from printing in color, select **Does not support color**.
PJL Encoding	Specifies the Printer Job Language encoding. If your printer needs to support double byte characters, set this to UTF-8, and check the **Override Encoding Specification**.
Max. page count	The maximum number of pages a print job may use. Print requests exceeding this limit will are accepted. The maximum page count includes the cover page.
Max. printed size	The maximum data size of a print job. Print requests exceeding this limit will are accepted.

Setting	Description
Duplexing	Defines the duplexing configuration. If you prefer to let the printer control duplexing, select **Not Managed**.
Paper sizes	The paper sizes are available for the printer and manage what paper-selection options the user can choose when they print.

16.1.2.4 Print Delivery Station settings

Setting	Description
Allow Printing Directly to PDS	When checked, indicates that print jobs are sent to the PDS server. **Note:** Only select this option if the PDS is accessible from the main server. In some cases, print jobs can only be delivered to a PDS using an intermediate Print Delivery Hub (PDH).
Server Address	The fully qualified network address of the Print Delivery Station server. Select a scheme to indicate whether SSL will be used. Usually this is simply the local server. **Note:** As a best practice, you should specify an explicit port along with the server address to improve print performance. The server automatically selects the specified port, if supplied. Otherwise, it scans ports 80, 443, and 631, as well as SSL and non-SSL connections, which can slow delivery.
Print Directly to PDS Only	When checked, all print jobs are printed directly to the PDS, and are not sent to a PDH. This setting only applies if a PDH is available. In most cases, you should enable this setting.
Use an alternate/local Print Delivery Hub to host print jobs	When checked, indicates that a Print Delivery Hub server is available for printing. This option should be specified if a PDS is accessible directly by the server. In some cases, this option may be used if multiple PDS servers are deployed for the same printer, for redundancy. Configuring both a PDS and PDH server can assist desktop printing using PrintWhere for roaming users who may move between networks regularly and cannot always contact PDS. When checked, you must specify the fully qualified network address of the PDH server.

16.1.3 Configuring the Payment & Authorization settings

Setting	Description
Guests will be charged for printing	When checked, users are charged a fee for each print job sent to this printer. When you enable this setting, additional settings appear, letting you define the specific payment details, such as currency, cost per page, and others.
Requires Authentication to Print	When checked, users are prompted for their credentials when scanning the QR code via the PrinterOn mobile apps.
Redirect to authorize user, track pages or bill customer	When checked, users are redirected to a specified URL for authorization.

When you enable this setting, additional settings appear, letting you define the **User Authentication URL**, **Web Authorize URL**, and **Mobile Authorize URL**. To supply a URL, check the adjacent check box, then enter the URL in the text field. |

16.2 Configuring printer location settings

You can set a unique address and GPS co-ordinates set for each printer listing within the PrinterOn directory.

To configure printer location settings:

1. Log in to the PrinterOn.com web admin portal at www.printeron.com/administrators.

2. Click the **Printers** icon .

3. In the list of printers, locate the printer you want to define location information for, then click **Set Address** from the **Options** list.

Printer name and address		Features	? Legend	Options
				Take printer Offline
		🔲 🇬🇧		Set Address
🖨 **Enterprise Printer**				Set Printer Language
				Printer Departments
[300581145793] **mycompany1**				Hide in Searches
221 McIntyre Dr				Copy Printer Settings
Kitchener, ON N2R1G1				Server Configuration
Canada				Printer Formats
				Delete
Required Settings Optional Settings Payment & Authorization				

4. Configure the following settings:

Setting	Description
Address1, Address2, City, Zip/Postal Code, Country, State/Province	The physical address for the printer. Mobile app users looking for a PrinterOn enabled printer can search on any value of the address to locate a printer. The mobile app also displays the address in the Printer Details.
Latitude, Longitude	The GPS coordinates for the location of the printer. The GPS coordinates are used to display the printer location on a map when users attempt to locate a printer using the PrinterOn Mobile app. Click **Get Geo Coordinates** to get the latitude and longitude of the address you provided.
Show map in searches	When checked, the printer location will be displayed in a map in searches by users using the PrinterOn Mobile Apps.

16.3 Updating the Service URL

The Service URL (shown in the **Site Summary** box on the web admin portal homepage) is an important factor in supporting API submissions. API submissions refer to submissions made by mobile apps, native iOS, IPP, Google Cloud Print, and any custom submission applications you may have created based on PrinterOn APIs.

You can update the Service URL from the PrinterOn.com web admin portal.

To configure the Service URL:

1. Log in to the PrinterOn.com web admin portal at www.printeron.com/administrators.

2. Click the **Service Details** icon 📋 .

3. Locate the **Account Profile** section, at the bottom of the page.

4. In the **Service URL** field, enter the IP or DNS address for the server hosting your PrinterOn software. You must append /cps to the end of the address. For example:

   http://print.company.com/cps

   > **Note:** In a multi-server environment, this value should reflect the address users will visit to complete a web submission. This is most likely a load-balanced address.

5. Click **Update**.

A

Advanced configuration settings

Beginning with version 3.2.1, you can display the Configuration Manager in two views:

- **Basic view**: Displays commonly configured settings.
- **Advanced view**: Displays all Basic view settings plus additional advanced settings. Advanced settings are those that are only rarely configured or are specific to a particular deployment.

By default, the Configuration Manager opens in Basic view. You can toggle between the two views using the **Show Advanced Settings** switch on the **Settings** menu. As you turn Advanced view on and off, the interface is updated in real time.

This chapter provides a list of Advanced settings. In most cases, you won't need to configure these settings.

To view these settings, you must turn on the **Show Advanced Settings** toggle.

To show or hide advanced settings:

1. In the Configuration Manager, click the **Settings** button ( ).
2. Click **Show Advanced Settings** to toggle advanced settings on or off.
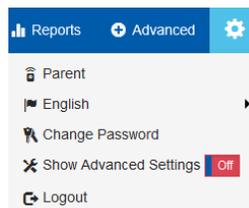
A.1 Advanced settings list

The following table lists all settings that only appear in the Configuration Manager in Advanced view.

Location	Advanced Settings
Home > **General Settings**	• **Printer Synchronization Settings** panel • **Advertised Capabilities** panel
Workflow > **Web Print**	Advanced settings in the **Web Presentation** panel: • **Job Submit Refresh Interval** • **Job Approval** • **Smart Printer Selection** • **Department Sidebar View** • **Number of Printers Displayed Per Page** • **Number of Departments Displayed Per Page**
Workflow > **Email Print**	• **Accept Request to response address** setting (all email types) • **Advanced Email Settings** panel (all email types)
Workflow > **PQMS**	**PQMS Settings** panel
Workflow > **IPP and Native iOS Printing**	Advanced settings in the **Network Broadcast Settings** panel: • **Additional Port** settings
Authentication > **Authentication** > **LDAP/AD**	Advanced settings in the **LDAP/AD Settings** panel: • **Trusted Application Behavior** • **Web Authentication Enabled for Mobile** Advanced settings in the **LDAP/AD Profile Details** panel: • **Mode** • **Follow LDAP Referrals** • **Prepend "smtp:" to E-Mail Address Searching** • **Enable Configuration Manager Access** • **User Display Name Attribute** • **User First Name Attribute** • **User Surname Attribute** • **User Phone Number Attribute(s)**

Location	Advanced Settings
Authentication > Authentication > Azure AD	Advanced settings in the **Azure AD Settings** panel: • **Prefer UserInfo API Over Graph API** • **Preferred User ID Claim** • **Prompt**
Authentication > Authentication > Third-Party Identity Management Service	Advanced settings in the **Third-Party Identity Management Service Settings** panel: • **Preferred User ID Claim** • **Echo Refresh Token for Clients** • **Prompt** • **Resource**
Authentication > Authentication	Advanced settings in all Authentication Methods on the **Authentication** tabs: • **Trusted Application Behavior** (all authentication methods)
Printers > Printers > Configure **Printers > Secure Release Anywhere Pools > Configure**	• **Web Services ID in the Printer Configuration section** • **Labels** section • Advanced settings in the **Job and User Information** section: • **Client UID** • **Session Meta Data** • Advanced settings in the **Releasing Print Jobs** section: • **Always use numbered release codes** • **Auto-generate release codes** • All Third-Party Integration settings • Advanced settings in the **Finishing Options** section: • **PJL Encoding** • **Override Encoding Specification**
Settings (⚙) > Settings	• **Authentication Settings** panel

Location	Advanced Settings

PDH >Internet Communication	• Advanced settings in the **Print Delivery Station Communication** section:
	
	  • **JWT-Based User Authentication**
	
	  • **Allowed JWT Issuer Suffixes**
	
	  • **JWT Signature Validation**
	
	  • **Enable PerPdsPdh Password**
	
	  • **PDH Endpoint Password**
	
	  • **CPS Signing URL**
	
	  • **JWKS URL**

B

PrinterOn system requirements

Before installing and configuring PrinterOn, you should ensure that you have met the following requirements:

- System account requirements
- Hardware requirements
- Software requirements
- Network communication requirements

B.1 System account requirements

You must have **Local Administrator** access on the computer that will run the PrinterOn software. You should create a dedicated account for PrinterOn. The administrator account must have a password (a blank password is not allowed).

B.2 Hardware requirements

PrinterOn has the following hardware requirements:

- A dedicated physical server or virtual machine
- Intel compatible processor with 2GHz multi-core processor (quad-core recommended)
- 4 GB RAM minimum for dedicated servers (8 GB recommended)

- 10 GB of disk space for PrinterOn software and third-party applications (20 GB recommended)

B.3 Software requirements

PrinterOn has a number of software requirements, recommendations, and limitations. You should be aware of these requirements before installing the PrinterOn software:

- Required software
- Recommended software
- Software that should be removed or disabled
- SQL Server installation requirements and issues

B.3.1 Required software

PrinterOn requires the following software:

Software	Requirement
Windows Server	PrinterOn supports the following: • Windows Server 2012 including 2012 R2 with current patches installed (Datacenter and Standard Editions) • Windows Server 2016 (Datacenter and Standard Editions) • Windows Server 2019 (Datacenter and Standard Editions)
Internet Explorer	Internet Explorer 10 or later with latest patches.
SSL Certificates	PrinterOn recommends as best practice that you deploy digitally signed SSL Certificates from a recognized certificate authority.

B.3.2 Recommended software

Where possible, PrinterOn uses native applications for rendering. For the greatest quality output, you should ensure that the native applications for the documents being printed are installed on the same machine as your PrinterOn software.

For example, printing Microsoft Office documents with LibreOffice will not provide the same output quality.

Software	Requirement
Microsoft Office	Microsoft Office 2010 to Microsoft Office 2019/ Microsoft Office 365 (Office 2016 or later recommended), including Word, Excel, PowerPoint, and Visio. If you are integrating PrinterOn with Microsoft Exchange, installing Microsoft Outlook is also recommended. **Note:** You should start each application included with Office at least once to ensure that they are properly installed and fully functional.
OpenOffice/LibreOffice	OpenOffice.org **OR** LibreOffice 5.0 or later (32-bit only) recommended. Only one of OpenOffice or LibreOffice should be installed at one time. **Note:** You should start each application included with OpenOffice/LibreOffice at least once to ensure that they are properly installed and fully functional.

B.3.3 Software that should be removed or disabled

The PrinterOn installation includes the following software:

- Apache Tomcat
- Microsoft SQL Server Express 2016
- Microsoft .NET Framework 4.5.1 and Microsoft .NET Framework 4 (installed by SQL Server)

Prior to installing PrinterOn, make sure that the following software is either not installed or disabled:

Software	Requirement
Internet Information Services (IIS)	If you have Internet Information Services (IIS) installed on your server, make sure that it is **disabled**. IIS interferes with the Tomcat installation.

Software	Requirement
Microsoft SQL Software	Ensure that there are **no other instances** of SQL Server installed.

B.3.4 SQL Server installation requirements and issues

Beginning with PrinterOn Enterprise 4.2.3, the PrinterOn installation includes a copy of Microsoft SQL Server Express 2016. Previous versions included Microsoft SQL Server Express 2014.

> **Note:** If you are upgrading a previous installation of PrinterOn Enterprise, the installer will not upgrade the SQL Server software. SQL Server Express 2016 is only installed with new installations.

If any issues are found during the installation of the SQL Server, it is recommended that you manually install the Microsoft .NET framework prior to installing the PrinterOn software.

> **Important!**   The version of SQL Server Express that is installed with PrinterOn requires that TLS v1.0 is enabled on the host computer. However, by default, PrinterOn disables TLS v1.0 on the host computer during the installation process. As a result, if you intend to use the PrinterOn-installed version of SQL Server, you must enable TLS v1.0 on the host machine.

You can also choose to use an alternative database, rather than use the SQL Server Express instance installed with the PrinterOn software. PrinterOn supports the following databases:

Software	Requirement
Microsoft SQL Software	The PrinterOn server supports the following versions of SQL Server: • SQL Server 2012, 2014, 2016

B.4 Network communication requirements

To ensure that PrinterOn has no network communication issues, make sure that your server meets the following requirements:

Consideration	Requirement
Port	For internal network communication, ensure that the server has inbound and outbound access on port 443. It is recommended, but not required, to have ports 80 and 631 available also.
Network routing permissions	If you intend to set up a Hybrid deployment of PrinterOn, ensure that the DNS and network routing allows PrinterOn to communicate with the following addresses: • http://www.printeron.net • https://secure1.printeron.net • https://download1.printeron.net
Internet access	If you intend to set up a Hybrid deployment of PrinterOn, ensure that Internet access is available at all times.

C
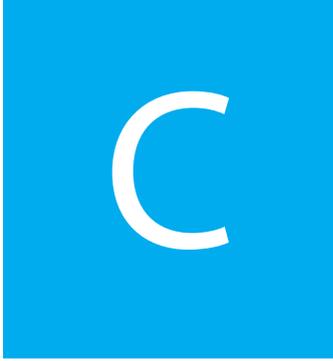
Securing PrinterOn

PrinterOn Enterprise/Express is intended to provide a secure printing solution, and includes many features to ensure that it's components, and the print data that they manage, are kept secure.

Although PrinterOn components are designed with security in mind, PrinterOn also relies on Apache Tomcat, a third-party component used for communication across networks. To achieve the highest level of security, you may need to manually configure the Tomcat settings.

This chapter has the following sections:

- PrinterOn changes to Windows default SSL settings
- Enabling TLS support in Tomcat
- Using encrypted passwords for PrinterOn Enterprise/Express

C.1 PrinterOn changes to Windows default SSL settings

By default, Windows is configured to use less secure SSLv3 and TLSv1 protocols. These protocols do not meet the security requirements of most security-conscious services such as PrinterOn.

As of version 4.0, PrinterOn Enterprise pro-actively implements the highest security standard protocols, TLSv1.1 and TLSv1.2. By default, SSLv3 and TLSv1 are disabled due to known vulnerabilities. Clients such as PrintWhere also pro-actively disable these protocols during installation.

C.2 Enabling TLS support in Tomcat

Configuring TLS for your installation may vary slightly depending on your preferred criteria.

It is recommended that you review and follow the steps provided by Apache for completing the process. Detailed instructions regarding the process can be found at: tomcat.apache.org/tomcat-8.0-doc/ssl-howto.html.

The steps below are used to create a self-signed certificate for use with your service. Many applications and browsers will warn any user accessing your service that the site may not be secure if you deploy a self-signed certificate. For best results receiving a valid signed certificate from a Certificate Authority is recommended.

To create a self-signed certificate for use with your PrinterOn service:

1. Create the certificate:

   a) On the command line, go to *<JRE_Install_Dir>*\bin

   b) Run the following command:

   ```
   keytool -genkey -alias tomcat -keyalg RSA
   ```
   Your keystore will be stored in the home directory of the user under which you ran the command.

2. Configure the certificate:

   a) Create a password and follow the prompts that follow. The information you enter here is displayed to users who access a secure page in your application. Make sure it matches what users would expect to see.

   > **Important!** Your Private Key and Keystore passwords should be the same.

3. Configure Tomcat:

a) In a text editor, open C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\Conf\server.xml.

b) Locate the following entry:

```
<!-- Define a SSL HTTP/1.1 Connector on port 443
<Connector port="443"
    protocol="com.printeron.tomcat.http11.Http11NioProtocol"
    SSLEnabled="true" maxThreads="150" scheme="https"
    secure="true" clientAuth="false"
    sslEnabledProtocols="TLSv1.1,TLSv1.2"
    keystoreFile="${pon.data.root}\KeyStore\keystore"
    keystorePass="rz6KZSpMD7fy7Co6UfIBmw%3D%3D"
/>
```

c) Remove the comment fields surrounding the Connector port and edit the highlighted code below for your preferred implementation:

- SSL using JSSE:

```
<Connector port="443"
    protocol="org.apache.coyote.http11.Http11NioProtocol"
    SSLEnabled="true" maxThreads="150" scheme="https"
    secure="true" clientAuth="false"
    sslEnabledProtocols="TLSv1.1,TLSv1.2"
    keystoreFile="C:\Path\to\keystore\.keystore"
    keystorePass="keystore password"
/>
```

- SSL using APR:

```
<Connector port="443"
    protocol="org.apache.coyote.http11.Http11AprProtocol"
    SSLEnabled="true" maxThreads="150" scheme="https"
    secure="true" clientAuth="optional"
    sslEnabledProtocols="TLSv1.1,TLSv1.2"
    SSLCertificateFile="C:\Path\to\certificate\server.crt"
    SSLCertificateKeyFile=" C:\Path\to\certificateKey\server.pem"
    SSLPassword="changeit"
/>
```

d) Save the file.

C.3 Using encrypted passwords for PrinterOn Enterprise/ Express

With version 3.2.4, PrinterOn Enterprise/Express supports encrypted passwords. By default, all passwords used in the PrinterOn software are encrypted.

However, by default, Apache Tomcat is not designed to use encryption. As a result, if you are need to access remote services that require encrypted password, there may be some additional manual steps you'll need to complete to ensure that you are implementing the highest level of security available. This section guides you through the upgrade process and outlines any manual steps.

To ensure that your PrinterOn software uses these security features, perform the following tasks:

1. Run **PSIM.exe** to launch the PrinterOn Installation Wizard and upgrade your PrinterOn installation to the latest version.

2. By default, PSIM should have encrypted all passwords using the encryptor.jar. Verify that your passwords have been properly encrypted.

   If they are not encrypted by default, you can encrypt your passwords manually.

3. Configure Apache Tomcat to use encrypted passwords.

4. Restart the machine. All services will be restarted and will use the updated SSL/TLS protocols and encrypted passwords.

C.3.1 Verifying that your passwords are encrypted

To make sure that your passwords have been properly encrypted:

1. In a text editor, open C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\Conf\server.xml.

2. Locate the following entry:

```
<Connector port="443"
    protocol="com.printeron.tomcat.http11.Http11NioProtocol"
    SSLEnabled="true" maxThreads="150" scheme="https" secure="true"
    clientAuth="false"
    sslEnabledProtocols="TLSv1.1,TLSv1.2"
    keystoreFile="${pon.data.root}\KeyStore\keystore"
    keystorePass="rz6KZSpMD7fy7Co6UfIBmw%3D%3D"
/>
```

3. If the value for keystorePass is encrypted, the upgrade successfully encrypted your passwords.

   If the password is not encrypted, your you are adding your own keystore certificate, you can encrypt your password manually using the Encryptor tool and paste the encrypted password into the system.xml file. For more information, see Encrypting passwords manually.

4. Save the file, but keep this document open. You'll need to modify this entry later.

C.3.1.1 Encrypting passwords manually

If your passwords are not encrypted in the server.xml file, or you are adding your own keystore certificate and need to update the password in the system.xml file, you can encrypt passwords manually using the Encryptor tool included with the PrinterOn installation.

To run the Encryptor tool:

1. On the command line, enter the following command:

```
cd "C:\Program Files (x86)\PrinterOn Corporation\PrinterOn Server
Install Manager\Tools\Encrpytor" "%PON_JAVA_HOME%\bin\java.exe" -jar
encryptor.jar PASSWORD
```

   where PASSWORD is the plain-text password you need to encrypt.

2. Copy the encrypted password provided by the Encryptor and paste into any PrinterOn properties file.

C.3.2 Configuring Apache Tomcat to use encrypted passwords

By default, Apache Tomcat is not designed to use encrypted passwords. You'll need to update Apache Tomcat to use the encrypted passwords when PrinterOn attempts to access remote services, such as an LDAP server.

To configure Tomcat:

1. On the command line, run C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\bin\tomcat8w.exe. The Tomcat Properties dialog appears.
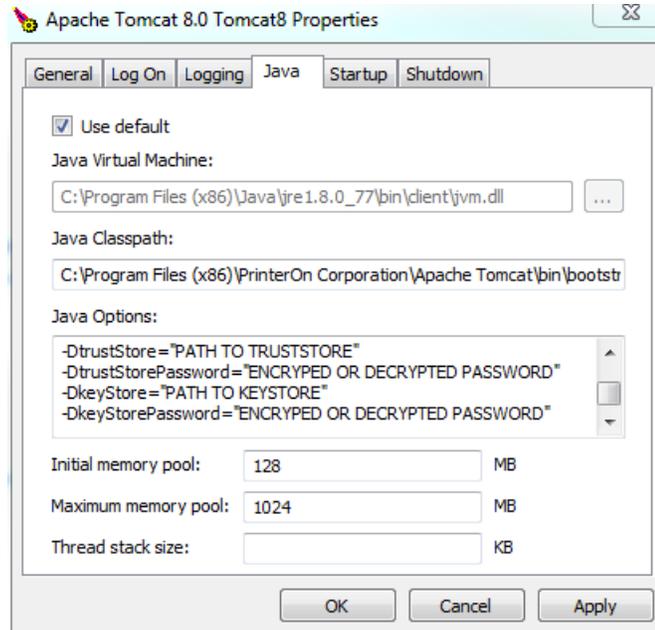
2. Open the **Java** tab.

3. In the **Java Options**, enter the following entries, if applicable:

   ```
   -DtrustStore="PATH_TO_TRUSTSTORE"
   -DtrustStorePassword="ENCRYPTED_OR_DECRYPTED_PASSWORD"
   -DkeyStore="PATH_TO_KEYSTORE"
   -DkeyStorePassword="ENCRYPTED_OR_DECRYPTED_PASSWORD"
   ```

4. To disable DNS caching, in the **Java Options**, enter the following:

   ```
   -Dsun.net.inetaddr.ttl=0
   ```

5. Click **OK**.

6. Restart the machine. All services will be restarted and will use the encrypted passwords.

D

Enabling and using the new PrinterOn Web Print UI

With PrinterOn Enterprise 4.3.5, administrators can choose to display a new Web Print UI for their users. This user interface offers an improved end-user experience, with fewer steps in the printing workflow, allows users to submit multiple documents at once, and displays a jobs list so users can monitor the print status of each submitted job.

Because this new UI is more resource intensive than the old UI, and because the features offered will likely not be required by most organizations, the new UI is disabled by default. You must enable the new UI for users to access it. Once enabled, the new UI will replace the old UI when users launch the Web Print portal.

Enabling the new Web Print UI

By default, the new Web Print UI is disabled and will not appear to the user when they navigate to the Web Print portal URL. With PrinterOn Enterprise 4.3.5, a new setting has been added to the Web Print workflow configuration in Configuration Manager allowing you to enable the new UI.

To enable the new Web Print UI:
1. Launch and log into the PrinterOn Configuration Manager.
2. In the Configuration Manager, click **Workflows** > **Web Print**.

3. Turn on **Enable New Web Print UI**.
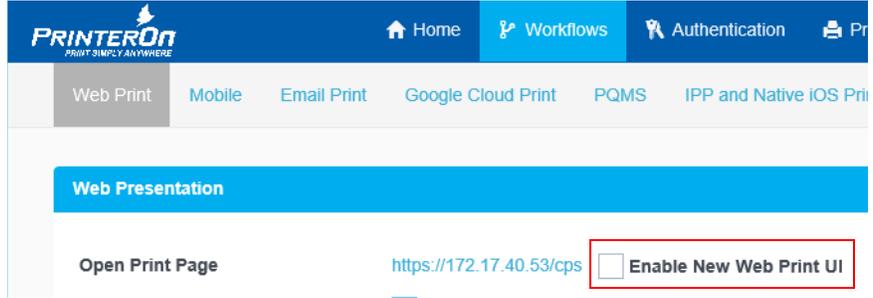
Using the new Web Print UI

To print with the new Web Print UI:

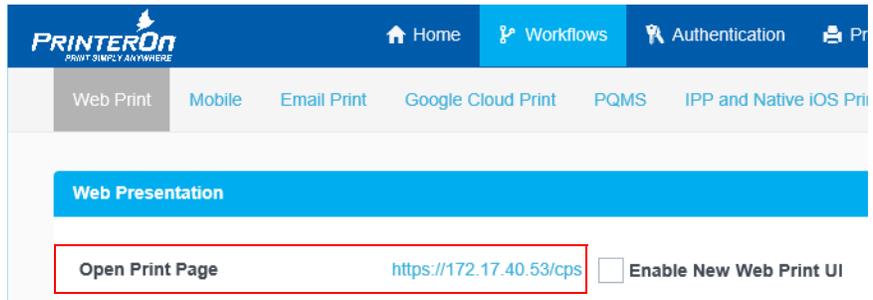1. Launch the Web Print portal using one of the following methods:

   • In the Configuration Manager, click **Workflows** > **Web Print**, then click the link next to **Open Print Page**.

   or

   • Choose **Start** > **All Programs** > **PrinterOn** > **Print Now**.

2. On the Web Print Home Page, click **Print**.
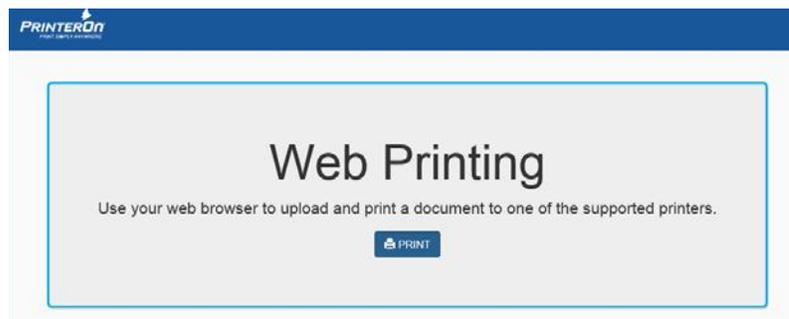
3. Select **Auto-generated Printer 1**.

4. Next. Select your document(s) and print options:
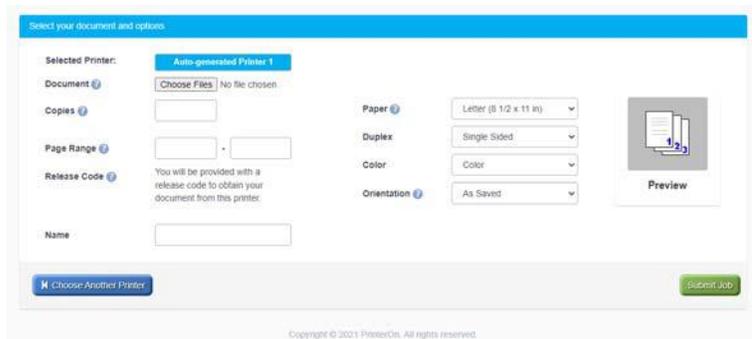
a) Click **Choose Files** to choose one or more documents to print. You can choose to print up to five documents or web pages. For this test, enter a URL to print in the **Web Page** field.
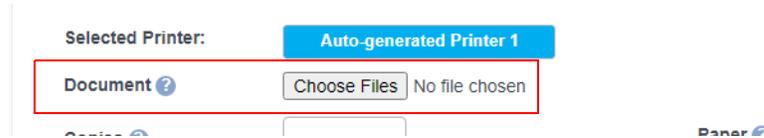
b) If necessary, enter the number of copies and a page range to print.

c) Choose your paper and print options:

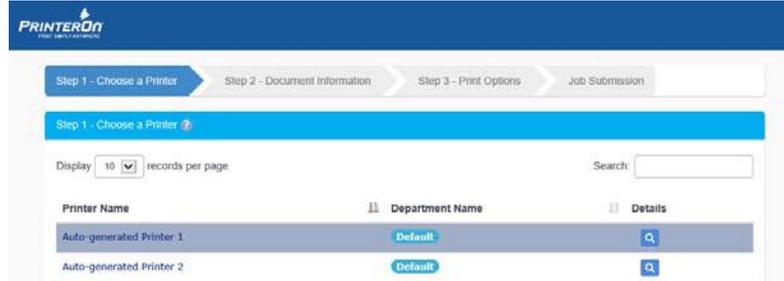5. Click **Submit Job**. PrinterOn begins to process your print job(s). A Jobs list appears below the print options allowing you to monitor the progress of your job and to verify that your job was correctly sent to the selected printer.
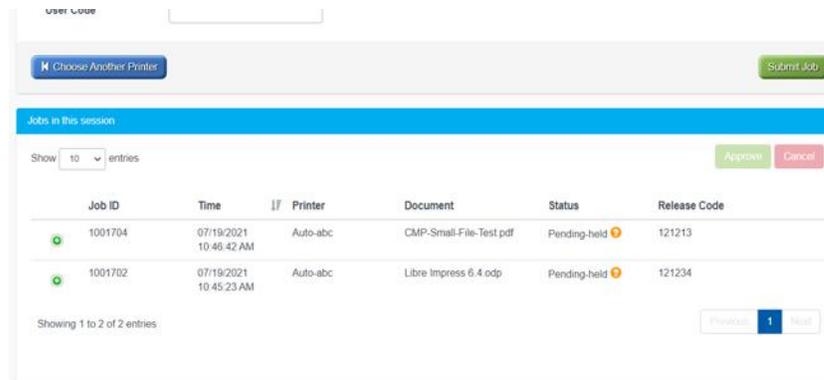
This list will display all the jobs submitted in the session, as well as the status and release code for each. You can approve or cancel any pending job by selecting the job and click **Approve** or **Cancel**.

•

E

Using the PDG for iOS/macOS devices without Bonjour

iOS and macOS devices use the Bonjour protocol for printer discovery. However, in many cases, the Bonjour protocol is not robust enough to overcome certain deployment scenarios. The limitations of Bonjour, and as a result native print for iOS, can make it either difficult or impossible to maintain a functional printing infrastructure.

You can use the Print Delivery Gateway to provide the same benefits of the native iOS print workflow without the need for Bonjour. To accomplish this, PDG uses other tools to inform iOS devices how and where to find printers on a network.

E.1 Minimum requirements for native iOS/macOS Print without Bonjour

To support printing from an iOS or macOS device though PrinterOn without using Bonjour, you need to create a printer profile to define printer configuration information, and then push that profile to those devices.

You'll need to meet the following requirements:

Consideration	Requirement
PDG port configuration	PDG must be configured to listen for IPP requests on the default IPP port 631. The Apple Configurator only works if PDG is configured use this port.
Device OS	iOS devices must be running iOS 7 or later.
Printer Profile distribution tool	To push the Printer Profile to devices, you'll need one of the following tools: • Apple Configurator • MDM/MAM-provided Print Profile configurator (for example, AirWatch, MobileIrone, etc) **Note:** Refer to your MDM/MAM documentation for more information regarding your specific solution.

E.2 Sample configuration

The following section describes a sample configuration process using the Apple Configurator and a standard Print Delivery Gateway configuration.

Note: The Apple Configurator is useful for validating a configuration and preparing information, but is not recommended for larger scale deployments. PrinterOn recommends using tools provided by an MDM/MAM provider.

To provide iOS printing without Bonjour:

1. Retrieve the PDG Server's IP address or DNS name. This address should be accessible from the iOS devices that will be printing. By default, the PDS reports this information on the Service Settings tab for the selected Broadcast Interface as well as on the IPP tab

2. Configure the PDG IPP Listening Port to use 631. You can configure this in the **Network and Broadcast Settings** panel of the **Networking** tab.

3. Retrieve the desired print queue identifier (that is, the PrinterOn Printer ID or printer name). This is often referred to as the **Resource Path (rp)**.

   You can access the printer name from the **Printers** tab.

4. Configure a Printer Profile using the Apple Configuration:

    a) Locate the **AirPrint Profile Configuration Settings**.

    b) Enter the PDG IP address in the **IP address field**.

    c) Enter the PrinterOn Printer ID in the **Resource Path** (ex: /300122322323).

> **Note:**
>
> • When entering the Resource Path, ensure there is a slash in front of the ID.
>
> • At the time of documenting this, a bug was identified in the Apple Configurator, the cursor MUST be in the IP Address field, or the information will not be saved.
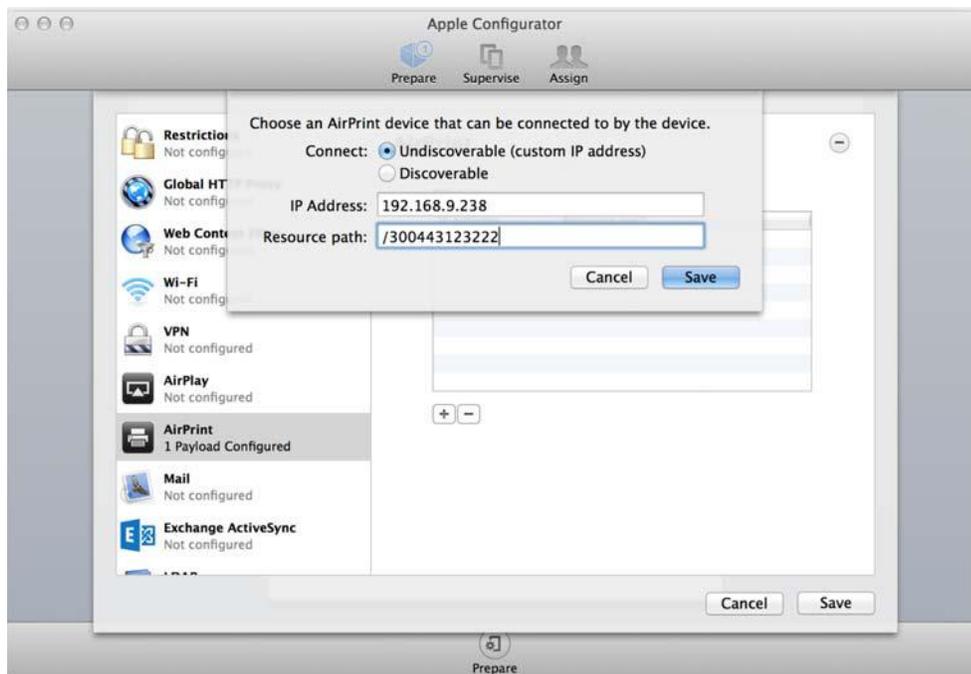
5. Save the settings and Push the Printer Profile to the iOS device to validate the configuration.

You can follow a similar configuration process when configuring devices using an MDM/ MAM solution.

F

PrinterOn Server components glossary and overview

F.1 Central Print Services

Central Print Services (CPS) is the primary entry point for all requests submitted to the PrinterOn Enterprise Server. CPS is responsible for providing a centralized interface for all Enterprise printing including end-user web printing, mobile application printing as well as for 3rd parties who develop integrations to the Enterprise Server for custom print services. CPS is a Java Servlet based solution that is hosted by Apache Tomcat as its Servlet Container. CPS implements PrinterOn Document and Directory Search APIs to facilitate submission of print jobs.

In addition to providing print service access, CPS also provides a web-based administrative console allowing administrators to manage their service and control how jobs are received and submitted to the underlying print subsystem.

F.2 PrintAnywhere

The PrintAnywhere Server provides job management and print processing of documents as part of PrinterOn's print services. The PrintAnywhere Server comprises a number of software services that facilitate the receiving and printing of documents and the delivery of the processed documents to a PrinterOn enabled printer.

For information on creating a PrintAnywhere cluster, see Advanced clustering and document processing scalability.

F.2.1 Web Plugins

PrintAnywhere's web plugins are the interfaces by which PrinterOn's Central Print Services (CPS) solution delivers print jobs to the PrintAnywhere server for processing. These plugins are required when installing PrinterOn's CPS solution. These plugins are available as part of the installation, as either a Java Servlet or ISAPI based interface.

F.2.2 PrintAnywhere Status Server

The PrintAnywhere Status Server is responsible for managing all incoming and in-process print requests. All print jobs received via email, the web or from mobile apps are first received by the Status Server. The Status Server is responsible for delivering requests to available Processing Servers and managing the jobs while they are being processed.

You can cluster multiple Status Servers to provide greater redundancy in a multi-server environment. For more information, see Adding Status Servers.

F.2.3 PrintAnywhere Processing Server

The PrintAnywhere Processing Server is responsible for converting a document received by the server into a printer-usable format. The Processing Server integrates with applications installed on the server and the PrinterOn PrintWhere Driver to render documents.

You can deploy multiple Processing Servers as part of a PrintAnywhere cluster to increase capacity and redundancy. For more information, see Adding Processing Servers.

F.3 PrinterOn PrintWhere Driver Server Edition

The PrinterOn PrintWhere driver is installed as part of the Processing Server. It is a key component of the overall printing process and is integrated into the Processing Server as part of a PrintAnywhere deployment.

The PrintWhere Driver is managed by the Processing Server using an internal API system. The Processing Server encapsulates communication between PrintAnywhere and the PrintWhere driver using a subcomponent of PrintAnywhere named the PrintWhere Bridge (PWCBridge.exe).

F.4 Print Delivery Gateway

The Print Delivery Gateway Software (PDG) serves as a protocol gateway to PrinterOn Enterprise printers, allowing users to submit jobs using a number of different methods, including:

- IPP and Native iOS (iPhone, iPad, other iOS devices), powered by **PDG iOS Connector**
- Google Cloud Print (Smartphones, Tablets, NetBooks, Chrome Browser, etc...), powered by **PDG GCP Connector**
- Standard Windows Printer Queues (Print Servers Integration), powered by **PDG PQMS Connector**

The PDG acts as a bridge that supports multiple print workflows, allowing IT Administrators to streamline the deployment, management, and administration of Enterprise printers, while simultaneously retaining the native printing experience unique to each platform.

F.5 Print Delivery Station

The role of the Print Delivery Station (PDS) is to provide a bridge between the PrinterOn delivery infrastructure and the physical printer or print queue. PDS communication is based on the IPP specification and provides extensions to the protocol for advanced functionality, such as encryption.

The simplest description of PDS is an IPP print server that supports various connection protocols to printers or print queues.

- IPP is based on HTTP and uses custom HTTP headers for metadata delivery and a structured binary body to deliver print data.
- PDS implements an IPP listener to receive print jobs from PrintWhere.
- Print jobs received by PDS can be delivered to their destination automatically or manually, based on the PrinterOn configuration.

- The process of receiving jobs and delivering them to their destination remains the same regardless of whether PDS is configured to hold for user input prior to delivering to their destination.

For more information on adding configuring PDS settings, see Managing and configuring Print Delivery Stations (PDS).

F.6 Print Delivery Hub

For Enterprise deployments delivering print jobs to printers installed in disparate networks, it may not be possible to deliver print jobs from a PrinterOn Enterprise Server or the PrinterOn PrintWhere universal driver directly to the PDS. In other cases, leveraging a simple and rapid deployment of print devices, such as Ricoh HotSpot printers, will benefit from the centralized installation of a Print Delivery Hub (PDH). In this arrangement, print jobs are delivered to the PDH setup and the PDS servers communicate with PDH to detect and download the print jobs.

In such a scenario, the PDH service must be accessible over the network to the PDS servers. The PDH service can be installed in a central network operating center. Access to the PDH will be configured such that the PrintAnywhere Server, desktop PrintWhere clients and PDS deployments can access the PDH server. This configuration generally minimizes network changes, as the PDH is the only service requiring incoming network traffic access.

For information about adding and configuring a PDH, see Adding a Print Delivery Hub.

G

Creating a printer configuration profile

A configuration profile is a CSV text file that defines the configuration properties for multiple printers. Configuration profiles simplify the printer creation and configuration process when you have a large number of printers.

A printer configuration profile defines a number of settings, including:

- Printer Name
- Printer Description/Location Settings
- Print Workflows Options
- Print Driver Settings
- Printer Capabilities

To further simplify the process, you can use printer configuration profiles in conjunction with printer templates. For certain properties, if values are left blank, the server applies the value found in the specified template.

Once you have created a CSV file, you can import that file into the Configuration Manager to create or update printers. For more information on importing a CSV file, see Importing a printer configuration profile into the Configuration Manager.

G.1 Optimizing performance

Importing a printer configuration profile is resource intensive. For optimal performance, before you attempt to use a configuration profile to create or update multiple printers, you should consider the following system requirements:

- You should have at least 4 GB of RAM available on your server.
- Set your log level to a value of **Warning** or lower. Higher logging levels can result in too many messages and can slow performance.
- Disable the printer synchronization settings for both PDG and PDS. Printer synchronization drastically increases the time it takes to import and apply the settings. You should disable both the **Synchronize By Default** and **Automatic Printer Synchronization** settings.
- Increase the memory allocation for Apache Tomcat. Tomcat should have an **Initial memory pool** value of 256 MB, and a **Maximum memory pool** value of 1024 MB.
- Adhere to the following limitations:
  - Creating printers: Maximum 5000 printers per operation
  - Updating printers: Maximum 300 printers per operation

G.1.1 Changing the memory pool for Tomcat

To maximize the performance of a bulk printer creation or update operation, you can increase the memory pool allocated to Apache Tomcat.

To change the memory pool for Tomcat:

1. Navigate to C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\bin\ and open tomcat8w.exe. The Central Print Services Properties dialog appears.
2. Click the **Java** tab.
3. In the **Maximum memory pool** field, set a value of 1024 MB.
4. Click **OK**.

G.2 Structure of a printer configuration profile

The basic rules to keep in mind while entering values into the printer configuration profile are as follows:

- A CSV file provides fields/columns separated by commas. You can use any spreadsheet program, such as Microsoft Excel, to create the file, then save it as a CSV file when you are ready to import it.

    Note: To ensure that the Configuration Manager can successfully import and read the content of your CSV file, you should make sure that the file is encoded as UTF-8.

- Fields with embedded commas are enclosed by double-quotes. For example, consider the following entry: 1223,"This is a, comma", abcd. In this entry, "This is a, comma" is a single field.
- Fields with line breaks must also be enclosed by double-quotes.

G.2.1 CSV Headers

The first row of the printer configuration profile is reserved for specifying CSV field header information. This header row describes how each entry is structured so that the PrinterOn Server can successfully apply the settings for each printer.

The header row lets you define which configuration values you're setting for imported printers, and in what order they are specified for each entry. You can list the headers in any order, but you must make sure that values entered for each imported printer are provided in the same order.

G.2.2 CSV Data Types

Configuration data can be one of the following types:

Data Type	Description
Required (R)	Required data MUST be supplied for each entry in the CSV file. If a required field is not supplied, the CVS entry will not be processed and an appropriate error will be provided in the final Portal Creation report.
Template Alternative (TA)	Data that may optionally be supplied in the CSV file. If a TA setting is not defined in the CSV file, the server configures the setting to the value from the template printer (specified by **templatePrinterId**). If a value supplied for a Template Alternative setting is invalid or uses an incorrect syntax, the import fails. The server does not replace invalid values with the template value.

G.3 Printer configuration profile settings

The section below lists each header with a description and its supported values. Each entry is a distinct comma-separated data point.

Header	Description and link to UI setting	Supported values	Type
action	Indicates whether a new printer is created, an existing printer is modified, or an existing printer is deleted.	• 0: Updates a printer • 1: Creates a printer • 3: Deletes a printer	R
createPds	Indicates whether to create a new PDS or to associate the printer with an existing PDS.	• 0: Associates with an existing PDS	
templatePrinterId	The PrinterOn ID of the Template Printer. If the createPrinter value is 0, this field represents the ID of the printer to update.	A valid PrinterOn Printer ID	R
printerName	The name of the printer. ⬈ If the createPrinter value is 0, this field is used to update the printer name.	Any valid Printer name	R
printerDescription	A descriptive label/Location Information ⬈	Front Office Later	R
departmentName	Printer Department Name ⬈ Note: The value will be use to specify the printer department for Enterprise printers. Should generally be left empty for Express printers.	An existing printer department	TA
streetAddress	The street address of the printer location. ⬈	Any street address	TA
streetAddress2	The street address of the printer location. ⬈	Any street address	TA

Header	Description and link to UI setting		Supported values	Type
city	The city the printer is located in.	⬈	Any city name	TA
state	The state/province (PrinterOn ID) the printer is located in.	⬈	See State/Province codes.	TA
country	The country (PrinterOn ID) the printer is located in.	⬈	See Country Codes.	TA
postalCode	The postal code of the printer location.	⬈	A valid postal code	TA
gpsLatitude	The GPS latitude value.	⬈	Any valid GPS value	TA
gpsLongitude	The GPS longitude value.	⬈	Any valid GPS value	TA
externalId	The external ID for this printer, typically the MAC address of the printer.	⬈	A valid MAC address	TA
printerModel	The printer driver information that is shown to the user when viewing printer details.	⬈	A printer driver	TA
printerModelName	The printer model name, used to optimize output for Samsung printer models.	⬈	Any valid printer model name	TA
printWhereEnable	Indicates whether the printer supports the PQMS workflow.	⬈	• 0: Disabled • 1: Enabled	TA
docApiEnable	Indicates whether the printer supports mobile, GCP, and IPP/iOS Native Print workflows.	⬈	• 0: Disabled • 1: Enabled	TA
emailDomain	The email domain of the printer.	⬈	• 0: Disabled • 1: Enabled	TA
emailPrintingEnable	Indicates whether the printer supports the Email Print workflow.	⬈	• 0: Disabled • 1: Enabled	TA
printEmailBody	Indicates whether the body of an email is printed when receiving email print jobs. If disabled, only attachments are printed.	⬈	• 0: Disabled • 1: Enabled	TA
enableAdvanceIntegration	Enable advance integration features	⬈	• 0: Disabled • 1: Enabled	TA
printManagementService	Print Management Service	⬈	See Print Management Service IDs.	TA
additionalIntegrationInfo	Additional Integration information. Valid only when printManagementService is set to 27 (Equitrac) or 55 (SecuPrint).	⬈	See Additional Integration Info IDs.	TA
injectPjlHeader	Indicates whether the server injects a PJL Header container, if none exists.	⬈	• 0: Disabled • 1: Enabled	TA
injectPjlForPassthrough	Indicates whether the printer processes and modify PJL headers.	⬈	• 0: Disabled • 1: Enabled	TA
pdsOutputType	The URL scheme for the output destination, such as local://, tcp://, or https://.	⬈	A valid URL scheme	

Header	Description and link to UI setting	Supported values	Type
pdsAddress	The network address for the printer's output destination. ⧉ **Note:** If you import printers using a CSV file but want to set the printer's output destination in the PDS, you must to enable the **Override Settings** check box when configuring the PDS software. For more information, see Configuring the Print Delivery Station software.	A valid URL or IP address	
useDocumentConversion	Indicates whether the printer supports converting the document into an electronic presentation format such as XPS, rather than render it for printing. ⧉	• 0: Disabled • 1: Enabled	TA
printEmbeddedDocuments	Indicates whether the printer extracts and prints any documents that are embedded in the original document. ⧉	• 0: Disabled • 1: Enabled	TA
lateBindingsEnabled	Indicates whether the user can change finishing options for the print job at the printer before printing the document. ⧉	• 0: isabled • 1: Enabled	TA
insertCopiesMode	Indicates whether the printer injects PJL-based copies. ⧉	• 0: Application based • 1: PJL based • 2: Driver based	TA
nupSupported	Indicates whether the printer supports multi-page layouts, in which multiple pages are printed on a single sheet of paper. ⧉	• 0: Samsung PCL • 1: Samsung SPL • 3: None	TA
pjlEncoding	The Printer Job Language encoding. ⧉	• 0: Not managed • 1: UTF-8	TA
overrideEncoding	Indicates whether the printer supports double byte characters ⧉	• 0: Disabled • 1: Enabled	TA
ippPrinter	Indicates whether the printer is an IPP printer. ⧉	• 0: Not an IPP printer • 1: An IPP printer	TA
serialNumber	The serial number of the PDS with which the printer is associated. For example: ⧉ X4531-TY76-UU78	A valid serial number of an existing PDS	TA
ippLan	The fully qualified network address of the Print Delivery Station server. ⧉	A valid IP address	TA
ippLanOnly	Indicates whether print jobs are printed directly to the PDS only. ⧉	• 0: PDS or PDH • 1: PDS only	TA
ippUrl	The fully qualified network address of the Print Delivery Hub server. ⧉	A valid IP address	TA

G.3.1 Sample printer configuration profile

The following sample illustrates the contents of a configuration profile defined in a spreadsheet, which can later be saved as CSV and imported into the Configuration Manager. For more information, see Importing a printer configuration profile into the Configuration Manager.

Note that undefined values for Template Alternative settings can be left blank or omitted altogether. The PrinterOn Server handles empty entries as described in CSV Data Types.

createPds	createPrinter	templatePrinterId	printerName	printerDescription	printWhereEnable	docApiEnable	emailPrintingEnable
0	1	900005211111	bulk-imported-printer-0001	Bulk Printer 0001	1	1	1
0	1	900005211111	bulk-imported-printer-0002	Bulk Printer 0002	1	1	1
0	1	900005211111	bulk-imported-printer-0003	Bulk Printer 0003	1	1	1
0	1	900005211111	bulk-imported-printer-0004	Bulk Printer 0004	1	1	1
0	1	900005211111	bulk-imported-printer-0005	Bulk Printer 0005	1	1	1
0	1	900005228231	bulk-imported-printer-0006	Bulk Printer 0006	1	1	1
0	1	900005228231	bulk-imported-printer-0007	Bulk Printer 0007	1	1	1
0	1	900005228231	bulk-imported-printer-0008	Bulk Printer 0008	1	1	1
0	1	900005228231	bulk-imported-printer-0009	Bulk Printer 0009	1	1	1
0	1	900005228231	bulk-imported-printer-0010	Bulk Printer 0010	1	1	1

G.3.2 CSV ID reference

G.3.2.1 Country Codes

PrinterOn uses the ISO standard two-letter abbreviations to represent specific countries. When supplied, PrinterOn will associate the newly created printer with the supplied country ID.

Note: These values are Template Alternative values and are not required.

Country	Code	Country	Code	Country	Code
Argentina	AR	France	FR	Mexico	MX
Australia	AU	Germany	DE	Pakistan	PK
Brazil	BR	Great Britain	GB	Spain	SP
Canada	CA	Indonesia	ID	Thailand	TH
China	CN	Italy	IT	United States	US
…		…		…	

For a complete list of country codes, you can search the ISO database here.

G.3.2.2 State/Province codes

PrinterOn uses the ISO standard codes for state/provinces to represent specific regions. When supplied, PrinterOn will associate the newly created printer with the supplied region code.

> **Note:**
>
> - These values are Template Alternative values and are not required.
>
> - Not all states and provinces are represented within the State/Province Identifier field. PrinterOn Only supports specifying state/province for the US, Canada, China, and Australia. In other regions, the state/province code should match the country code. For example, Germany would be set as country=DE, state/province=DE.

The following is a small subset of state/province identifiers for reference.

US State	Code	CA Province	Code	CN Province	Code	AU State	Code
Alabama	AL	Alberta	AB	Beijing	11	New South Wales	NSW
California	CA	Manitoba	MB	Fujian	35	Northern Territory	NT
Illinois	IL	New Brunswick	NB	Guangxi	45	Queensland	QLD
Maine	ME	Ontario	ON	Hong Kong	91	South Australia	SA
Massachusetts	MA	Quebec	QC	Shandong	37	Tasmania	TAS
Michigan	MI	Saskatchewan	SK	Shanghai	31	Victoria	VIC
New York	NY	Yukon Territory	YT	Yunnan	53	Western Australia	WA
...		...		...		...	

For a complete list of state/province codes, you can search the ISO database here, then select the country to view the subdivision codes.

G.3.2.3 Print Management Service IDs

These IDs are used to configure the type of third-party integration service to apply to the printer. Leave blank if none is required, otherwise, specify the numeric ID.

Third-Party Integration	ID
None	
Samsung BCPS	5
SecuPrint	35
Samsung Secure Release	36
Litech	37
Samsung Secure Release Code	38
Samsung SecuThru Pro	40

G.3.2.4 Additional Integration Info IDs

Some print management systems can be used with additional integrations. The following table lists supported secondary integrations and the primary integration(s) (specified using the **printManagmentService** value) with which they can be used.

Secondary Third-Party Integration	ID	Valid Primary Third-Party Integration
SecuPrint	35	Samsung Secure Release Code (38)
Samsung Secure Release	36	SecuPrint (35) Samsung Secure Release Code (38)
Litech	37	Samsung Secure Release Code (38)
Samsung SecuThru Pro	40	SecuPrint (35) Samsung Secure Release Code (38)

H

Importing users into the PrinterOn user store

If you are adding a number of users to the PrinterOn user store at the same time, adding them individually through the Configuration Manager interface is not very efficient. To facilitate multiple user entries, you can create a user list as a CSV file, then use a SQL script provided by PrinterOn to import those users.

To import multiple users into your PrinterOn user store, you'll need to complete the following tasks:

- Create a User List CSV file with the required values for each user.
- Run the SQL script provided by PrinterOn to import the contents of the file into your IMCAS database.

H.1 Creating the User List CSV file

The User List CSV file defines the basic values required to add a new user entry in PrinterOn's IMCAS database. You can create the file in any text editor, or you can create a spreadsheet and export it as a CSV file.

> **Note:** Password are not set using the User List CSV file. Instead the SQL script simply assigns a password of "password" to every new user added to the table; users can set their own passwords upon logging in for the first time.

To create a User List CSV file:

1. In a text editor or spreadsheet editor, create a new text file or spreadsheet.

2. Add an entry for each user. Each line in the file must contain the following five values, each separated by a comma:

Value	Description
Row	The entry order for the user. The first entry in the CSV file must always have a value of 1, and subsequent lines must increase sequentially.
User ID	The name with which the user signs into PrinterOn service.
First Name,	The first name of the user.
Last Name	The last name of the user.
Email	The email address associated with this user.

For example:

```
1,mberenyi,Miki,Berenyi,mberenyi@mycompany.com
2,jcole,Jeremy,Cole,jcole@mycompany.com
3,sbraithw,Stuart,Braithwaite,sbraithw@mycompany.com
4,engyuen,Eddie,Nguyen,engyuen@mycompany.com
5,nnahrin,Nowshi,Nahrin,nnahrin@mycompany.com,
6,jlannerh,Julia,Lannerheim,jlannerh@mycompany.com
```

3. When you have added all the entries, save the file. By default, the SQL script provided by PrinterOn requires the file to be called csv.txt, and that it be located in the root C:\ folder.

Once you have created a User List CSV file, you can import that file into the IMCAS database. For more information, see Running the SQL script.

H.2 Running the SQL script

PrinterOn provides a SQL script that you can use to import your User List CSV file into your IMCAS database.

Note: The PrinterOn script relies on a default filename and location for the User List CSV file (C:\csv.txt), and creates or modifies a default table in the database (CSV2.txt).

If you want to change these default values in the script, you can modify the script as necessary. However, modifying the SQL script is outside the scope of this document.

The PrinterOn script performs the following tasks:

1. Creates a table in the IMCAS database named CSV2.txt.
2. Opens the csv.txt file located in the C:\ folder.
3. Populates the CSV2.txt table with contents of the csv.txt file.
4. Sets a default user password of "password" for all users.

To execute the SQL script:

1. Download and extract the SQLQuery2.sql script from the following location:

   dl.printeron.com/imcas/SQLScript.zip

2. Launch SQL Server Management Studio.
3. In SQL Server Management Studio, click **File** > **Open**, then browse to the location of the SQLQuery2.sql script file and select it.
4. Click **Execute**.
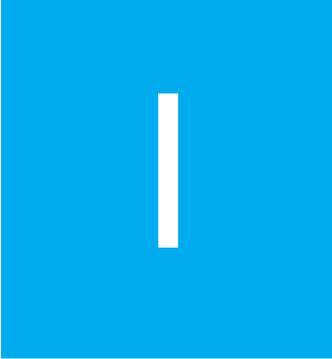
Troubleshooting proxy issues

On the **Home** > **General** tab of the Configuration Manager, you can define settings to allow your service to communicate through a proxy server. The settings you define here are only used by the CPS. In most deployments, this is sufficient, since all communication with the PrinterOn Directory flows through the CPS.

However, there are two scenarios in which simply setting the CPS proxy settings is insufficient:

- **If you have implemented a Hybrid Direct deployment, in which each component communicates directly with the PrinterOn Directory.** In this case, you'll need to configure the proxy settings for PAS and PDS individually.

  For more information on configuring proxy settings for a component, see Configuring the proxy settings for an individual component.

- **If you have a proxy configured in the Internet Explorer/Windows settings.** In this case, the Windows proxy functionality causes a known issue to arise that prevents PrintAnywhere from communicating with other local components.

  To work around this issue, you'll need to configure the proxy settings for PrintAnywhere, and then whitelist the local addresses required by CPS.

  - For more information on configuring proxy settings for PrintAnywhere, see Configuring the proxy settings for an individual component.

  - For more information on whitelisting certain addresses, see Configuring proxy exceptions.

I.1 Configuring the proxy settings for an individual component

To configure the proxy settings for an individual component:

1. In the Configuration Manager, click **Advanced** > **Components**, then click the **Configure** button adjacent to the component you want to set proxy settings for.

2. Click the **Proxy** tab, and configure the settings as necessary.

3. Click **Apply Settings**.

I.2 Configuring proxy exceptions

If you configure a proxy in the Internet Explorer/Windows settings, a known issue may arise where Windows does not correctly honor the **Bypass for Local Addresses** setting. This prevents PrinterOn components from communicating with other local components. This known issue primarily impacts the PrintAnywhere server.

To work around this issue, you can whitelist local IP addresses and hostnames to allow PrintAnywhere to correctly communicate with CPS.

To configure the proxy settings for an individual component:

1. In the Configuration Manager, click **Advanced** > **Components**, then locate PrintAnywhere Server and click the adjacent **Configure** button.

2. Click the **Proxy** tab, and configure the settings as necessary.

3. click **Advanced** > **Components**, then locate Central Print Services and click the adjacent **Configure** button.

4. Click the **Proxy** tab.

5. In the **Proxy Exceptions** field, enter the following IP addresses and hostnames:

   - 127.0.0.1
   - localhost
   - the internal IP address

   Note: If you have any remote components installed that PAS may need to communicate with (for example, PDS or PDH), enter their IP addresses in this field as well.

J

PrinterOn Server network port usage

The following table provides an overview of all ports used by the PrinterOn Servers. The ports listed below cover all sub components of the server.

> **Note:**
>
> - Some ports are used for interprocess communication on a local server. They are required but do not pose a security risk. A local firewall may be used to block the ports, as long as it does not interfere with local communication.
>
> - Some ports, such as the PrintAnywhere ports for Processing Server and Status Server communication, are used for both interprocess communication AND clustering.
>
>   - If clustering is not enabled, a local firewall may be used to block the ports, as long as they do not interfere with local communication.
>
>   - If clustering is enabled, access can be limited to end points in the cluster.
>
> - Some ports are configured as optional alternatives during installation, such as port 8080 in PDS. You can reconfigure and/or disable these ports if necessary.
>
> - Some ports above 10000 may be created temporarily for interprocess communications on the same server. These are expected and may change from instance to instance.

Port	Required?	Description	Owner	To disable:
80	No	Used for internal subcomponent communication for configuration, authentication, and Web Print.	CPS	Redirect to SSL Port in Tomcat or block by firewall.
443	Yes	Used for internal subcomponent communication for configuration, authentication, and Web Print.	CPS	N/A
631	Yes	Used to receive print jobs from PrintAnywhere and PrintWhere.	PDS	N/A

Port	Required?	Description	Owner	To disable:
4999	Yes	Deprecated as of version 3.2.3.	PDS	Deprecated.
5000	Yes	Deprecated as of version 3.2.4.	PDG	Deprecated.
5009	Yes	Used for Local Server Interprocess communication.	PAS (Processing)	Block by firewall.
5200	Yes	Used for communication between PrintAnywhere server components when clustering. Only required if clustered.	PAS (Status)	N/A
5400	Yes	Used for communication between PrintAnywhere server components when clustering. Only required if clustered.	PAS (Processing)	N/A
6310	No	Used for receiving IPP/AirPrint jobs from iOS devices and Apple Desktops.	PDG	Disable the Print Delivery Gateway.
8009	No	Used by the AJP Connector for load balancing Tomcat instances or integrating with Apache. Redirects to port 443.	Apache Tomcat	Remove the port in the server.xml file.
8057	Yes	Used to provide access to the Configuration Manager. Access to Web Configuration tools	Configuration Manager	Block by firewall.
8080	No	An alternate/optional port used for Receiving print jobs. This port is used for internal communication, except in a multi-server deployment, or when receiving print jobs from PrintWhere. This port is configurable.	PDS	Disable the port in the PDS admin page.
8081	No	An alternate/optional port used for Receiving IPP/AirPrint jobs from iOS devices and Apple Desktops. This port is configurable.	PDG	Disable the Print Delivery Gateway.
8181	No	Used by the Web Release User Interface. This port is only required if using the web release interface for job release.	PDS	Block by firewall.
8182	no	Used by the Brother BSI API Interface. This port is only required when using the Brother BSI API for job release.	PDS	Block by firewall.
9444	No	Used by the Storage Server. This port is only required to support Print Preview.	Storage Server	Block by firewall.
10051	Yes	Used for Local Server Interprocess communication.	PWC Bridge	Block by firewall.
48300, 49300, 50300	Yes	Used by internal PrintWhere processes.	Satellite, Post Render and Driver	Block by firewall.

K

Managing and scaling the PrinterOn database

The PrinterOn software includes Microsoft SQL Server Express 2014 as part of the installation. This database is freely distributable and meets the requirements of most PrinterOn deployments.

The database used by the PrinterOn server stores printer, user, and transaction/print job information. This information is used to create reports and provide printer configuration information used during the print process. The following table includes information about the data requires as well as guidelines for scalability.

K.1 Maintaining database integrity during upgrades

PrinterOn uses Flyway to manage the PrinterOn products' database versioning. This product creates a specialized table in the PrinterOn-dedicated database to manage modifications between versions and upgrades. This table is a critical piece of the PrinterOn product upgrade process and helps to ensure that the integrity of the database is maintained. PrinterOn creates a dedicated database instance in SQL Server to ensure that there is no impact with other databases deployed on the same instance.

As a result, it is important that the state of this Flyway table is not modified after it is created, either manually or through any other applications. If any third party application or process modifies this Flyway table, it will have negative impact and will likely break future upgrades of the product.

K.2 Database management and scaling

The PrinterOn software includes Microsoft SQL Server Express 2014 as part of the installation. This database is freely distributable and meets the requirements of most PrinterOn deployments.

K.2.1 PrinterOn database data types

The PrinterOn database stores the following information:

Data Type	Description	Storage Size
Printer	The PrinterOn database stores your PrinterOn printers and Secure Release Anywhere pools. Each printer is represented in the database and stored with its configuration information, such as name, location information, and capabilities. Printer data size is fixed and scaling requirements can be calculated by multiplying the number of printers by 1.5	1.5KB/printer
User Record	The PrinterOn database houses the PrinterOn user store, if used. If you configure your PrinterOn service to use the Internal Users, Azure AD, or Third-Party Identity Management Service authentication methods, the PrinterOn user store is created and used to store information about user accounts, user groups, and access control rules. User data size is fixed.	1KB/user
Print Job	Each print job processed by the server is stored in the database for reporting purposes. The transaction record information about the job, its size, the type of document and more. A job that is aborted or does not complete may require less data storage than a fully completed job depending on the point at which the job was ended.	2.2KB/Job

K.2.2 Guidelines for scalability

When determining the size of the data used by the server, the information about the number of printers, the number of users, and the estimated number of print jobs should be used.

Data Type	Deployment Size	Storage Requirements
Printer	100 Printers	150KB or 0.15MB
	1000 Printers	1500KB or 1.5MB
	5000 Printers	7500KB or 7.5MB
	10000 Printers	15000KB or 15MB
User record	100 users	100KB or 0.1MB
	1000 users	1000KB or 1MB
	5000 users	5000KB or 5MB
	10000 users	10000KB or 10MB

In the examples below, the number of printers will not be represented as the data usage is minimal.

Jobs/day	Jobs/year	Time Period	Data Requirements
1000 jobs/day	Approx 375,000	1 year	784 MB
		5 year	3,920 MB
2000 jobs/day	Approx 750,000	1 year	1,570 MB
		5 year	7,841 MB
5500 jobs/day	Approx 2,000,000	1 year	4,300 MB
		5 year	21,500 MB

K.2.3 Microsoft SQL Express capacity limitations

Data size is not the only factor to consider when deciding whether to upgrade from Microsoft SQL Server Express to the full Microsoft SQL Server. However, based on the data requirements above, the SQL Express version included with PrinterOn Enterprise and Express is capable of handling nearly **5 million job records**.

K.2.4 Increasing Tomcat memory to handle high Web Print volume

If you are expecting or experiencing a high volume of printing using the Web Print portal, increasing the memory allocated to the Tomcat Java VM may improve the application's overall performance and responsiveness.

By default, Tomcat is configured with a memory allocation of 256MB and a maximum of 512MB. The recommended values for heavy usage are 512MB and 1024MB.

> **Important!** Only modify the Tomcat memory allocation if your web printing portal is exhibiting slow response times under heavy usage.

To modify the Tomcat memory allocation:

1. On the command line, run C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\bin\tomcat8w.exe. The Tomcat Properties dialog appears.
2. Open the **Java** tab.
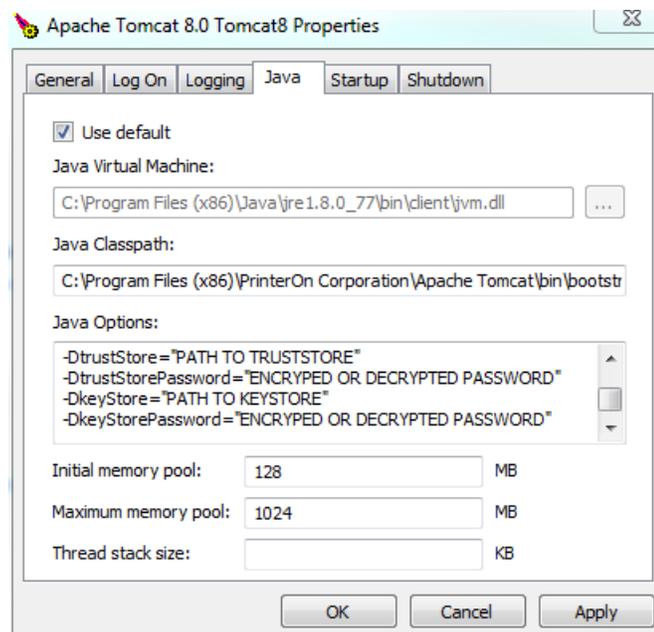
3. Change the **Initial memory pool** and **Maximum memory pool** to 512 and 1024, respectively.
4. Click **OK**.
5. Restart Tomcat to apply the changes.

K.3 Managing account permissions and database access

Microsoft's SQL Server supports two modes of authentication:

- **Windows Authentication**: Uses standard Windows Accounts to verify the identity of a user, both on the PrinterOn Server and the SQL Server.

- **SQL Server/Mixed Mode Authentication**: Supports a combination of Windows Accounts and additional accounts defined and managed directly in SQL Server itself.

By default, PrinterOn installs SQL Server with Windows Authentication enabled. All components are on the same system and therefore use the same account.

K.3.1 Setting up access for distributed components

By default, all PrinterOn components are installed on the same server. In this case, the Windows Account identified during the installation is used to run the SQL Server and also to control access by the PrinterOn Server to the database.

Below are some guidelines and best practices when determining how to setup access for distributed components.

- The same Windows Account should be used to run the SQL Server Windows Service and the PrinterOn Central Print Services Windows Service.

  These Windows services should use the same username and password for all instances, regardless of the authentication methods.

- If the SQL Server instance is joined to a Windows Domain, the PrinterOn Server running Central Print Services must also be joined to the same Domain.

  When any of the components are joined to a Windows Domain, the server will validate both the domain name and the user name, and the combination of both must match.

- If using Windows accounts is not desirable, you can enable Mixed Mode authentication. Mixed Mode authentication allows accounts to be created in SQL Server directly and independent of Windows accounts.

  > **Important!** Enabling Mixed Mode Authentication requires a change to the PrinterOn configuration. See Enabling SQL Server/Mixed Mode Authentication.

K.3.2 Enabling SQL Server/Mixed Mode Authentication

To use Mixed Mode authentication, the authentication method must be enabled in SQL Server and then the PrinterOn configuration updated to use it.

- Enabling mixed mode authentication for SQL Server
- Updating the Central Print Services configuration

K.3.2.1 Enabling mixed mode authentication for SQL Server

As long as you can connect to SQL Server with Windows authentication, you can enable mixed mode authentication easily using SQL Server Management Studio.

To enable Mixed Mode authentication:

6. Launch SQL Server with SQL Server Management Studio.

7. In **Object Explorer**, right-click the server that you want to reconfigure, then select **Properties**.
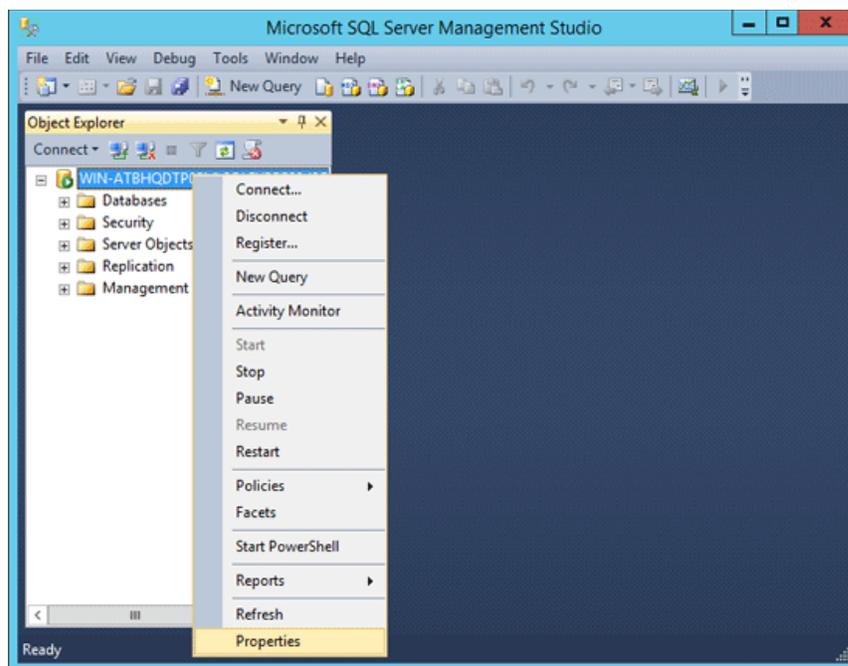
8. In the Server Properties dialog box that appears, from the left pane, select **Security**.
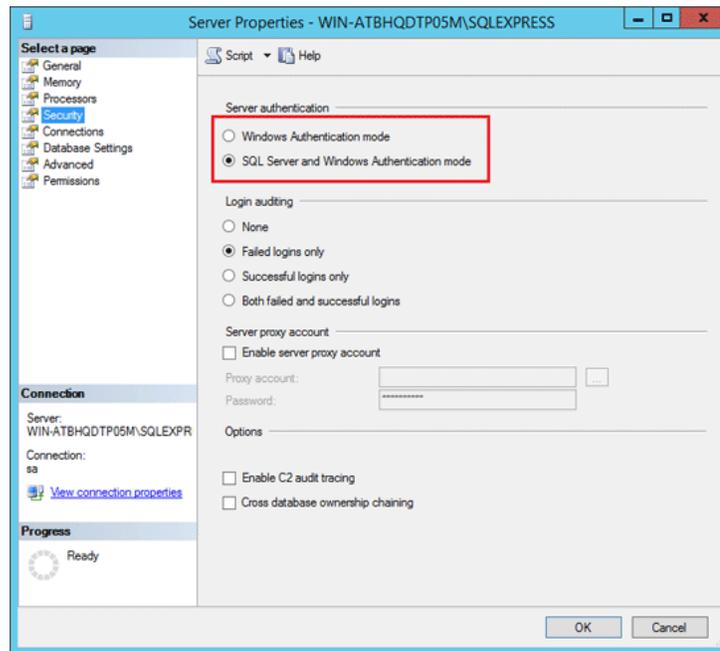
9. In the Server Authentication section in the right-panel, choose SQL **Server and Windows Authentication mode** (also known as Mixed Mode authentication).
10. Click **OK** to save the changes.
11. Restart the SQL Server service, then create the desired user account using Management Studio.

K.3.2.2 Updating the Central Print Services configuration

Once you have set the Authentication mode for SQL Server, you can update the authentication credentials used by the PrinterOn Central Print Services (CPS) when connecting to the SQL Server. To update the credentials, you need to manually modify the cps-db.properties file.

To update the CPS authentication credentials:
1. In the Configuration Manager, stop the Central Print Services.
2. In a text editor, open the following file:

    C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\lib\cps-db.properties

3. In the cps-db.properties file, locate the `jdbc.url` entry.

4. Modify the value of the integratedSecurity setting to false:

```
integratedSecurity=false
```

5. Modify the values of the `jdbc.user` and `jdbc.password` settings in the cps-db.properties file to reflect the username and password of the SQL Server account.

6. Save the file.

7. In the Configuration Manager, restart the CPS.

K.4 Using an alternative database

If you have an existing SQL Server that you would prefer to use instead of the default Microsoft SQL Server Express 2014 installed with the PrinterOn software, you can create new databases for PrinterOn and IMCAS data in your existing SQL Server and point the PrinterOn service to the new location. The PrinterOn service will begin using the new databases immediately.

> **Note:** The IMCAS database is only used if you are using third-party IDMs or the PrinterOn internal user store to manage user identities and authentication. If you are using some other authentication method, the IMCAS database is not used.

If you are using IMCAS, it is recommended that you install both the PrinterOn database and the IMCAS database on the same server.

In addition, as a best practice, it is recommended that you migrate the existing PrinterOn and IMCAS databases to their new locations. You can migrate each database by backing it up in Configuration Manager and restoring it to the new database.

> **Important!** If you are migrating the PrinterOn and IMCAS databases, you'll need to backup the existing databases *before* pointing the PrinterOn service to your new database locations.

To use your own SQL Server to host the PrinterOn database, you'll need to complete the following tasks *for each database*:

1. Create a new database.
2. Create a new login account for the database, if necessary.
3. Migrate the existing PrinterOn database to the new database.
4. Modify the PrinterOn service to point to the new database location.

K.4.1 Creating a new database in your existing SQL Server instance

You'll need to create a new database for each of the PrinterOn database and the IMCAS database, if used.

To create a new database:

1. Launch SQL Server Management Studio.
2. In SQL Server Management Studio, right-click **Databases**, then select **New Database**. The New Database dialog appears.
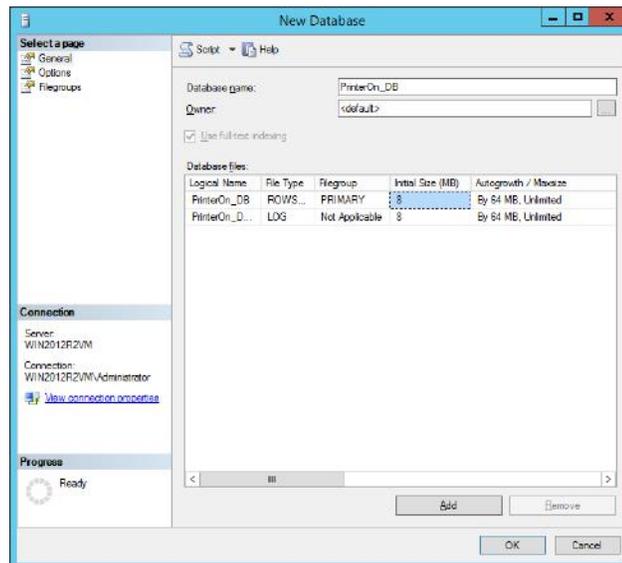
3. In the **Database Name** field, provide a unique name for the database.

4. Click the **...** button adjacent to the **Owner** field to associate one or more login accounts with the database. The Select Database Owner dialog appears.

> **Note:** If necessary, you can create additional login accounts and associate them with the database later. For more information, see Creating a new database login account.
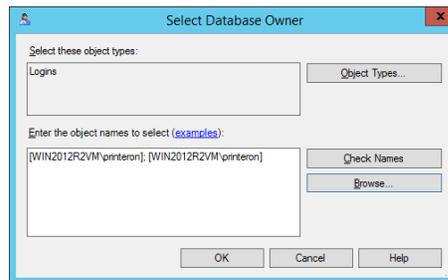
5. Click **Browse**. The Select Objects dialog appears.
6. Check each defined login account that you want to set as the owner of the new database, then click **OK**.
7. Click **OK** to return to the New Database dialog.
8. Click **OK** to save the new database. The new database appears under **Databases**.

K.4.2 Creating a new database login account

If desired, you can create a login account for the new database and link it to the database you just created.

To create a new database owner:

1. In the SQL Server Management Studio, expand the **Security** folder, then right-click **Logins** and select **New Login**. The Login dialog appears.
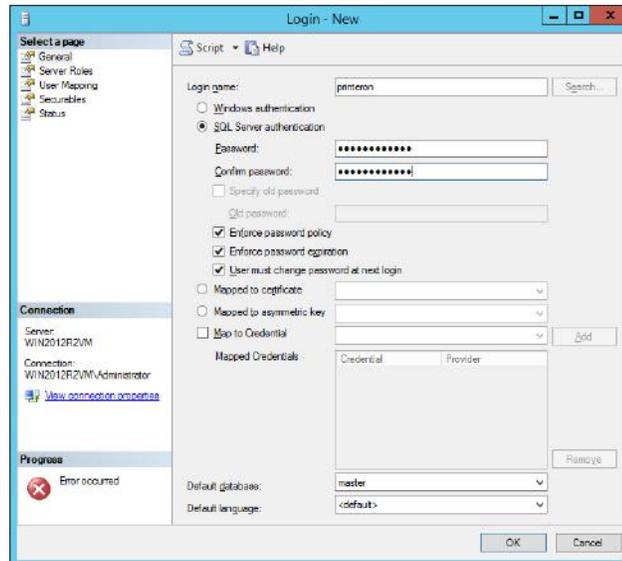
2. In the **Login name** field, enter the name used to login to the database.

3. Choose the authentication method.

    *   If you choose **Windows authentication**, the user must be logged into Windows with the specified login name to be able to access the database.

    *   If you choose **SQL Server authentication**, enter and confirm a **Password** for the account.

4. Configure the remaining login settings as necessary.

5. To associate the account with the new PrinterOn or IMCAS database, choose the database from the **Default database** drop-down.

6. Click **OK** to save the login information.

K.4.3 Migrating data to your SQL Server

As a best practice, it is recommended that you migrate the data of both the PrinterOn database and the IMCAS database, if used, to their new SQL Server locations. Migrating the databases ensures that the new databases are set up with the correct schema and avoids any issues later on.

To migrate the PrinterOn or IMCAS data to your own SQL Server, you'll need to back up the database in Configuration Manager, then restore it to the new location.

To migrate the PrinterOn or IMCAS data to your SQL Server:
1. Back up the databases.
2. Move the backup to your existing SQL server instance.
3. Verify the database schema.

K.4.3.1 Backing up the databases

To backup the PrinterOn and IMCAS databases:
1. In the Configuration Manager, click **Advanced** > **Components**.
2. Click the **Configure** button adjacent the **SQL Server** component. The SQL Server Backup Configuration page appears.
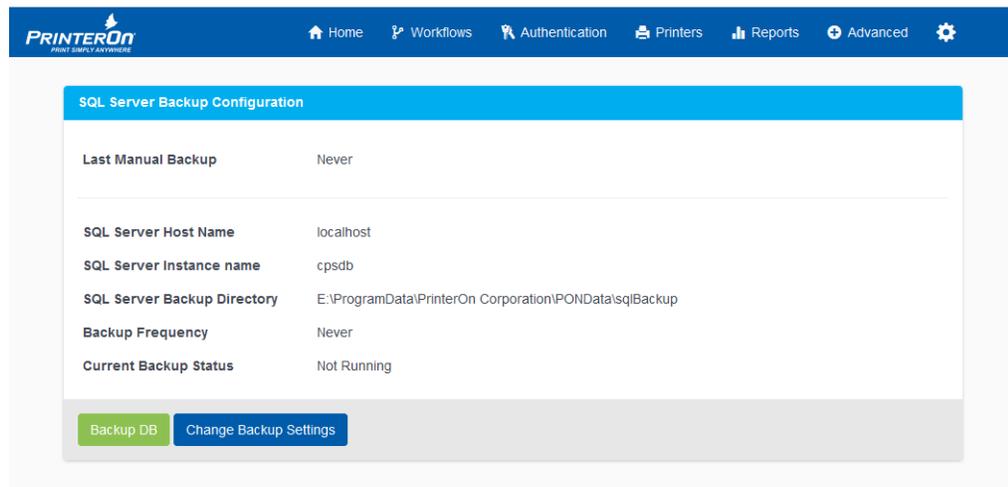
3. Confirm that the SQL Server Backup Directory is pointing to the location where you want to save the backup files.

To change where the backup is stored:

    a) Click **Change Backup Settings**.

    b) In the **SQL Server Backup Directory** field, enter the location where you want Configuration Manager to save the backup file.

    c) Click **Apply Settings**.

4. Click **Backup DB**.

K.4.3.2 Moving the PrinterOn database to your existing SQL Server instance

To move the database to your existing SQL Server instance:

1. In SQL Server Management Studio, right-click **Databases**, then select **Restore Database**. The Restore Database dialog appears.
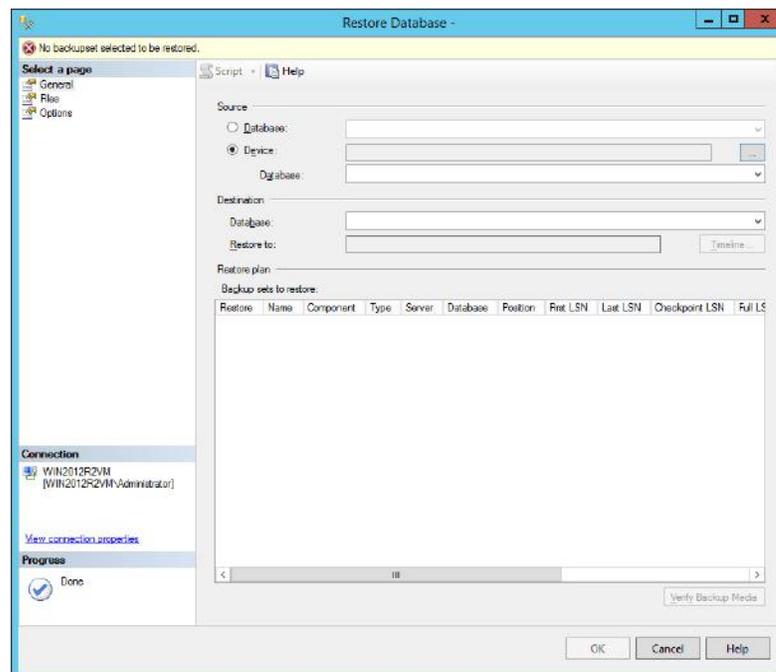
2. Browse to your PrinterOn or IMCAS database backup file:

    a) In the **Source** section of the Restore Database dialog, select **Device**, then click the **...** button. The Select Backup Devices dialog appears.
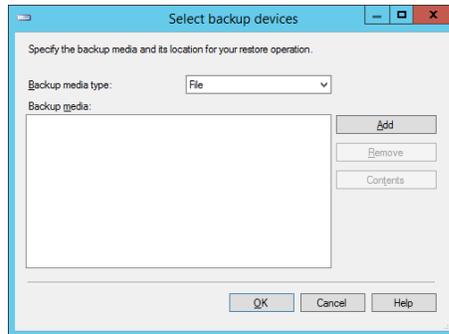
b) In the Select Backup Devices dialog, choose **File** as the **Backup media type**, then click **Add** to display the Locate Backup File dialog.
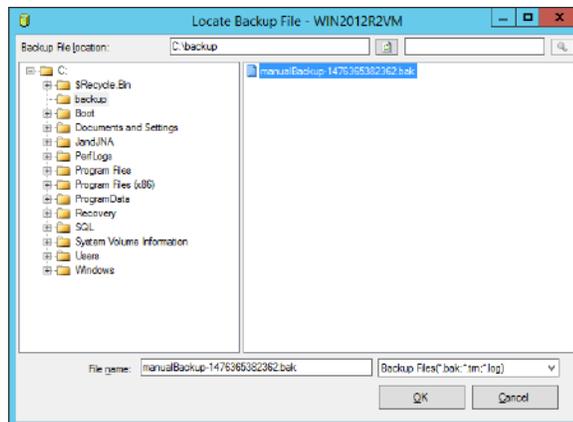
c) Navigate to the database backup file you created, then click **OK**.

3. In the **Destination** section of the Restore Database dialog, choose the database to restore the backup file to from the **Database** drop-down.

4. Click **Verify Backup Media** to ensure the backup file contains valid content.

5. Click **OK**.

K.4.3.3 Verifying the database schema

To ensure that the database tables were restored correctly:

1. In SQL Server Management Studio, create a query by right-clicking cpsdb and selecting **New Query**.

2. Enter the following query:

```
select * from printer
```

3. Press the F5 key to execute the query. The printer listing should be returned in bottom pane as shown below.
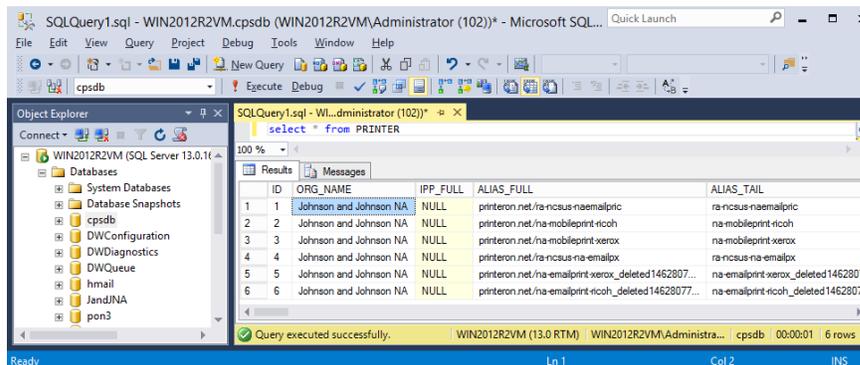
K.4.4 Modifying the PrinterOn service to use the new database locations

Once you have completed the migration of the PrinterOn databases, you can configure the PrinterOn server to use the new database locations. To point to the new databases, you need to manually modify the database properties files.

To point to the new database:

1. In the Configuration Manager, stop the Central Print Services.

2. In a text editor, open one of the following files:

    • C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\lib\cps-db.properties

    • C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\lib\imcas-db.properties

3. In the properties file, locate the `jdbc.url` entry.

4. Modify the connection string as follows:

    • Modify the server location (by default, set to `jdbc:sqlserver://localhost`) to point to your SQL Server. The entry must conform to the following syntax:

      `jdbc:sqlserver://[serverName[\instanceName][:portNumber]]`

    • If the login account for the database is a SQL Server account, remove the following property from the connection string:

      `integratedSecurity=true`

5. If the login account is a SQL Server account, modify the values of the `jdbc.user` and `jdbc.password` settings in the cps-db.properties file to reflect the username and password of the SQL Server account.

6. Save the file,

7. If necessary, repeat Steps 2 through 6 to modify the other properties file.

8. In the Configuration Manager, restart the CPS.

L
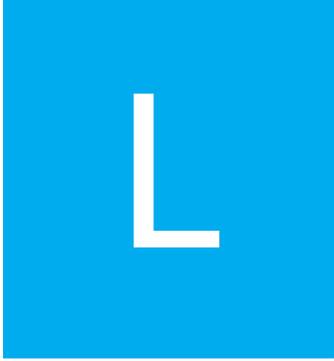
Integrating PrinterOn with third-party IDMs

This appendix outlines how to integrate the PrinterOn service with your third-party Identity Management Service. This process must be completed to configure PrinterOn to use any of these services for authentication.

The tasks outlined in this appendix are intended to provide some guidance to help you determine how to configure access permissions and retrieve communication settings to allow PrinterOn to use an external service for authentication and identity management.

This appendix provides integration information for the following services:
- Microsoft identity platform (both v2 Auth and legacy Azure AD v1 Auth)
- Ping Identity
- Okta

L.1 Integrating with the Microsoft identity platform

With PrinterOn Enterprise 4.2.3, PrinterOn supports both Microsoft v2 Auth and Microsoft v1 Auth. These versions differ slightly in how you integrate with the Printer service, and each provides its own unique set of endpoints.

- Integrating with the Microsoft identity platform (v2 Auth)
- Integrating with legacy Azure AD authentication (v1 Auth)

L.1.1 Integrating with the Microsoft identity platform (v2 Auth)

With v2 Auth, Microsoft has updated its identity platform to support personal Microsoft user accounts in addition to organizational accounts, and has more closely aligned the platform with the OAuth 2.0 specification.

The following section briefly outlines how to use the Azure AD management experience portal to configure the integration between Azure AD and the PrinterOn service.

Integrating PrinterOn with Microsoft identity platform involves the following steps:

1. Registering the PrinterOn service as a trusted app in Azure AD.
2. Adding additional Redirect URLs for PrinterOn client apps.
3. Granting PrinterOn permission to access Azure AD data.
4. Retrieving communication information from Azure AD to complete the configuration of PrinterOn's authentication settings.

L.1.1.1 Registering the PrinterOn service as a trusted app in Azure AD

To use Azure AD as an Identity management service, the PrinterOn service must first be registered as a trusted app within Azure AD.

To register PrinterOn with Azure AD:

1. Log in to the Azure portal at portal.azure.com.
2. In the left-hand pane, select **Azure Active Directory Service**.

3. Click **App Registrations** > **New registration.** The Register an Application panel appears.
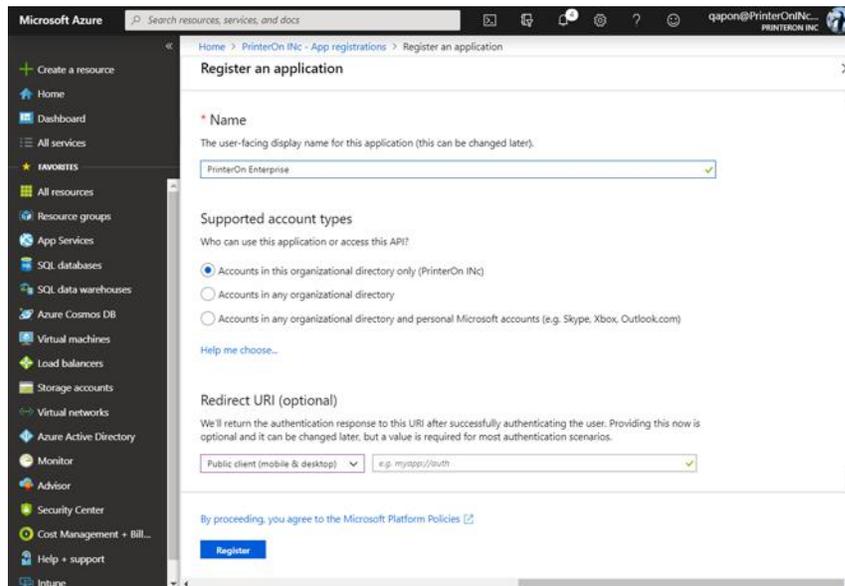
4. In the Register an application panel, enter the following information to identify the PrinterOn service:

Setting	Description
Name	A user-visible name for the application using Azure as it Authentication service. Set this value to **PrinterOn Enterprise**.
Supported account types	The accounts that you'd like users to authenticate with: • **Accounts in this organizational directory only**: Specifies that the PrinterOn service is only for use by users in your organization. • **Accounts in any organizational directory**: Specifies that the PrinterOn service is for use by any business or educational users. • **Accounts in any organizational directory and personal Microsoft accounts**: Specifies that users can access the PrinterOn service using their business account or a personal Microsoft account.

Setting	Description
Redirect URL	The type of app and the URL that Azure redirects the user to after authenticating. For PrinterOn Enterprise, specify the following values:

- For the app type, select **Public client (mobile and desktop)**.
- For the Redirect URL, specify the PrinterOn Sign-on URL. Set this value to https://*<PrinterOn_Service_URL>*/servlet/ LoginServlet. For example:

  https://123.45.67.89/cps/servlet/LoginServlet

  Note: The Sign-on URL must be accessible to external clients and must use SSL.

5. Click **Register**. PrinterOn Enterprise is registered by Azure AD as a trusted application. Azure displays the Overview panel for the PrinterOn Enterprise App.

You can now configure additional redirect URLs used by other PrinterOn client apps, such as PrintWhere or the PrinterOn Mobile Apps..

L.1.1.2 Adding additional Redirect URLs for PrinterOn client apps

If you intend to support printing from PrintWhere or the PrinterOn Mobile App, you'll need to add additional Redirect URLs for those client apps.

To add additional redirect URLS for the PrinterOn client apps.

1. In the App Registrations panel, locate and click the PrinterOn Enterprise app. The PrinterOn Enterprise app overview appears.
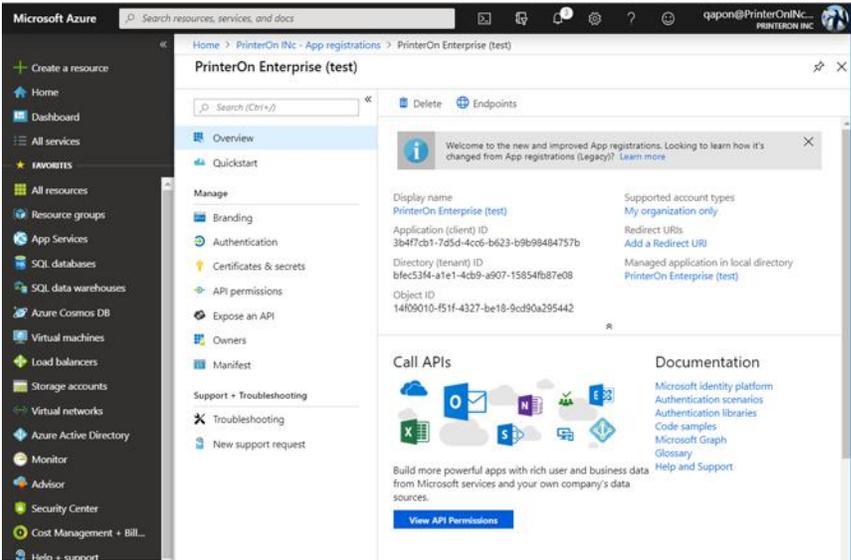
2. In the navigation pane of the Overview panel, click **Add a Redirect URI**, or, in the **Manage** menu, click **Authentication**.

   The Authentication Panel appears.

3. In the Redirect URIs section of the panel, add new

   • From the **Type** drop-down, select **Public client (mobile and desktop)**.

   • In the Redirect URI field, specify one of the following URIs as necessary:

Redirect URI	Used by
http://127.0.0.1:64000	**PrintWhere,** **PrinterOn Mobile App for Android**
https://sentinel.printeron.net/oauthredirect	**PrinterOn Mobile App**
ponauth://oauthredirect/	**PrinterOn Mobile App for iOS** **PrinterOn Mobile App for Android**

4. Repeat Step 2 for each of the required URIs.

5. Click **Save**.

You can now configure permissions that allow the PrinterOn service to access the required Azure AD data.

L.1.1.3 Granting PrinterOn permission to access Azure AD data

To permit PrinterOn to access the data it needs from Azure AD, you need to configure a number of permissions in Azure AD. In Microsoft v2 Auth, these permissions are associated with the Microsoft Graph API. The Microsoft Graph API lets PrinterOn synchronize with the Azure AD data.

> **Note:** PrinterOn only needs access to a very limited amount of Azure AD data. To keep your data secure, you should ensure that you only grant the necessary permissions, described in the following task.

To configure permissions in Azure AD:

1. In the App Registrations panel, locate and click the PrinterOn Enterprise app. The PrinterOn Enterprise app overview appears.

2. In the navigation pane, click **API Permissions**. The API permissions panel appears.
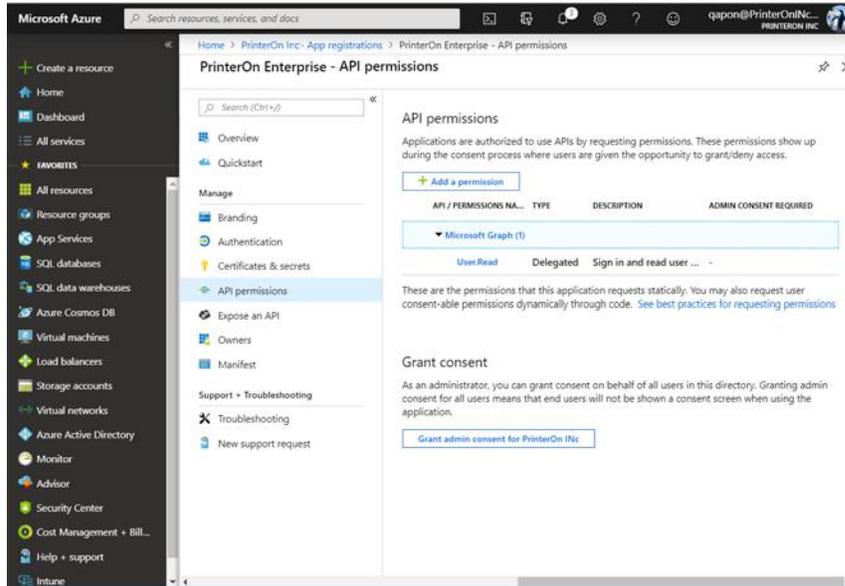

3. From the list of permissions, select **Microsoft Graph**. The Request API permissions panel appears. The Request API Permissions panel contains two tabs which allow you to set different levels of permissions:

   • **Delegated Permissions**: These permissions allow the PrinterOn service to access Azure AD on behalf of the user (for example, to submit authentication credentials on behalf of the user).

   • **Application Permissions**: These permissions allow the PrinterOn service to access Azure AD without a user being signed in (for example, to retrieve data).

4. In the **Delegated Permissions** tab, enable the following permissions:

Permission	Description
email	Allows the PrinterOn service to read your users' primary email address.
offline_access	Allows the PrinterOn service to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.
openid	Allows users to sign in to the PrinterOn service with their work or school accounts and allows the app to see basic user profile information.
profile	Allows the PrinterOn service to see your users' basic profile (name, picture, user name).

Permission	Description
Directory > Directory Read All	Allows the PrinterOn service to read data in your organization's directory, such as users, groups and apps.
Users > Users Read All	Allows the PrinterOn service to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.

5. Click the **Application Permissions** tab.
6. In the Application Permissions tab, enable the following permission:

Permission	Description
Directory > Directory Read All	Allows the PrinterOn service to read data in your organization's directory, such as users, groups and apps.

7. Click **Update Permissions**. The Request API Permissions Panel closes and returns you to the API Permissions Panel.
8. In the API Permissions Panel, click **Grant Admin Consent** to allow the PrinterOn service to access Azure AD without requiring user consent.

You can now retrieve the key Azure endpoints and application information so it can be added to PrinterOn's Configuration Manager, enabling the PrinterOn service to successfully communicate with Azure AD.

L.1.1.4 Retrieving communication information from Azure AD

To successfully authenticate and communicate with the Azure AD user store, you'll need to configure PrinterOn with the following information from Azure AD:

- The Azure AD endpoints:
  - **Authorization Endpoint**: The location where PrinterOn redirects the user when they attempt to sign in to use the service.
  - **Token Endpoint**: The location from which PrinterOn requests Access, ID, and Refresh tokens, which PrinterOn uses to determine the authentication status of the user.
  - **Graph API Endpoint**: The location where PrinterOn accesses the Azure AD Graph API, which allows PrinterOn to synchronize data between the Azure AD and PrinterOn user stores.

Note: Endpoints are the same for all applications in the same directory.

- **Application ID**: Automatically assigned to your PrinterOn service when you registered it as a trusted application in Azure AD.
- **Application Key**: A secret code that you must generate in Azure AD, also automatically generated when you registered the PrinterOn service.

You'll need to copy these pieces of information from Azure AD into Configuration Manager to configure your authentication settings.

To retrieve the communication information from Azure AD:

1. In the App Registrations panel, locate and click the PrinterOn Enterprise app. The PrinterOn Enterprise app overview appears.
2. At the top of the Overview panel, click **Endpoints**.
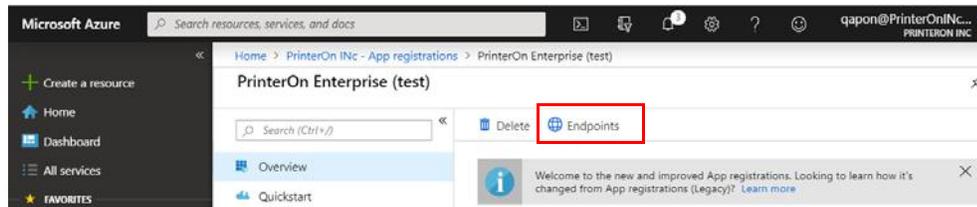
The Endpoints panel appears.
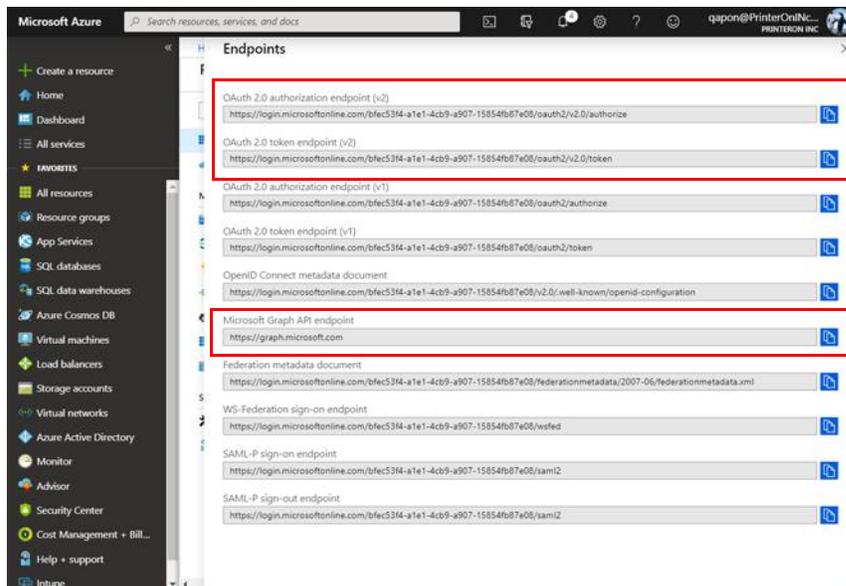
3. Locate and copy each of the following endpoints. You'll paste these values into the fields of the same name in the Azure AD configuration in Configuration Manager.

- OAuth 2.0 Authorization Endpoint (v2)
- OAuth 2.0 Token Endpoint (v2)
- Microsoft Azure AD Graph API Endpoint

> **Note:** Ensure that you copy the v2 Authorization and Token endpoints.

4. Close the Endpoints panel to return to the Overview panel, then locate and copy the **Application (client) ID** value. You'll paste this value in the Application ID field in the Azure AD configuration in Configuration Manager.
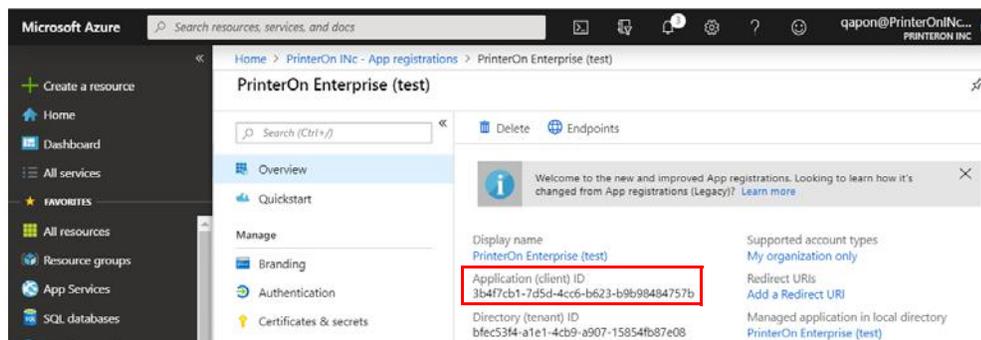
5. In the Overview panel, under API Access, click **Certificates & secrets**. The Certificates & secrets panel appears.
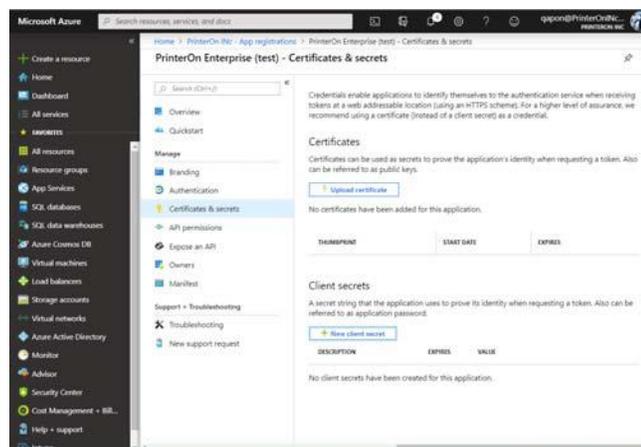
6. In the Client Secret section of the panel, click **New Client Secret**. The Client Secret dialog appears, where you can generate your secret key.
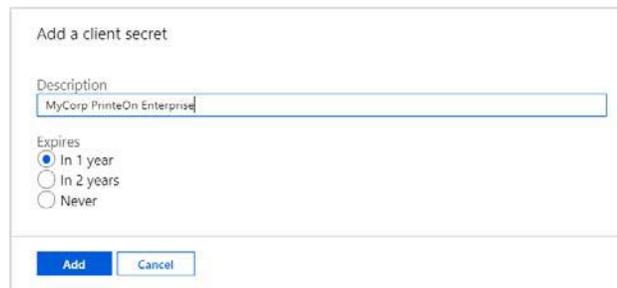
a) Complete the **Description** and **Expires** fields.

b) Click **Add**. Azure AD generates the Application key.

7. Copy and save this value. You'll use this value in the Application Key field in the Azure AD configuration in Configuration Manager.

L.1.2 Integrating with legacy Azure AD authentication (v1 Auth)

The following section briefly outlines how to use the Azure AD management experience portal to configure the integration between legacy Azure AD authentication for use with the PrinterOn service.

Integrating PrinterOn with legacy Azure AD authentication involves the following steps:

1. Registering the PrinterOn service as a trusted app in Azure AD.
2. Adding additional Redirect URLs for PrinterOn client apps.
3. Granting PrinterOn permission to access Azure AD data.
4. Retrieving communication information from Azure AD to complete the configuration of PrinterOn's authentication settings.

L.1.2.1 Registering the PrinterOn service as a trusted app in Azure AD

To use Azure AD as an Identity management service, the PrinterOn service must first be registered as a trusted app within Azure AD.

To register PrinterOn with Azure AD:

1. Log in to the Azure portal at portal.azure.com.
2. Go to the directory where you want to register the app.

3. Click **App Registrations (Legacy)**. The App Registrations panel appears.
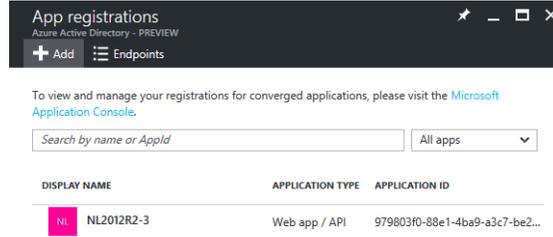
4. Click **New Application Registration**. The Create Panel appears.

5. Enter the following information to identify the PrinterOn service:

Setting	Description
Name	A user-visible name for the application using Azure as it Authentication service. Set this value to **PrinterOn Enterprise**.
Application Type	The type of application, used by Azure AD to determine a specific authentication workflow. Select **Web App/API** from the drop-down. PrinterOn should always be defined as Web App/API (even if users will primarily be using the mobile app).
Sign-on URL	The Sign-on URL is used by the Web Print Portal. Set this value to https://*<PrinterOn_Service_URL>*/servlet/ LoginServlet. For example: https://123.45.67.89/cps/servlet/LoginServlet The Sign-on URL must be accessible to external clients and must use SSL. This value will also impact the default Reply-URLs.

6. Click **Create**. PrinterOn Enterprise is registered by Azure AD as a trusted application and added to the App Registration panel.

You can now configure additional redirect URLs used by other PrinterOn client apps, such as PrintWhere or the PrinterOn Mobile Apps..

L.1.2.2 Adding additional Redirect URLs for PrinterOn client apps

If you intend to support printing from PrintWhere or the PrinterOn Mobile App, you'll need to add additional Redirect URLs for those client apps.

To add additional Redirect URLs:

1. In the Registration panel, click **All Settings**.
2. In the Settings panel, click **Reply URLs**. The Reply URL panel appears with the Web Print URL already listed.
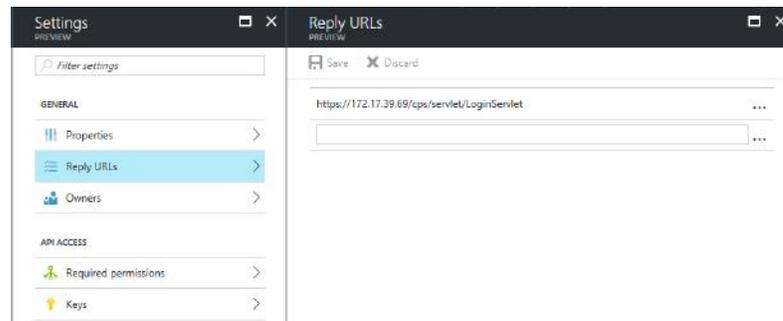
3. In the Reply URLs panel, add the following URLs:

Authentication URL	Used by
http://127.0.0.1:64000	**PrintWhere,** **PrinterOn Mobile App for Android**
https://sentinel.printeron.net/oauthredirect	**PrinterOn Mobile App**
ponauth://oauthredirect/	**PrinterOn Mobile App for iOS** **PrinterOn Mobile App for Android**

4. Click **Save**.

You can now configure permissions that allow the PrinterOn service to access the required Azure AD data.

L.1.2.3 Granting PrinterOn permission to access Azure AD data

To permit PrinterOn to access the data it needs from Azure AD, you need to configure a number of permissions in Azure AD. These permissions are associated with two Azure AD APIs:

- **Microsoft Azure Active Directory**: Lets PrinterOn sign in to Azure AD.
- **Microsoft Graph**: Lets PrinterOn synchronize with the Azure AD data.

> **Note:** PrinterOn only needs access to a very limited amount of Azure AD data. To keep your data secure, you should ensure that you only grant the necessary permissions, described in the following task.

To configure permissions in Azure AD:

1. In the Registration panel, click the PrinterOn Enterprise app. The PrinterOn Enterprise app summary appears.

2. Click **All Settings**. The Settings panel appears.
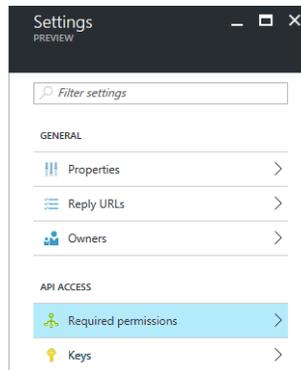
3. In the Settings panel, click **Required Permissions**. The Required Permissions panel appears, listing the APIs to which you can grant permissions.

4. In the API list of the Required Permissions panel, click **Microsoft Azure ActiveDirectory**. The Enable Access panel appears displaying all Azure AD permissions.
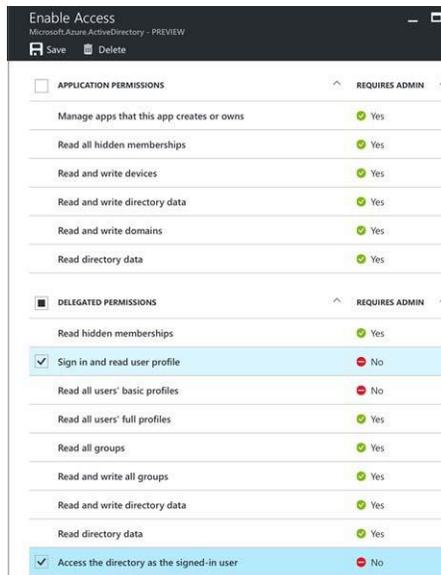
5. Enable the following permissions:

Permission	Description
Sign in and read user profile	Allows users to sign-in to the app, and allows PrinterOn to read the profile of signed-in users as well as basic company information of the signed-in user.
Access the directory as the signed-in user	Allows PrinterOn to have the same access to information in the directory as the signed-in user.

6. Click **Select**.

7. If the Microsoft Graph API is not listed, then in the Required Permissions panel, click **Add** and add the **Microsoft Graph** API to the list.
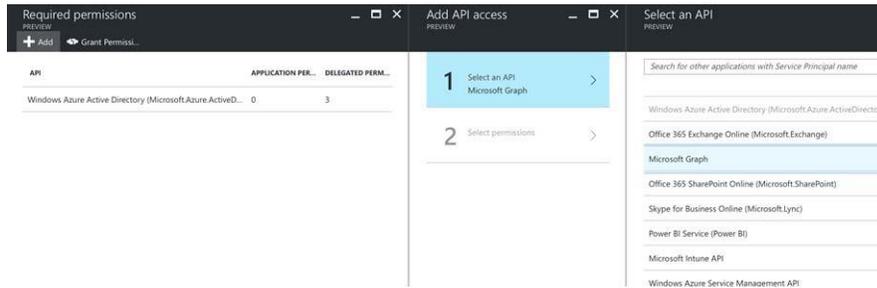
8. In the API list of the Required Permissions panel, click **Microsoft Graph**. The Enable Access panel appears displaying all Microsoft Graph permissions.

9. Enable the following permissions:

Permission	Description
Read all groups	Allows PrinterOn to list groups, and to read their properties and all group memberships on behalf of the signed-in user. PrinterOn pulls the group information into the PrinterOn user store, allowing you to create user access rules without requiring you to first create the user groups manually.
Read all users' full profiles	Allows PrinterOn to read the full profile of all users in the organization. For some workflows, information available from the basic profile is not enough to enable PrinterOn to provide print services with the existing print infrastructure. Certain workflows, such as Email print and native iOS and macOS Printing, require PrinterOn to locate a user using their email address. This information is only available in the user's full profile. To support these workflows, PrinterOn requires the ability to read the full profile.

10. Click **Select**.

11. In the Required Permissions panel, click **Grant Permissions**, then confirm the action.

You can now retrieve the key Azure endpoints and application information so it can be added to PrinterOn's Configuration Manager, enabling the PrinterOn service to successfully communicate with Azure AD.

L.1.2.4 Retrieving communication information from Azure AD

To successfully authenticate and communicate with the Azure AD user store, you'll need to configure PrinterOn with the following information from Azure AD:

- The Azure AD endpoints:
  - **Authorization Endpoint**: The location where PrinterOn redirects the user when they attempt to sign in to use the service.
  - **Token Endpoint**: The location from which PrinterOn requests Access, ID, and Refresh tokens, which PrinterOn uses to determine the authentication status of the user.

- **Graph API Endpoint**: The location where PrinterOn accesses the Azure AD Graph API, which allows PrinterOn to synchronize data between the Azure AD and PrinterOn user stores.

> **Note:** Endpoints are the same for all applications in the same directory.

- **Application ID**: Automatically assigned to your PrinterOn service when registered it as a trusted application in Azure AD.
- **Application Key**: A secret code that you must generate in Azure AD.

You'll need to copy both these pieces of into Configuration Manager to configure your authentication settings.

To retrieve the communication information from Azure AD:

1. In the Azure Portal, click **App Registrations**. The App Registrations panel appears.
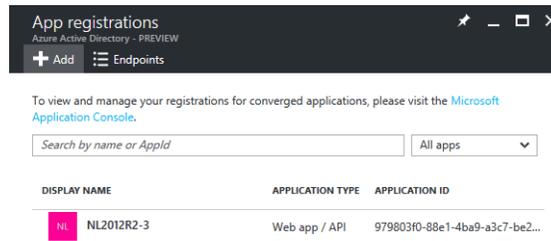
2. Click Endpoints. The Endpoints panel appears.
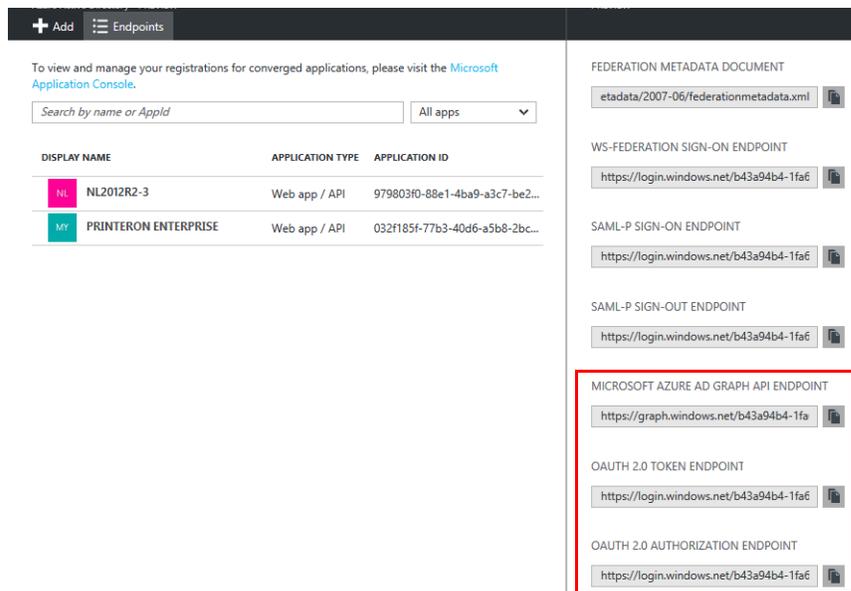
3. Locate and copy each of the following endpoints. You'll paste these values into the fields of the same name in the Azure AD configuration in Configuration Manager.

- Microsoft Azure AD Graph API Endpoint
- OAuth 2.0 Token Endpoint
- OAuth 2.0 Authorization Endpoint

4. In the Registration panel, click the PrinterOn Enterprise app. The PrinterOn Enterprise app summary appears.

5. In the PrinterOn Enterprise app summary, copy the Application ID value. You'll paste this value in the Application ID field in the Azure AD configuration in Configuration Manager.
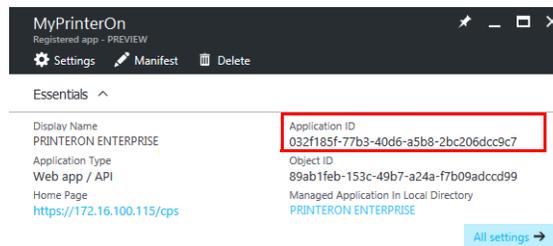
6. In the PrinterOn app summary, click **All Settings**. The Settings Panel Appears.
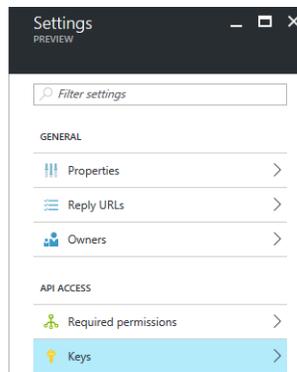
7. In the Settings panel, under API Access, click **Keys**. The Keys panel appears.

8. In the Keys panel, generate your secret key:
   a) Complete the **Description** and **Expires** fields.
   b) Click **Save**. Azure AD generates the Application key.

9. Copy and save this value. You'll use this value in the Application Key field in the Azure AD configuration in Configuration Manager.

L.2 Integrating PrinterOn with Ping Identity

When integrating the PrinterOn service with Ping Identity, you must configure Ping Identity with the following settings:

Setting	Description
Application Type	Register PrinterOn as a **Web Application**.
Client ID	Ping allows you to enter your own Client ID. Enter any value, such as PrinterOnServer or PrinterOnEnterprise. The value you enter in Ping must also be entered in the Client ID field in the **Third-Party Identity Management Service** configuration in Configuration Manager.
Client Secret	PrinterOn requires a client secret to be generated and shared with PrinterOn Enterprise. This value must be entered in the Client Secret field in the **Third-Party Identity Management Service** configuration in Configuration Manager.
Allowed Grant Types	You should configure the following grant types: • **Authorization Code**: Must be **enabled**. When enabled, Ping Identity returns an authorization code to the PrinterOn through a browser redirect. PrinterOn then exchanges the authorization code for an Access and Refresh Token. This is the most commonly used flow and will be used by the PrinterOn mobile apps, PrintWhere, and web print to provide a form for authentication • **Refresh Token**: Must be **enabled**. • **Resource Owner Credentials**: Must be **enabled**. This setting is used in conjunction with AirPrint. It allows PrinterOn to pass the user credentials through to AirPrint on the user's behalf, since AirPrint has no means of allowing the user to enter them.

Setting	Description

Redirection URLs	You must configure Ping Identity to use the following redirection URIs:
	
	• The Web Print authentication URL:
	
	    https://*<PrinterOn_ServiceURL>*/servlet/LoginServlet
	    For example:
	    https://123.45.67.89/cps/servlet/LoginServlet
	
	    This URL must be accessible to external clients and must use SSL. This value will also impact the default Reply-URLs.
	
	• The PrintWhere and PrinterOn Mobile App authentication URL:
	
	    http://127.0.0.1:64000
	
	    Note: In some cases, Ping Identity may have issues redirecting to this URL. If you experience issues, add the following URL in addition to the URL specified above:
	    http://127.0.0.1:64000/
	
	• PrinterOn Mobile App authentication URL:
	
	    https://sentinel.printeron.net/oauthredirect
	    ponauth://oauthredirect/

Bypass Authorization Approval	PrinterOn recommends that you disable this setting for an improved user experience.
ID Token Signing	This setting is not required.

L.2.1 Completing the Ping Identity integration

With the PrinterOn service registered as an app in Ping Identity, you can complete the integration by configuring the Third-party Authentication settings in Configuration Manager.

To configure the PrinterOn service to use Ping Identity, you'll need your Ping Identity **Client ID** and **Client Secret**.

L.3 Integrating PrinterOn with Okta

When integrating your PrinterOn service with Okta Identity Management service, you must register PrinterOn as a trusted app in Okta.

To register PrinterOn with Okta:

1. Log in to the Okta portal at your Okta Org URL.
2. In the Okta console, click **Applications**. The Applications tab appears.
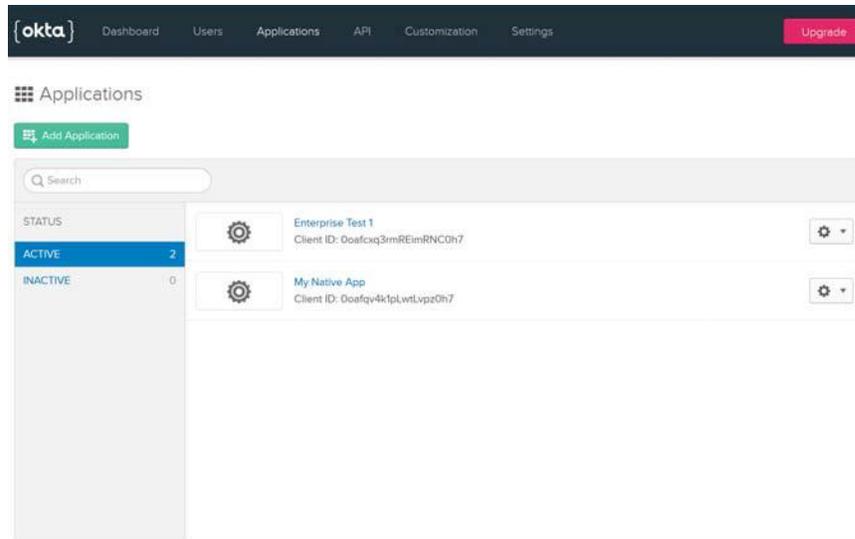
3. Click **Add Application**. The Create New Application page appears.
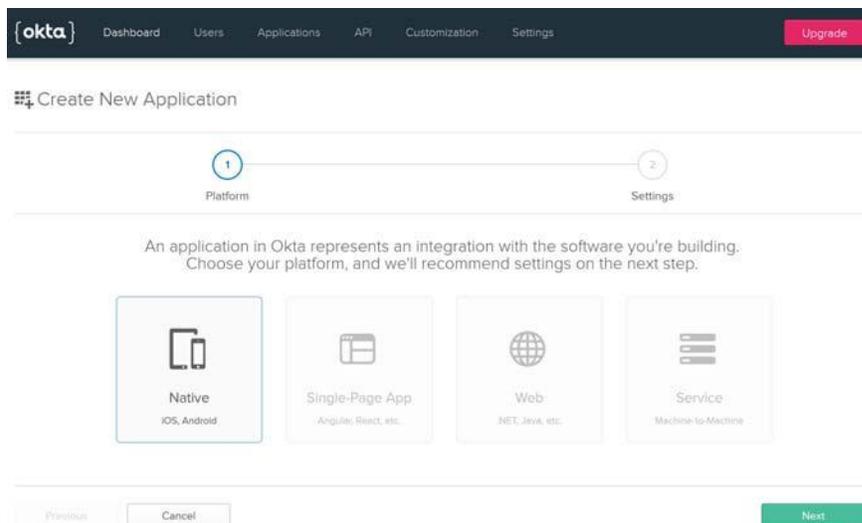
4. For the application platform, select **Native**, then click **Next**. The Settings page appears.

5. In the Application Settings section, configure the settings as follows:

Setting	Description
Name	Specify a unique name you'll use to identify the PrinterOn service.

Login redirect URIs	Specify the following redirect addresses. Click **Add URI** to add additional fields.
	
	• The Web Print authentication URL:
	
	    https://*<ServiceURL>*/cps/servlet/LoginServlet
	
	  where *<ServiceURL>* is the Service URL for your PrinterOn service.
	
	• The PrintWhere and PrinterOn Mobile App authentication URL:
	
	    http://127.0.0.1:64000
	    http://127.0.0.1:64000/
	
	• PrinterOn Mobile App authentication URLs:
	
	    https://sentinel.printeron.com/oauthredirect
	    ponauth://oauthredirect/

Grant types allowed	Configure the following grant types: • **Authorization Code**: Must be **enabled**. • **Refresh Token**: Must be **enabled**. • **Resource Owner Password**: Must be **enabled**. This setting is used in conjunction with AirPrint. It allows PrinterOn to pass the user credentials through to AirPrint on the user's behalf, since AirPrint has no means of allowing the user to enter them.

6. Click **Done**. The app is created and the General tab appears.

Once the app is created, there is one more setting you need to modify in order to generate the client secret, which you'll need to properly configure the PrinterOn server to use the Okta service.

7. In the General tab, scroll down to the **Client Credentials** panel, then click **Edit** to edit the credentials settings.
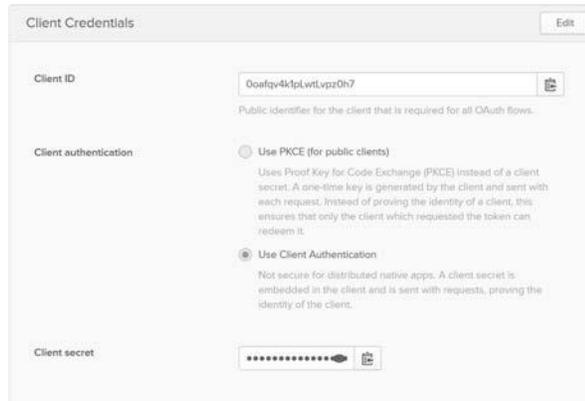
8. Change the Client authentication setting to **Use Client Authentication**, then click **Save**. A client secret is generated and displayed in the panel.

You'll need to copy the **Client secret**—as well as the **Client ID**—into Configuration Manager to configure your authentication settings.

L.3.1 Completing the Okta integration

With the PrinterOn service registered as an app in Okta, you can complete the integration by configuring the Third-party Authentication settings in Configuration Manager.

To configure the PrinterOn service to use Okta, you'll need your Okta **Client ID** and **Client Secret**. These values are found in the Client Credentials panel of the General tab. Okta provides a **Copy to clipboard** button beside each of these values, allowing you to easily copy them and pasting them into the PrinterOn Configuration Manager.

M

Registering your EWS mail client with Azure AD

If you are enabling OAuth authentication for your EWS service, you must register your EWS service with Azure AD and define the level of access to the EWS service the user has once authenticated.

You may also need to set up a client secret or a client certificate, depending on which authorization method you choose to use.

M.1 Registering the EWS mail client

To register your EWS service with Azure AD:

1. Log in to the Azure portal (portal.azure.com) using your Office 365 credentials.
2. Click **Azure Active Directory**.

3. In the left navigation, click **App registrations**.
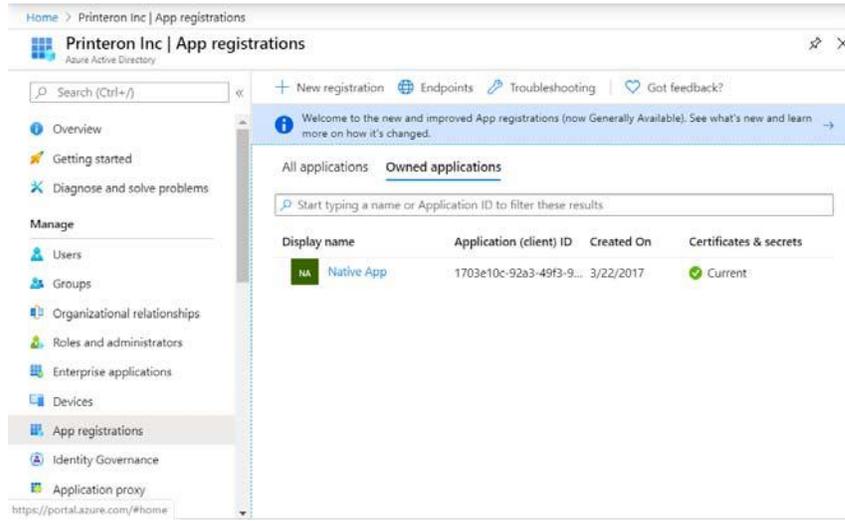
4. From the top menu, click **New registration**. The Register an Application page appears.
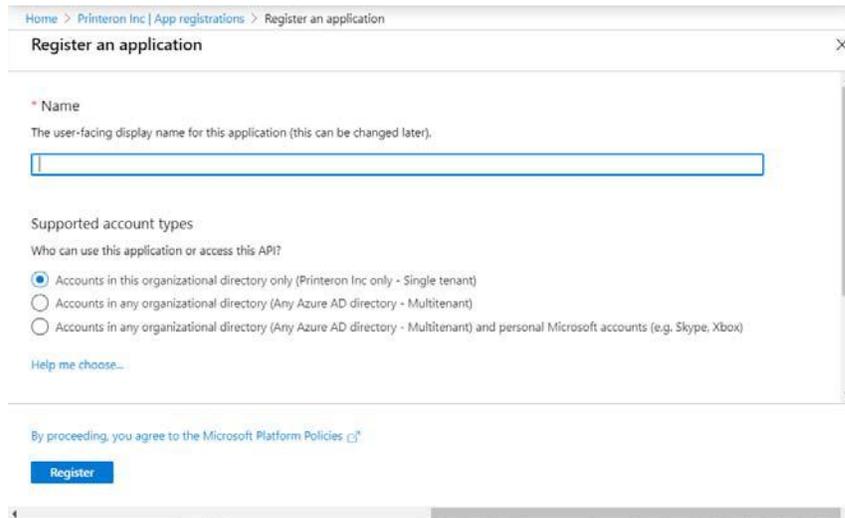
5. In the **Name** field, specify a name for you EWS mail client, then complete the remaining Registration settings as necessary.

6. Click **Register**. The EWS mail is registered by Azure AD and an overview of the app is displayed.
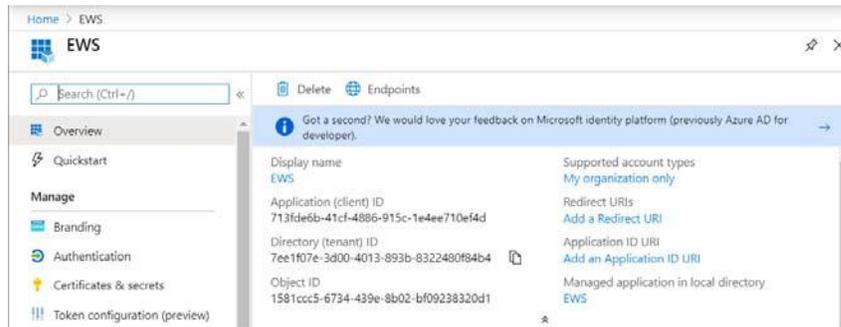
7. In the overview, locate and copy the **Application ID** and **Directory (tenant) ID** values.
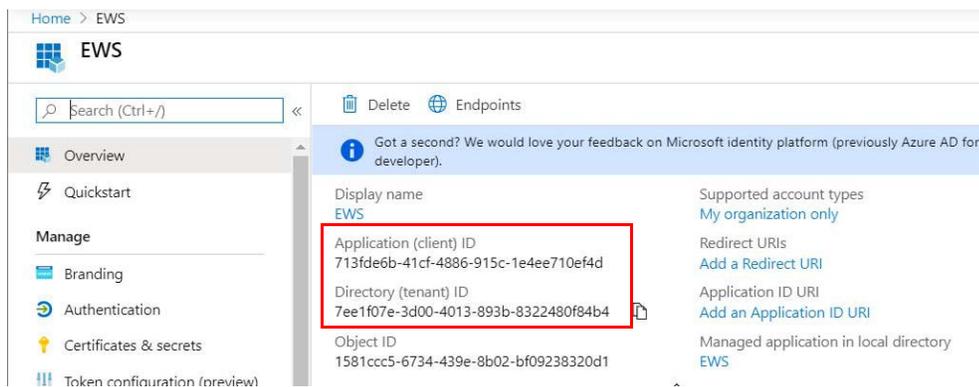
You'll need to paste this value as the Client ID and Tenant ID value in the OAuth Configuration settings in the Configuration Manager.

Next, you'll need to configure the Authentication settings for the EWS client.

M.2 Configuring authentication for the EWS mail client

With the EWS client registered with Azure AD, you can configure its authentication settings, which define how the client will authenticate to receive an Access token on behalf of the user. There are several supported methods that you can choose to use:

- **Client certificate:** The client certificate option offers the highest level of assurance, as it requires the EWS client to have a digital certificate to prove its identity against a server certificate before it can receive an Access token. However, it also

requires you to have an existing client certificate to upload into Azure AD, and the corresponding server certificate uploaded to the PrinterOn Server.

This method is only available for on-premise deployments of PrinterOn Enterprise.

For more information on setting up Client certificate authentication for your EWS mail client, Setting up Client Certificate authentication.

- **Shared client secret:** Though not considered as rigorously secure as the client certificate, the shared secret method still offers a high degree of assurance. You need only create a unique secret in Azure AD, then copy that secret into Configuration Manager. Azure AD compares the secret value to its own secret value and only returns an Access token if the values match.

  For more information on configuring a shared client secret, see Setting up a Client Secret.

- **ROPC (Resource Owner Password Credential) Flow**: With this method, the EWS mail client simply passes the Tenant ID or the OAuth Directory value to Azure AD to receive an Access token.

  > **Note:** Because it requires only a single, easily identifiable credential to prove the client's identity, this authentication method is not considered highly secure and is generally not recommended in production environments unless there is an implicit level of trust between the client and server.

  For more information on configuring ROPC Flow authentication, see Setting up ROPC Flow Authentication.

M.2.1 Setting up Client Certificate authentication

Before you can set up your email client to use a certificate for authorization, you'll need a certificate from a trusted Certificate Authority (CA). Acquiring a certificate is outside the scope of this documentation. However, there are a number of CAs you can contact.
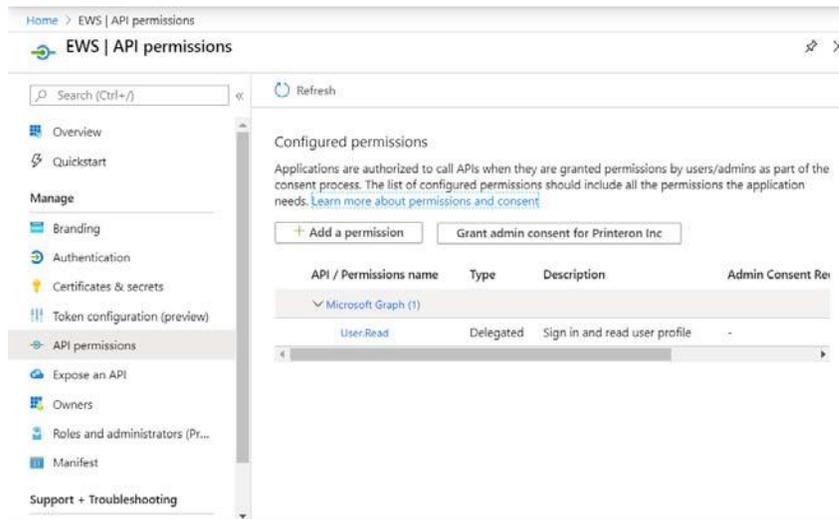
This procedure assumes you have a client certificate available and a server certificate installed on the PrinterOn server.

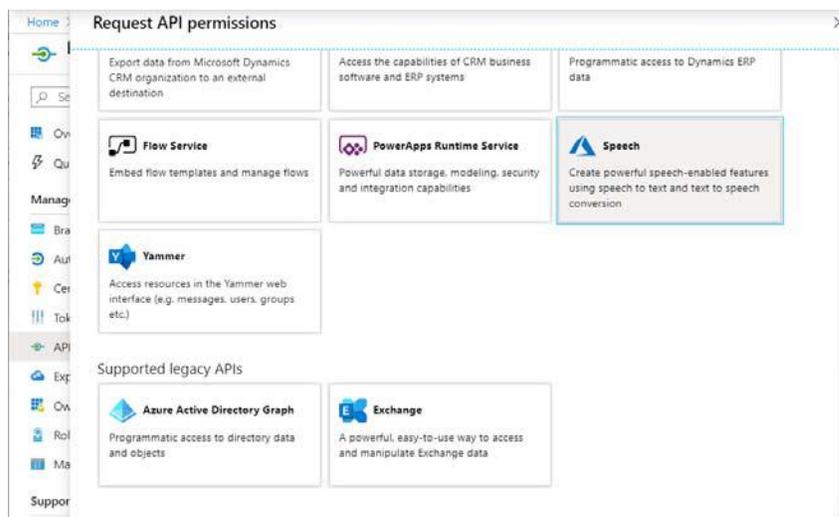This authentication method is not available for managed cloud deployments of PrinterOn Enterprise.

To set up a client certificate:

1. In the left navigation pane of the Azure portal, click **Certificates and Secrets**.

2. In the Certificates section, click **Upload Certificate**. The Upload Certificate dialog appears.

3. Browse the folder where the client certificate is stored and select the certificate.

4. Next, you can specify the API permissions for the app. From the left menu, click **API Permissions**. The API Permissions panel appears.
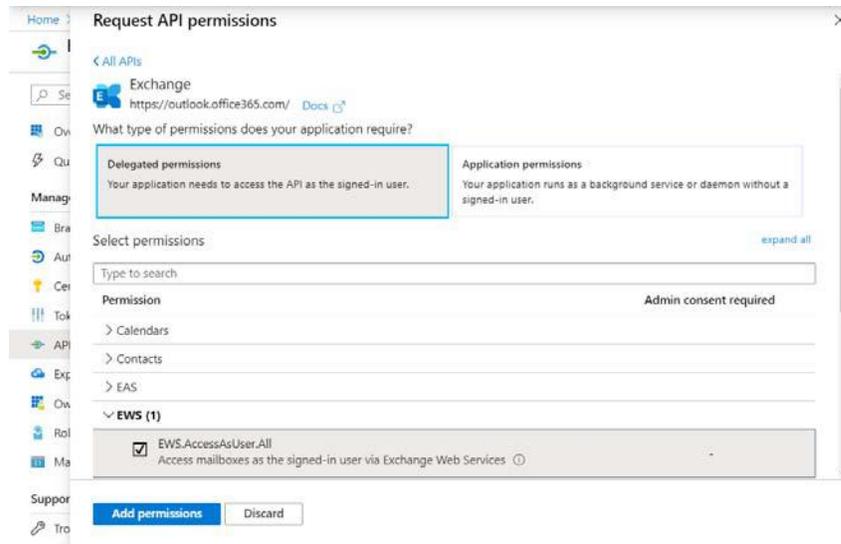

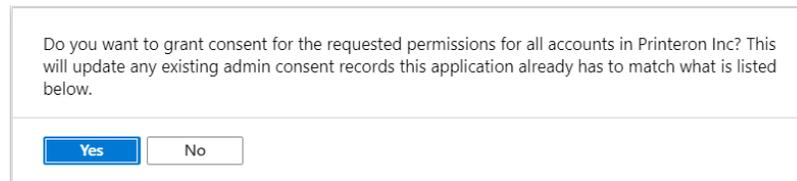5. Click **Add a permission**. The Request API Permissions page appears.

6. Scroll to the bottom of the page. Under the Supported legacy APIs section, select **Exchange**. The Exchange permissions page appears.

7. In the Exchange permissions page, choose **Application permissions**, then, from the list of delegated pemissions, expand the **EWS** group and click **EWS.AccessAsUser.All**.

8. Click **Add Permissions** to add the permission and return to the API permissions page.
9. Click **Grant admin consent**. A message will pop up asking you to grant consent for all accounts in your organization.



10. Click **Yes** to grant consent.

M.2.2 Setting up a Client Secret

To set up a client secret:

1. In the left navigation pane of the Azure portal, click **Certificates and Secrets**.
2. In the Client secrets section, click **New Client** secret. The Add a client secret dialog appears.
3. Enter a **Description** for the secret, and select an **Expiry** option.
4. Click **Add**. The secret is displayed in the list of secrets.

5. Copy the secret. You will add this value to the ClientSecret field in the OAuth Configuration settings in the Configuration Manager.

> **Note:** The secret is only visible immediately after it has been created. As soon as you perform another task or leave the page, the secret is permanently obfuscated and cannot be recovered. If you are unable to successfully copy the secret before it becomes obfuscated, you can simply create a new secret.
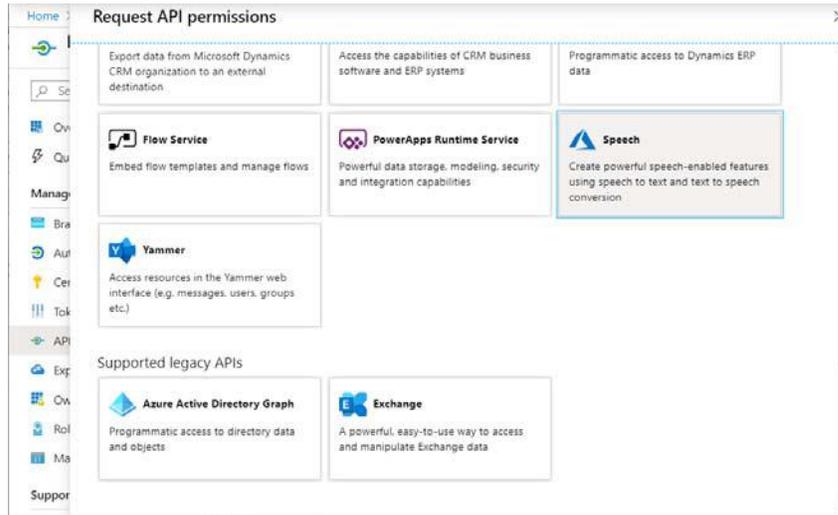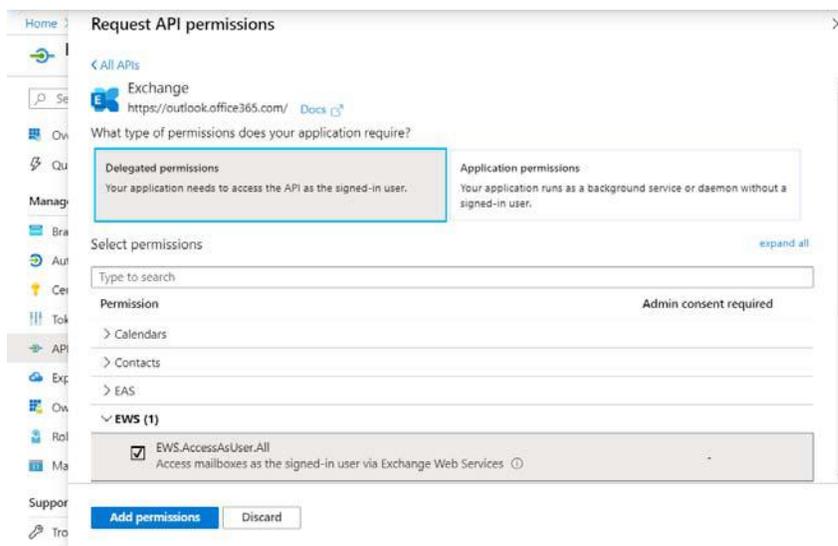
6. From the left menu of the Azure AD portal, click **Authentication**. The Authentication panel appears.
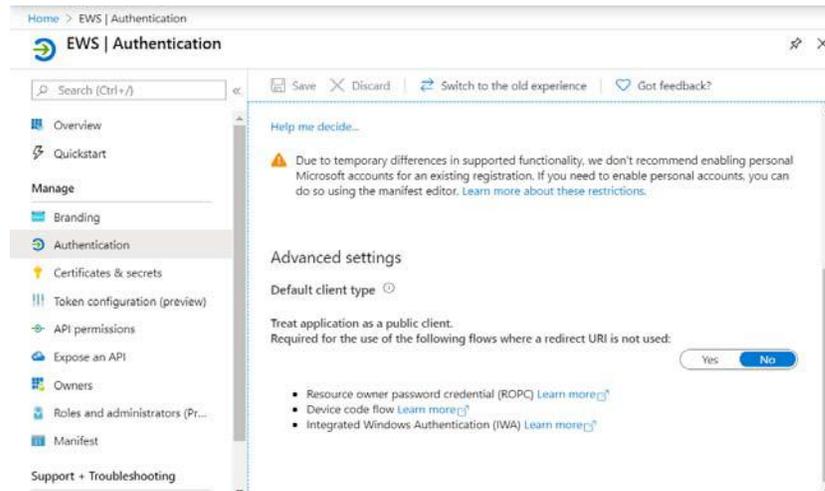
7. Next, you can specify the API permissions for the app. From the left menu, click **API Permissions**. The API Permissions panel appears.
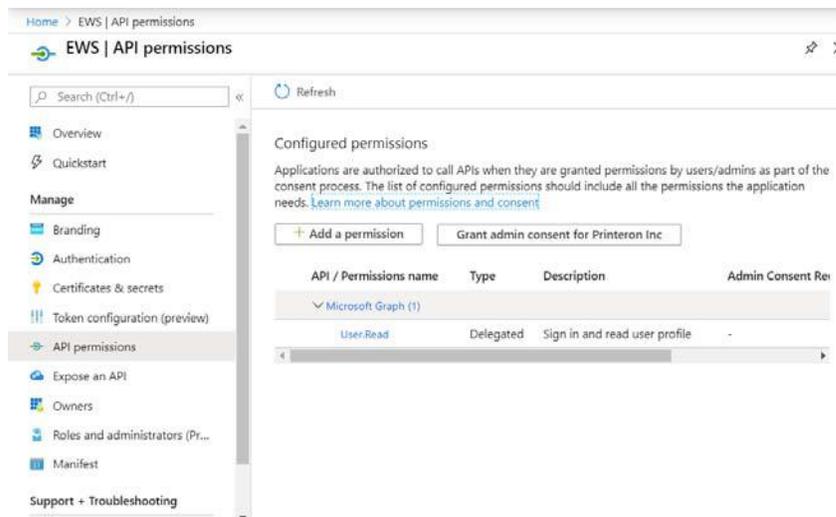
8. Click **Add a permission**. The Request API Permissions page appears.


9. Scroll to the bottom of the page. Under the Supported legacy APIs section, select **Exchange**. The Exchange permissions page appears.

10. In the Exchange permissions page, choose **Application permissions**, then, from the list of delegated pemissions, expand the **EWS** group and click **EWS.AccessAsUser.All**.

11. Click **Add Permissions** to add the permission and return to the API permissions page.

12. Click **Grant admin consent**. A message will pop up asking you to grant consent for all accounts in your organization.
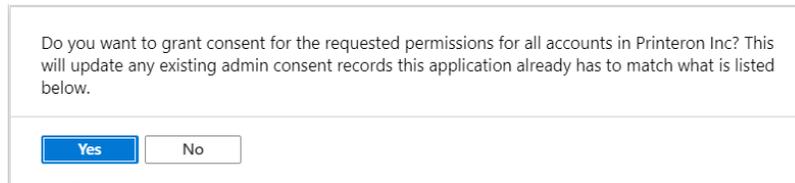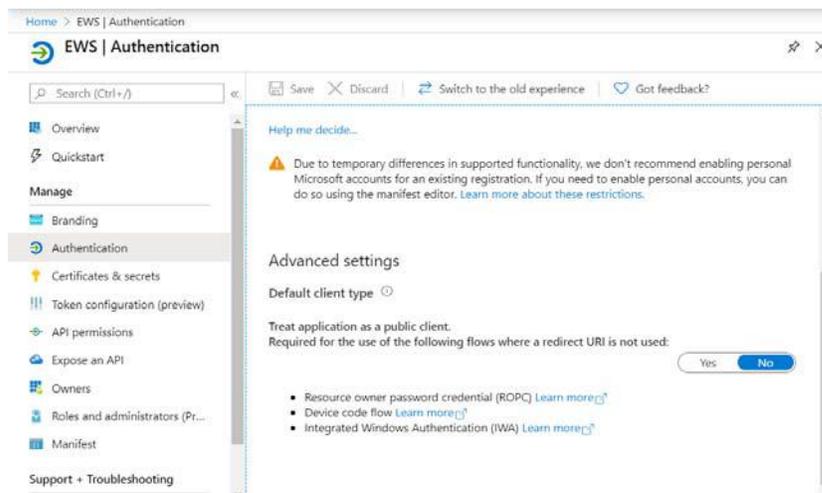

13. Click **Yes** to grant consent.

M.2.3 Setting up ROPC Flow Authentication

To set up ROPC Flow Authentication:

1. From the left menu of the Azure AD portal, click **Authentication**. The Authentication panel appears.


2. Scroll to the bottom of the Authentication panel and locate the Advanced Settings section. Toggle the switch to **Yes** to treat the application as a public client.

3. Click **Save**.

4. Next, you can specify the API permissions for the app. From the left menu, click **API Permissions**. The API Permissions panel appears.
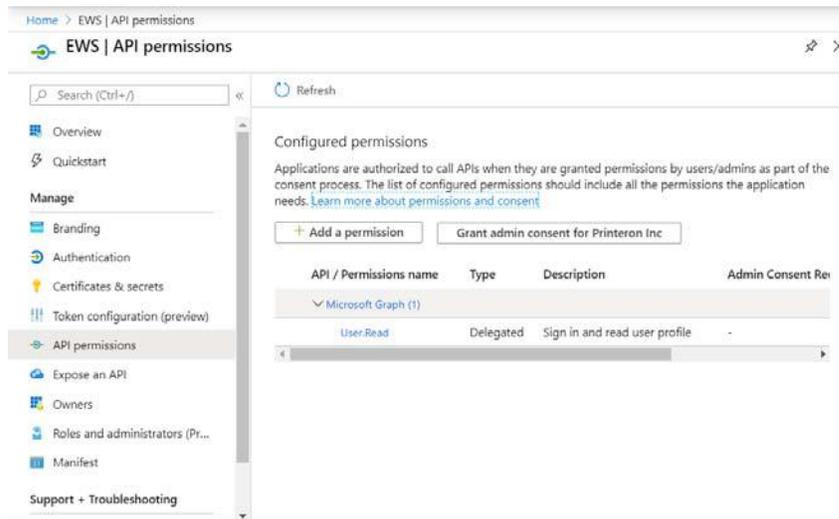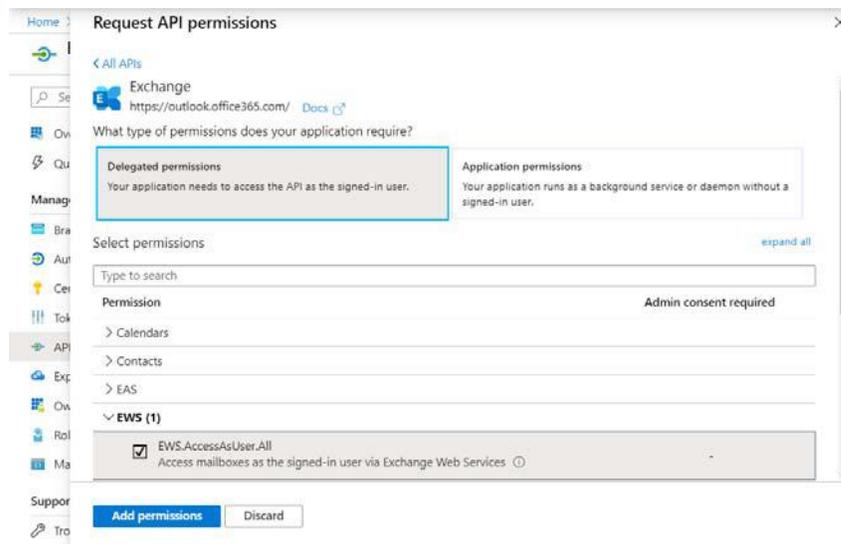

5. Click **Add a permission**. The Request API Permissions page appears.
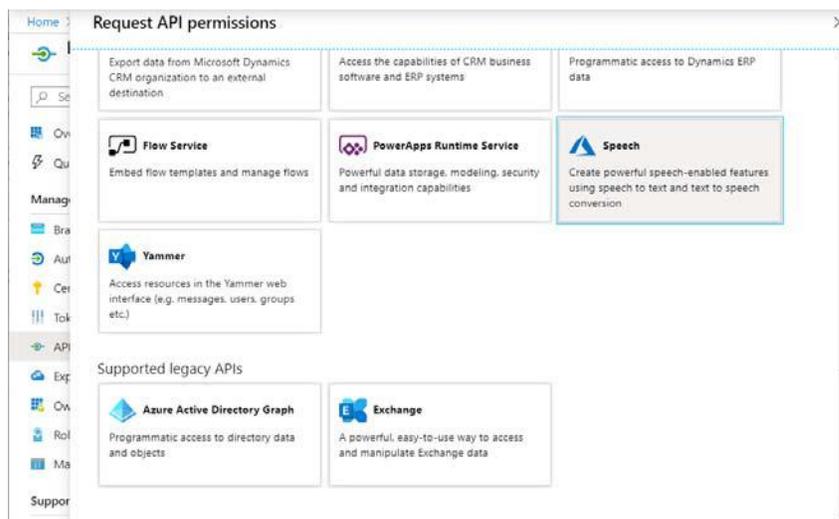
6. Scroll to the bottom of the page. Under the Supported legacy APIs section, select **Exchange**. The Exchange permissions page appears.

7. In the Exchange permissions page, choose **Delegated**, then, from the list of delegated pemissions, expand the **EWS** group and click **EWS.AccessAsUser.All**.

8. Click **Add Permissions** to add the permission and return to the API permissions page.

9. Click **Grant admin consent**. A message will pop up asking you to grant consent for all accounts in your organization.
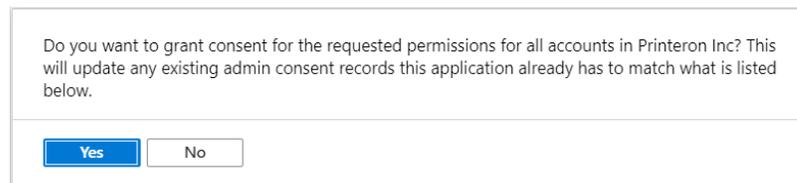
10. Click **Yes** to grant consent.

N

Additional configuration details

Due to system or network changes, or the unique needs or characteristics of your PrinterOn service deployment, you may need to perform some additional configuration tasks to optimize the service. This chapter describes the following tasks:

- Configuring Microsoft Office permissions to deal with a change in the way Windows handles permissions, which may cause errors when printing Microsoft Office documents.
- Reconfiguring the Print Anywhere Server for newly installed applications that were installed after the PrinterOn software was installed.
- Configuring region-specific encoding for text files for environments where text files of non-ASCII encoding (such as Chinese or Korean) are commonly submitted for printing.
- Enabling PrintAnywhere to permit print jobs from a remote CPS server, when PrintAnywhere and CPS are located on different servers.
- Disabling strict SSL verification for CPS, when man-in-the-middle proxies prevents communication with the PrinterOn Directory.
- Enabling LDAP/AD for PrintWhere, to allow PrintWhere to use LDAP/AD authentication.

N.1 Configuring Microsoft Office permissions

Some users have reported errors printing some Microsoft Office files when deploying PrinterOn Server along with Microsoft Office. This issue is caused by a change in Windows

permissions, which impacts automation to some installations of Windows Server 2012 and Server 2008.

At present, the only workaround to this issue is to manually modify the DCOM configuration for Microsoft Office applications. PrinterOn is working toward a solution that will remove the need to perform these manual steps in an upcoming service release.

To modify the DCOM configuration:

1. From the command prompt, type `mmc -32` to launch the Console.

2. Expand **Component Services**, then select **DCOM Config**.

3. Perform the Steps 4 to 6 for each of the following entries:

   > **Note:**
   >
   > - The version information below is correct, even if a later version is installed.
   >
   > - Not all options will be available for all installations.

   - Microsoft Word 97 -2003 Document
   - Microsoft Excel 97 -2003 Document
   - Microsoft PowerPoint 97 -2003 Document
   - Microsoft PowerPoint Slide
   - Microsoft Visio 97 -2003 Document (if installed)

4. Right-click and select **Properties**, then click the **Identity** tab.

5. Select **This User**, and enter the same dedicated Local Administrator user that was created to run the PrinterOn Services.

6. Click **Apply**.

7. Restart the Processing Server service:

   a) In the Configuration Manager, click **Home** > **Services**.

   b) Locate the **Print Anywhere Processing Server**, then click the adjacent **Restart** button.

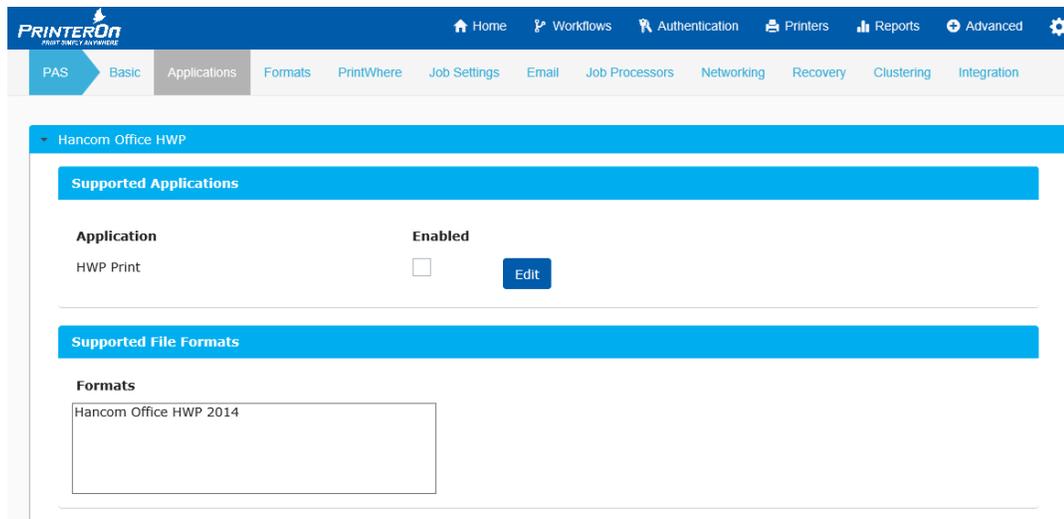## N.2 Reconfiguring the Print Anywhere Server for newly installed applications

The Application tab in the Print Anywhere configuration settings allow you to review and manage the applications available to the server. The PrintAnywhere Server can scan your

server to determine which applications have been installed and whether they can be used by the server to process print jobs.

If you have installed applications, such as LibreOffice or Microsoft Office, after installing the PrinterOn Server, you must refresh the server application configuration to use the newly installed applications

To refresh the application settings:

1. In the Configuration Manager, click **Advanced** > **Components**.
2. Click the **Configure** button adjacent the **Print Anywhere Server** component. The Print Anywhere Server (PAS) component configuration appears.
3. Click **Applications**.

4. At the bottom of the page, click **Auto Configure Settings**.

5. When the auto configuration is complete, restart the Processing Server service:
   a) In the Configuration Manager, click **Home** > **Services**.
   b) Locate the **Print Anywhere Processing Server**, then click the adjacent **Restart** button.

N.3 Configuring region-specific encoding for text files

> **Note:** These options only apply if you have Word or LibreOffice installed.

If users of your service regularly print simple text (TXT) files to your server, depending on your location, you may be able to improve the output of the text files with some additional configuration.

By default, the PrinterOn Server processes text files with a simple ASCII encoding. When a text file is submitted for printing, the server attempts to determine the encoding of file to select the best encoding automatically, such as UTF-8, ASCII, or UTF-16.

In some cases, the server cannot determine the encoding of a text file. You can specify a default encoding that the server uses for those cases when it cannot determine the encoding.

You should configure the default encoding if:

- Users regularly print text files.
- Users regularly submit text files other than ASCII or UTF-8, such as Korean or Japanese.
- The type of text file submitted is consistent across users.

> **Note:** Although setting the default encoding to a value such as Korean or Chinese allows the server to process jobs with that encoding, it may cause jobs with other encodings to produce unexpected output.

To set the default encoding:

1. In the Configuration Manager, click **Advanced** > **Components**.
2. Click the **Configure** button adjacent the **Print Anywhere Server** component. The Print Anywhere Server (PAS) component configuration appears.

3. Click **Formats**.
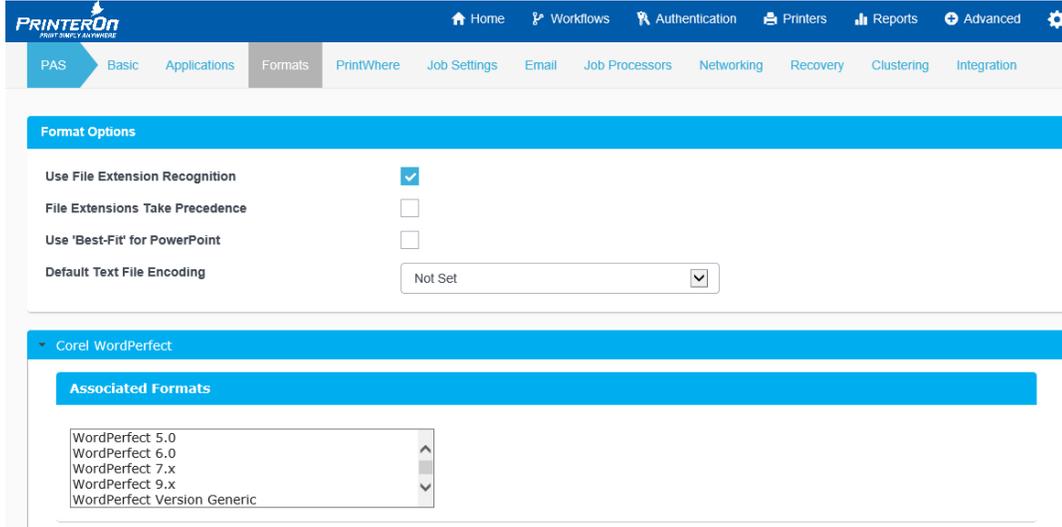
4. In the **Format Options** panel, select the desired language encoding from the **Default Text File Encoding** drop-down.

5. Restart the Processing Server service:

    a) In the Configuration Manager, click **Home** > **Services**.

    b) Locate the **Print Anywhere Processing Server**, then click the adjacent **Restart** button.

N.4 Enabling PrintAnywhere to permit print jobs from a remote CPS server

If you have a PrinterOn deployment in which the PrintAnywhere Server and the CPS are on different servers, you need to modify Apache Tomcat to allow PrintAnywhere to accept requests from the CPS server.

To allow PrintAnywhere to receive jobs from a remote CPS server:

1. From the server hosting PrinterOn, stop the CPS Apache Tomcat service.

2. Navigate to C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\Conf.

3. Open the server.xml file in any text editor.

4. Locate the following section:

```
<Context path="/PasServlet">

<Valve className="org.apache.catalina.valves.RemoteAddrValve"
            allow="127\.0\.0\.1"/>
```

```
    </Context>
```
The `allow` parameter specifies the IP address of the server(s) from which Tomcat accepts requests.

5. Modify the value of the `allow` parameter to the IP address of the server hosting CPS. For example:

    ```
    allow="172\.16\.39\.52" OR allow="172.16.39.52"
    ```

    > **Note:** If you have enabled email printing, or you have multiple CPS servers, you can enter multiple IP addresses by separating with a pipe character (|). For example:
    >
    > ```
    > allow="127.0.0.1|172.16.39.52"
    > ```

6. Save the changes to server.xml.
7. Start the Apache Tomcat service.

N.5 Disabling strict SSL verification for CPS

In some cases, certain networks do not allow communication to the PrinterOn Directory, due to services such as Man in the Middle proxies. In those cases, there may be a need to disable SSL verification.

There is no configuration option to disable this setting in the Configuration Manager. You must manually edit the CPS configuration file.

To disable strict SSL verification:

1. Browse to the following folder:

    C:\Program Files\PrinterOn Corporation\Apache Tomcat\Conf

2. Open CPS_Config.xml in any text editor.
3. Locate the following entry:

    ```
    <enableSSLVerify>true</enableSSLVerify>
    ```

4. Modify the value to:

    ```
    <enableSSLVerify>false</enableSSLVerify>
    ```

5. Save the changes to CPS_Config.xml.
6. Restart Tomcat.

N.6 Enabling LDAP/AD for PrintWhere

To enable LDAP/AD for PrintWhere:

1. Log in to the PrinterOn.com web admin portal at www.printeron.com/administrators.

2. Click the **Printers** icon and locate the printer you'd like to enable authentication for.

3. Select the **Payment & Authorization** tab.

4. In the **Authorizing Users** section, select **Redirect to authorize user, track pages or bill customer**.

5. Check **User Authentication URL**, then enter the pathname of the server hosting the PrinterOn CPS Admin application. For example:

    192.168.1.20/cps/aaaLogin.jsp.

6. Save your settings and test the driver.

Trademarks and service marks

The following are trademarks or registered trademarks of ePRINTit USA, LLC. under License:

PrinterOn®, PrintAnywhere®, Print Simply Anywhere®, PrintWhere®, PRINTSPOTS®, the PrinterOn Logo, the PrinterOn Symbol, PrintConnect™, Secure Release Anywhere™, and PrintValet™ are trademarks and/or registered trademarks of PrinterOn.

The following are trademarks or registered trademarks of other companies:

Windows, Internet Explorer, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and Microsoft Visio are trademarks or registered trademarks of Microsoft Corporation.

iPad, iPhone, AirPrint, and macOS are trademarks or registered trademarks of Apple.

iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple under license.

Android, Chrome OS, and Chromebook are trademarks or registered trademarks of Google Inc.

BlackBerry is a registered trademark of BlackBerry, Ltd.

Other brands and their products are trademarks or registered trademarks of their respective holders.

Copyright notice

Version 4.3.9 | February 16, 2022