WATCHDOC

INSTALLATION AND INITIAL CONFIGURATION MANUAL

Ricoh WES - Smart Operation Panel - 2.5 generation

DOXENSE Print, breathe !

47, avenue de Flandre - 59290 Wasqhehal - France
65, rue de la Tombe Issoire - 75014 Paris - France

T +33 (0)3 62 21 14 00
www.doxense.com

Table of contents

Copyrights

47, avenue de Flandre
59290 Wasquehal - FRANCE
contact@doxense.com

Tel : +33(0)3.62.21.14.00
Fax : +33(0)3.62.21.14.01
www.doxense.com

Introduction

Purpose of the manual

This manual describes the procedure for installing WES v3 (Watchdoc Embedded Solution) on RICOH SOP Gen. 2 and 2.5 devices.

Intended audience

This manual is intended to be used by technicians responsible for installing the WES on Watchdoc v6.x. Such technicians must have information on the print server, the Watchdoc hosting server, as well as the properties of the device.

Symbols used

The terms followed by an asterisk * are defined in the glossary.

> Information: reports important information required to fine tune the installation or configuration of the solution or information that may be useful for a better understanding or knowledge of a notion or a function of the tool, or provides a specific case of use of this tool.Contact Doxense®

Doxense's technical assistance service is reserved for certified, technical partners and can be contacted via Connect, customer portal dedicated to partners.

WATCHDOC Certified Partner

For all other questions, please contact your Doxense® consultant or send us an email at contact@doxense.com

Versions

Date	Description
01/2025	Update of the manual installation procedure
10/2024	Update of the document formatting
09/2024	Update of the installation prerequisites and the installation procedure
12/2023	Addition of an information relative to the Java working environment for the operation of Ricoh WESDeployer
10/2020	Update of the available devices list
05/2020	Add of the "Renewal of the Access Token before expiration part" in the Troubleshooting chapter.
03/2020	Add of prerequisites SPModes configuration
05/2017	Addition of the Authentication Method and Print Job Release Mode parts.
03/2017	UpDate of the screenshot.
02/2017	New graphical version, adding device prerequisites, adding Organisational Requirements
09/2016	First version.

Prerequisites and prior configuration

Configure ports

The network ports to open are the following:

Source	Port	Protocol	Target
Watchdoc	TCP 80 TCP 443	HTTP HPPS	Printing device

Configure the cards reader

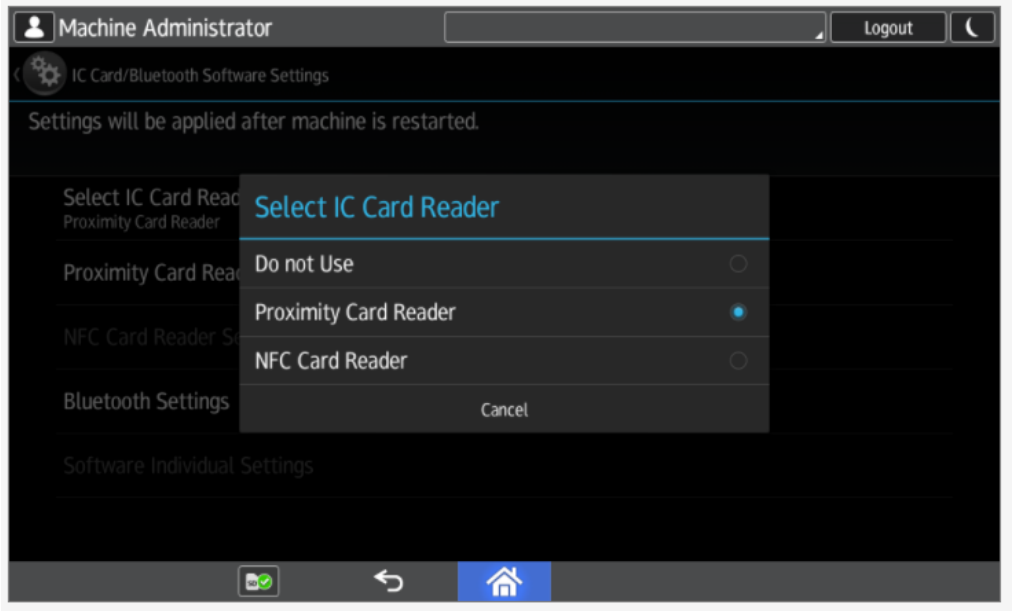
Principle

If users authenticate using a card, it is necessary to install and configure the cards reader before installing the Ricoh SOP Gen2 WES.
Ricoh® printing devices have a generic plug-in installed by default that can handle most cards readers, including the Elatec® brand cards readers that Watchdoc has been tested with. Consequently, in the most common installations, it is not necessary to install the Elatec® plugin.

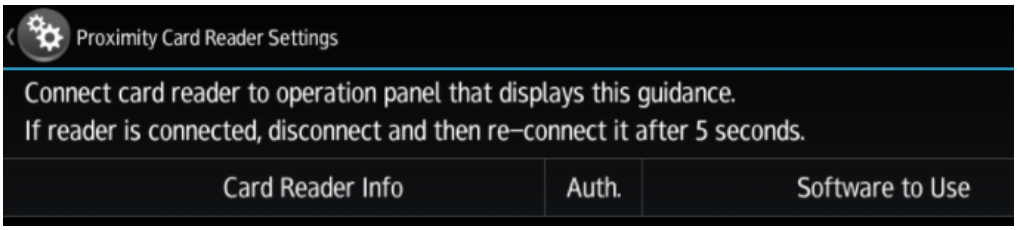
Procedure

To configure the cards reader:

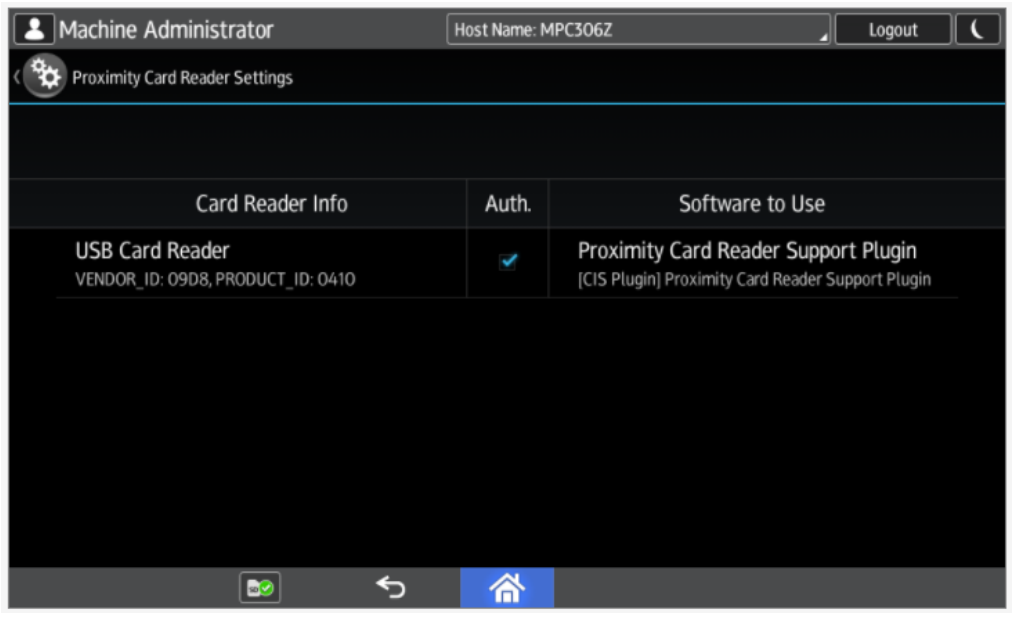
1. connect the card reader to the device;
2. from the printing device panek, click on **User Tools;**
3. then click on **Screen Features > Screen Device Settings > IC Card/Bluetooth Software settings** or **External Device Setting** for the gen 2.5 printing devices);
4. in **Select IC Card Reader,** choose **Proximity Card Reader Support Plugin** ;



5. follow the instructions on the screen:



6. when the badge reader is detected, click on the corresponding line to select the software associated with its use(**Proximity Card Reader Support Plugin**) ;



7. after configuring the badge reader, restart the printing device.

Configure the SP modes

Principle

To enable the WES to operate, certain SP Mode settings need to be changed. This modification is made from the device and requires authentication as an administrator. Only technicians authorised by Ricoh® and who have the access procedure are authorised to make these settings.

Configure the 5-113-002 SP Mode

This parameter is used to customise SDK/J authentication (OPTIONAL_COUNTER_TYPE__EXTERNAL_OPTIONAL_COUNTER_TYPE).

1. in the **SP Mode (Service)** interface, enter the code for the SP mode to be modified: 5-113-002-;
2. Expansion device: replace the existing value with **0**.

Configure the 5-401-230 SP Mode

This parameter authorises personalised user authentication:

1. access the SP Mode interface by following the specific procedure provided by Ricoh® ;
2. in the SP Mode (Service) interface, enter the code for the SP mode to be modified: **5-401-230** ;
3. the default value is 00000000. Replace the last digit of this value with 1 (**00000001**);
4. press the pound (**#**) button to confirm the new value and exit the interface;

> This configuration must be finalised in the device management web interface (see Installing the WES manually).

Configure the 5-401-240 SP Mode

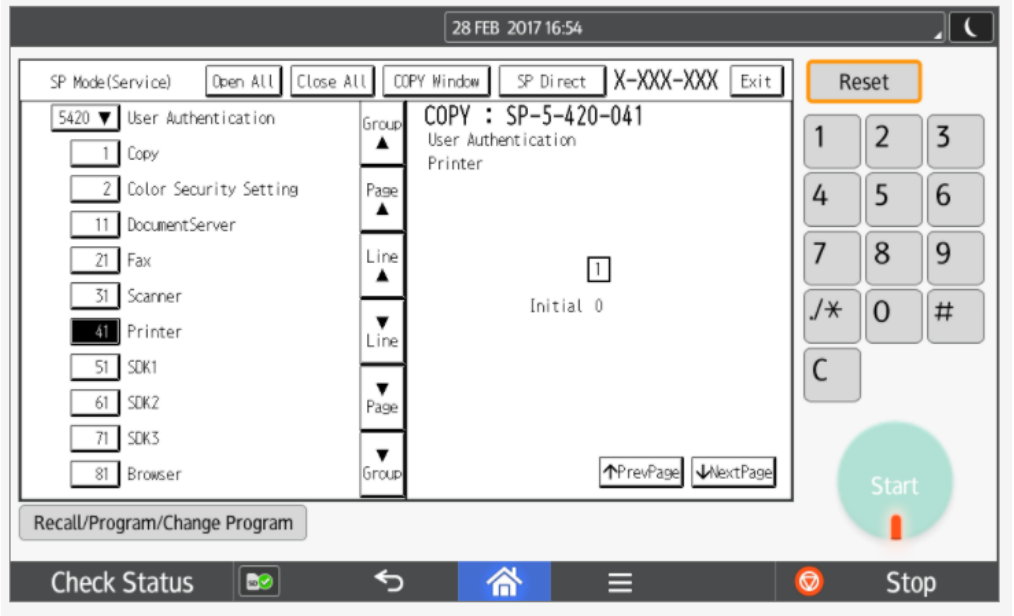
This parameter authorises management of Watchdoc security profiles (ACL).

1. From the SP Mode (Service) interface, use the numeric keypad to enter the code for the SP mode to be modified: **5-401-240** ;
2. by default, the parameter value is 0000
3. replace with the value 1000.

Configure the 5-420-041SP Mode

This parameter disables authentication for device functions:

1. from the SP Mode (Service) interface, use the numeric keypad to enter the SP mode code to be modified: **5-420-041** ;
2. by default, the **Printer Authentication** parameter is set to **ON(0)** ;
3. enter **OFF(1)** to change the default value.

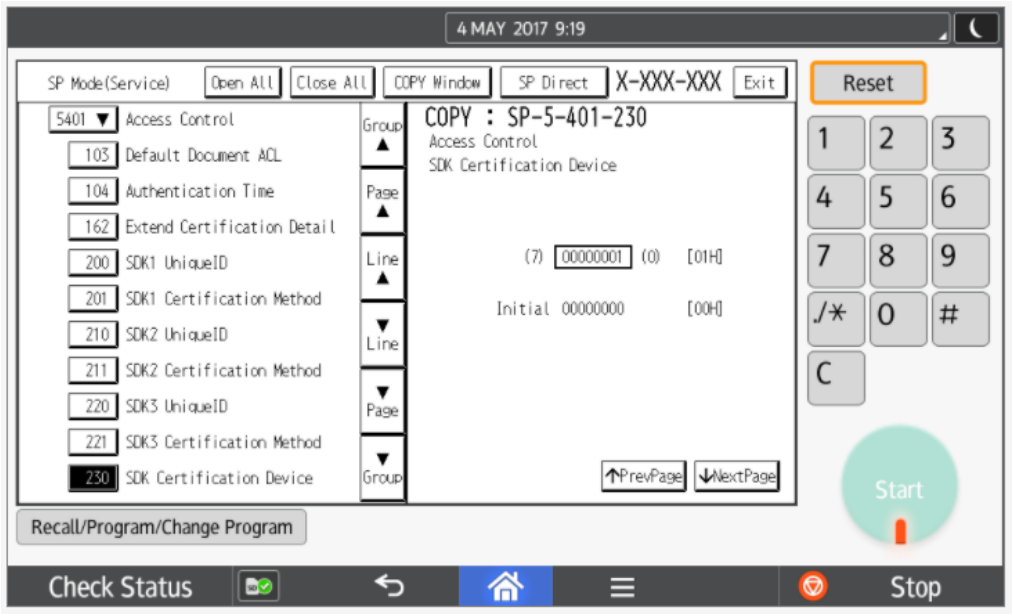


4. confirm the parameter by clicking on the hash key **#** on the numeric keypad.

Configure the 5-490-001 SP Mode

This parameter authorises printing on the server:

1. from the SP Mode (Service) interface, use the numeric keypad to enter the SP mode code to be modified: **5-490-001** ;
2. the value of the **Job Permit Settings** parameter is set to **Not allowed (0)** by default;
3. enter the value **Allowed (1)** to change the default value and allow print jobs.



4. confirm the setting by clicking the hash key # on the numeric keypad.

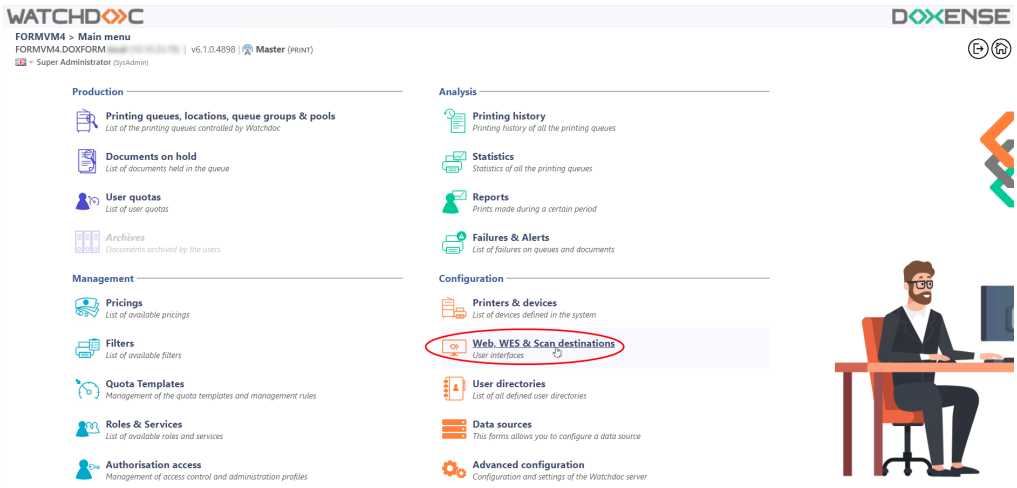
➔ With this setting, print jobs are executed with the default user name 99999999

Configure the WES profile

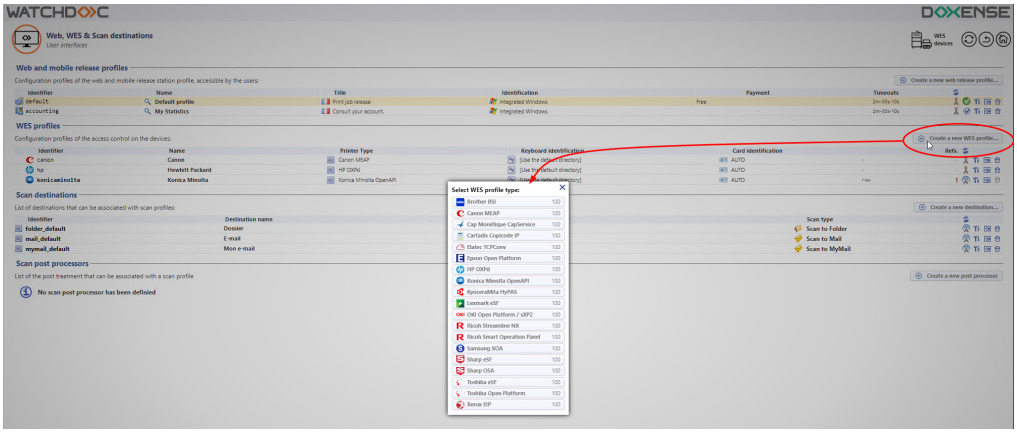
Create the WES profile

On a clean Watchdoc installation, a first WES profile is automatically created with default parameters at the end of the wizard procedure, but you can, at any time, edit existing profiles to modify them or create a new profile.

1. From the **Main menu** in the administration interface;
2. in the **Configuration** section, click on **Web, WES & Scan destinations**:



3. in the **Web, WES & Scan Destinations - Client Interface Management** interface, click on **Create a new WES profile**;
4. in the list, select the profile you want to create:



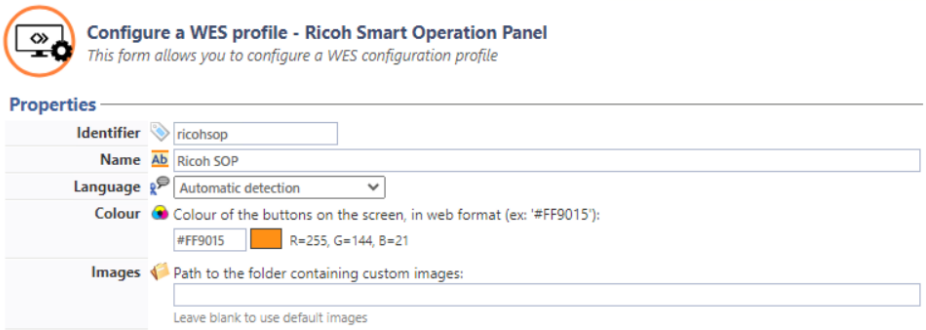
➔ you will access the **Create a WES profile** form, which contains a number of sections in which you can configure your WES.

Configure the Ricoh WES profile

Configure the Properties section

Use this section to state the main WES properties:

- **Identifier:** Enter the single identifier for the WES profile. It can comprise letters, numbers and the '_' character with a maximum of 64 characters. This identifier is only displayed in the administration interfaces.
- **Name:** Enter the WES profile name. This explicit name is only displayed in the administration interfaces.
- **Global:** In the case of a domain configuration (master/slaves), tick this box to replicate this profile on the slave servers.
- **Language:** Select the WES display language configured from the list. If you select Automatic detection, the WES adopts the language it finds by default in the device configuration.
- **Version:** Select the version of WES. For v3, you can customise the interface by choosing the colour of the buttons and images to match your graphic identity:
  - **Colour:** enter the Hexadecimal color value corresponding to the WES button's colour. By default, the buttons are Watchdoc orange customized (#FF901). Once the value is entered, the colour is displayed in the field.
  - **Images:** if you want to customize the WES images, enter the folder path in which are recorded images you want to display instead of the default images (stored in C:\Program Files\Doxense\Watchdoc\Images\Embedded\Doxense\[Manufacturer_Name] by default).
    see Customize the WES.

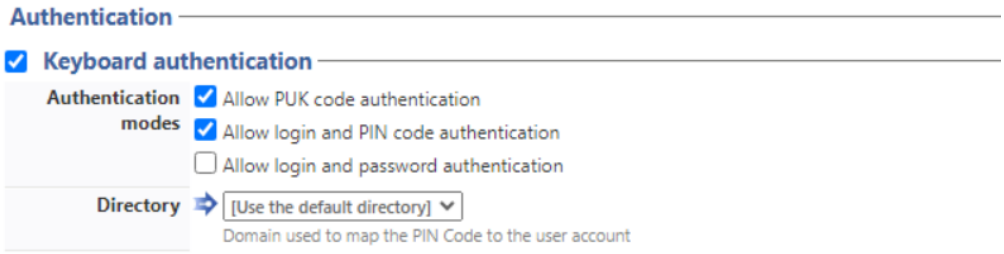


Configure the Keyboard authentication section

- **Keyboard authentication:** tick the box (at the section level) to enable user authentication from a physical keyboard or the touch screen one, then set out how this authentication works:

- **PUK[1] Code:** the PUK code is automatically generated by Watchdoc according to the parameters defined in the directory and communicated to the user on the "My account" page.
- **Login and PIN Code:** consisting of 4 or 5 digits, the user PIN code (1234, for example) is registered as anLDAP attribute or in a CSV file. It is associated to the user login (available with the Watchdoc 5.1 version).
- **Login and password:** users will use their LDAP credentials. We do not recommend using this mode :**Directory:**

- **Directory**: From the list, select the directory to query during keyboard authentication. If no directory is set, Watchdoc will query the default directory.



Configure the Card authentication section

- **Card authentication:** tick the box (at the section level) to enable user authentication from a card, then set out how this authentication works:
  - **Directory:** From the list, select the directory to query during cards authentication. If no directory is set, Watchdoc will query the default directory.
  - **Self registration :** If you enable the **self-registration**[2] from the WES, state how the user assigns their card to their account:
    - **with PUK code:** the embedded solution will ask the user for its PUK code. If the PUK code is correct, Watchdoc stores the card number with the user's login in its database;
    - **with login and PIN code:** the embedded solution will ask the user for his login and his PIN cpde.
    - **with login and password:** the embedded solution will ask the user for his login and his password. If the data keyed in are correct,

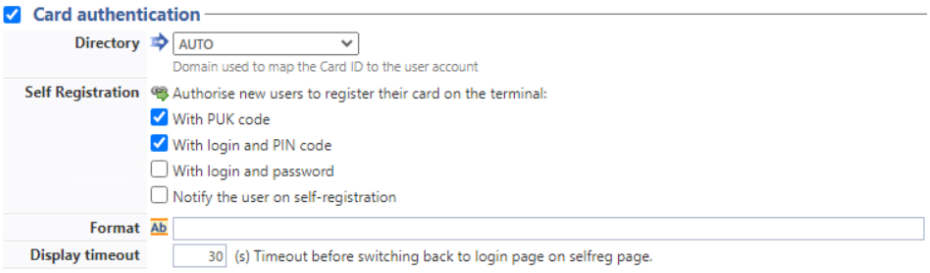
---

[1](Print User Key). In Watchdoc, this is a code associated with a user account to allow the user to authenticate in a WES. The PUK code is generated thanks to an algorithm. The user can consult it in the "My account" page of Watchdoc.
[2]An action in which a user account is associated with its own card code. Registration is carried out the first time a card is used. The registration can be carried out by the IT manager when he issues the card to a user or by the user himself who enters his identifier (PIN code, PUK code or username and password) which is then associated with his card code. Once the registration is completed, the card code is permanently associated with its owner.

Watchdoc stores the card number with the user's login in its database.

- **Notify the user on self-registration:** check this box to send a notification to the user when his badge has been enrolled.

- **Format :** State, where necessary, how the character string for the badge number string is to be transformed. E.g. raw;cut(0,8);swap.
  Specificity of the **Format** parameter: typically, when the code PUK is stored in an attribute of the LDAP directory, it is encoded for security reasons. Obtaining the code corresponding to that of the badge therefore requires a transformation of the format read by the badge reader. If you have a problem setting this parameter, contact Doxense Support.
- **Display timeout:** indicate, in seconds, the time to wait before a second badge swipe is taken into account (5s < Time < 15s)



Configure the Anonymous connection section

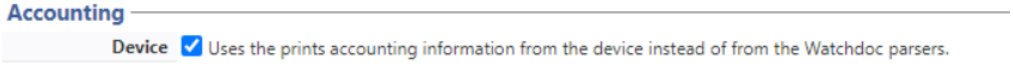
Check this section to enable anonymous login to allow a non-authenticated user to access the device by clicking on a specific button.
You can restrict the functionality that the anonymous user can access by applying a rights policy to the queue, group or server and using the Anonymous User filter.

- **Button label**: in this field, enter the label displayed on the device functions access button. The default text is Anonymous:

Configure the Accounting section

In this section, specify whether you want accounting to be performed by the device itself or from the Windows spooler.

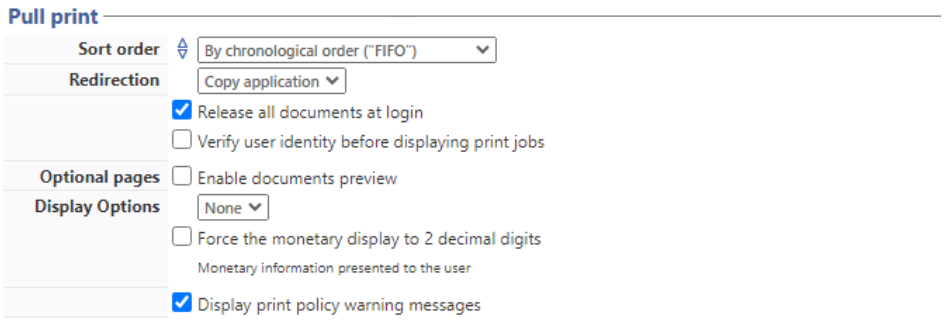
- **Device**: Uses the prints accounting: tick this box if you want accounting to be handled by the device. In this case, specify the accounting mode:



Configure the Pull-print section

In this section, you specify the parameters relating to the print-on-demand function, i.e. the interface from which the user accesses his pending jobs and from which he deletes or validates print-jobs:

- **Sort Order**: in the list, select the order in which the printouts should be presented on the WES :
  - **by reverse chronological:** from most recent to oldest;
  - **Chronological:** from oldest to most recent.
- **Redirection:** specify the behaviour of the WES when the user logs on, and in particular the redirection to a page other than the home page:
  - **Smart:** the WES displays the default home interface if the user has no pending documents; on the other hand, if the user has pending documents, the WES displays the list of documents;
  - **Waiting jobs:** the WES displays the list of pending documents even if there are none.
  - **Home:** the WES displays the default home interface and does not redirect to any other interface;
  - **Copy application:** the WES displays the copy interface and does not redirect to any other interface;
- **Release all documents at login:** tick the box to ensure that all queued jobs are automatically printed when the user logs on to the print device. In this case, the user does not access the list of queued jobs to validate which ones to print.
- **Verify user identity before displaying print jobs:** tick the box to the user is required to authenticate before accessing the list of his or her jobs.
- **Optionnal pages:**
  - **Enable documents preview:** tick this box so that the user can preview pending jobs before confirming printing.
- **Display Options**: In the list, select the monetary information presented to the user via the WES: none, the price or the cost of their prints.
  - **Force the monetary display to 2 decimal digits:**
  - **Display print policy warning messages**: tick the box to limit the number of decimal places displayed to the user in the tariff information.

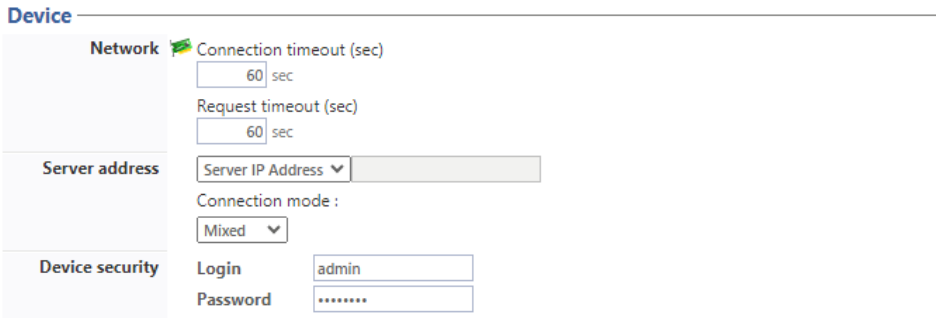


Configure the Device section

This section is used to define the connection mode between the server and the print devices.

- **Network:** the two values can be used to set :
  - **Connection timeout:** the maximum waiting time for the connection between the copier and Watchdoc during a request (server off or service stopped);
  - **Request timeout:** the waiting time for processing the request: retrieving information about a user, sending and processing accounting requests.

- **Server Address type:** The device needs to contact the Watchdoc server when the user tries to connect or wants to release his documents. You can specify the Watchdoc server address in three different ways: IP Address, DNS Address and Custom Address ;
- **Connection mode:** select the connection mode between the WES and the Watchdoc service:
  - **Mixed:**the WES adapts automatically according to the data communicated: it uses SSL for sensitive data (PUK code, login/mdp, etc.) and non-SSL for non-sensitive data;
  - **SSL:** the WES always uses SSL to communicate with the server. N.B.: activating SSL can cause slowness or alerts in the event of unrecognised certificates.
  - **No-SSL:** the WES never uses SSL to communicate with the Watchdoc service.N.B.: when SSL is deactivated, it is recommended not to use the connection or automatic association of the badge (enrolment) by account and password.
- **Device security:** specify the connection parameters that allow Watchdoc to communicate with the device:
  - **Account:** enter the administrator account and password;
  - **Password:** enter the password for the device administrator account;



Failover options section

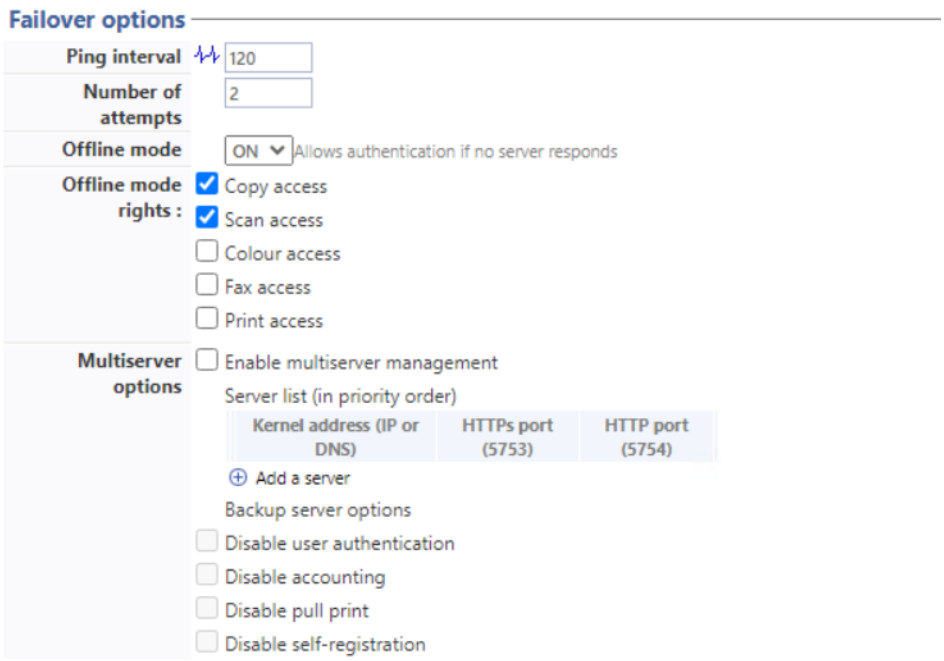
In this section, you configure the behaviour of the print devices in the event that the Watchdoc server does not respond.

- **Ping interval:** specify, in seconds, the frequency with which the device polls the server to check its configuration and inform it that it is operating correctly;
- **Number of attempts:** specify the number of connections the device should attempt to the main server before switching to the standby server.
- **Offline mode:** activate or deactivate **offline mode**[1] and complete the list by indicating the authorised functions if the server is off:

[1]Mode enabling the print device to operate in a degraded manner in the event of the print servers (main and backup) failing. In offline mode, printing is impossible, but the device's other functions can be offered: photocopying, faxing and scanning. If offline mode is disabled, in the event of a server failure, all device functions are blocked until the server is repaired. This mode is configured in the WES profile applied to the device.

- **Copy access:** Tick this box to enable the user to copy;
- **Scan access:** Tick this box to enable the user to scan;
- **Color access:** Tick this box to enable the user to print in color;
- **Fax access:** Tick this box to enable the user to send documents by fax;
- **Print access:** Tick this box to enable the user to print documents.

- **Multiserver options:** tick this box to relay requests to a backup server in the event of failure of the server with which the WES is associated, then enter the information required to access it in the table: backup server address; https port; http port.
  Then check the functions provided by the backup server:
  - **Disable user authentication:** tick this box if the rescue server does not authenticate users. For each request, it returns the details of an anonymous user with the rights defined for an anonymous user on the main server. The work carried out is then recorded under the "anonymous" account;
  - **Disable accounting:** If this is checked the accounting elements will be held on the device until it reconnects to the primary server. This is useful if you wish the accounting to be all sent to the same sever (if the databases are not common for example)
  - **Disable pull print:** With this option, the print on demand application will be disabled. This is useful because if the backup server has no access to the jobs of the user.
  - **Disable self-registration:** With this option, the self-registration will not be available on the backup server. This is useful if the cards database are not the same for both servers.



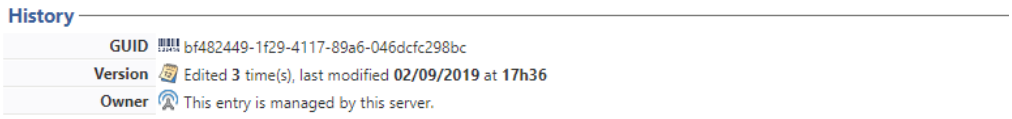
Configure the Misc. section

In this section, configure how and where the log files should be stored in the event of a of a malfunction between the WES and the server.

- **Log options - Destination:** Specify where the application should collect the information:
  - **file**: Tick this box so that the information is saved in a file accessible by Watchdoc;
  - **device**: Tick this box so that the information is saved on the device;
  - **all** : Check this box to have the information saved in a file accessible by Watchdoc and on the device.
- **Log options - Level:** indicate the level of detail of the information recorded:
  - **debug:** Option to keep track of WES malfunctions;
  - **verbose:** All detailed traces left by the WES;
  - **info:** Traces left by the WES;
  - **warning:** Traces left by the WES when there is a default;
  - **error:** Traces left when an error is detected at the WES.
  - **fatal:** Traces of faults detected on the WES
  - **none:** No trace

History section

This section displays information on the configured WES and on modifications made to it :



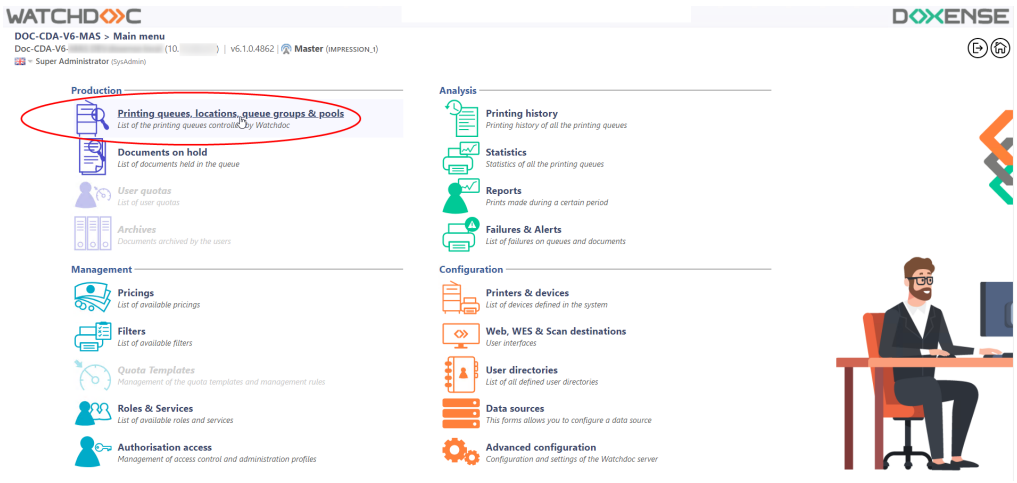
Validate the profile

1. Click the button  to validate the WES profile configuration.
→ Once validated, the WES profile can be applied to a print queue.

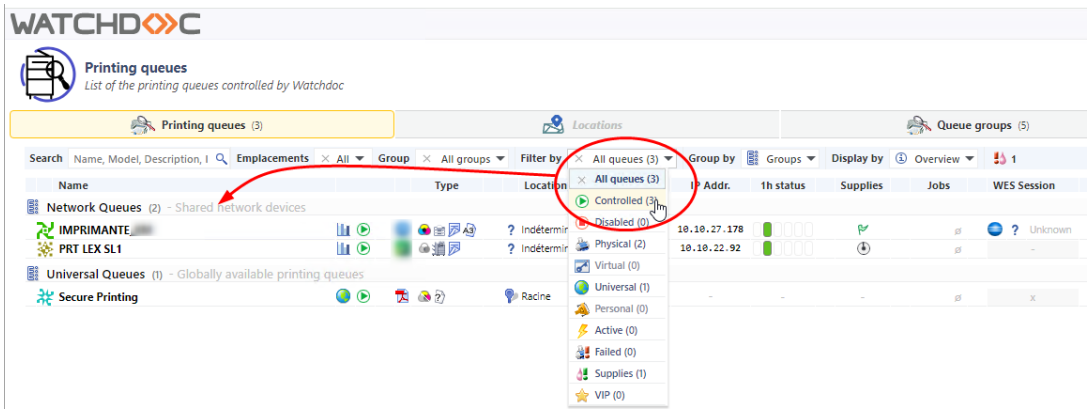
Configure the WES onto the queue

Access the interface

1. From the **Main Menu** of the Watchdoc administration interface, in the **Production** section, click **Print Queues, Queue Groups & Pools:**



→ This takes you to the print queues interface. In this queue, activate the **Controlled** filter, then select the queue you want to configure:



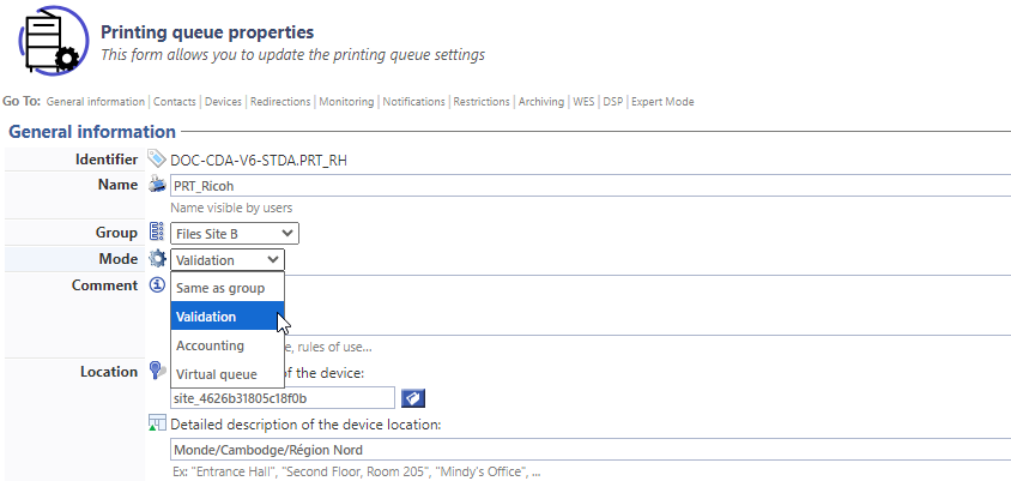
2. For this queue, click the **Edit Queue Properties button** at the end of the line.

➔You are taken to the **Print Queue Properties** interface in which several sections are displayed. WES properties are managed in the **WES** section.

Configure the print queue mode

In the Print Queue Properties interface, General Information section, select the operating mode for the queue:

- **Mode:** select **Validation** to have users validate queued jobs so that they are actually printed. If the queue belongs to a group configured in Validation mode, you can also select **Same as Group.**

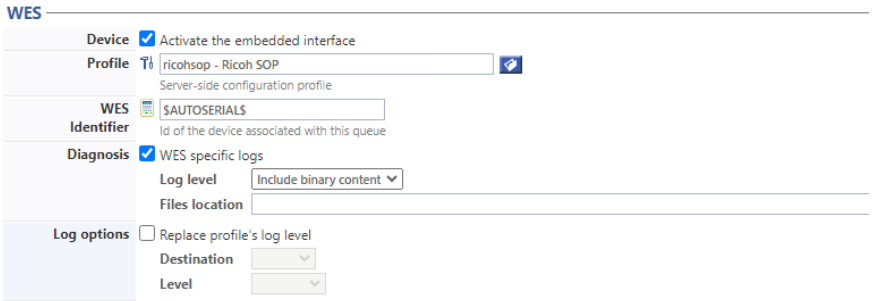


Configure the WES onto the queue

In the Print Queue Properties interface, click on **WES** to access the dedicated section.

- **Device - Activate embedded interface:** tick the box to use a WES.
- **Profile subsection:** From the list, select the WES to configure. The list comprises profiles created ahead of time in your instance of Watchdoc. If the desired profile is not found there, you will need to configure it (see Configure a WES article).
- **WES identifier subsection:** Once you have ticked the box and selected the profile, the ID of the WES field will fill itself with “$AUTOSERIAL$”. Keep it that way so that the server will determine itself the serial number of the device and use it as the WES ID. You can also input directly the serial number of the device in this field.
- **Diagnosis subsection:** It may be useful to activate WES trace logging, especially to diagnose an anomaly. Use this subsection to specify settings relating to WES trace log files:
    - **Log level:**From the list, select the type of requests you wish to trace:
        - **Network trace:** Communications between server and WES.
        - **All requests:** Used to keep a trace of all of the requests (to APIs, to RPCs).
          Although all options are possible, we recommend strongly to opt for the activation of **All Requests** so that as much information as possible can be View of the diagnosis. For the sake of performance, the traces must not Be activated only for analytical and diagnostic purposes.
        - **Requests to APIs and RPCs:** Used to retain traces of requests to the API and the RPC requests sent,
        - **API Requests:** Used to retain traces of the requests sent to the

APIs,
    - **None:** Not used.
  - **Files location:** Use this field to enter the path to the folder where you wish to save the trace files. If no path is specified, then by default, Watchdoc saves the trace files to C:\Program Files\Doxense\Watchdoc\logs.
- **Log options - Replace profile's log level:** if the WES trace files on this queue are different from the trace files configured on the WES, specify the parameters below:
  - **Destination:** Specify where the application should collect the information:
    - **file:** Tick this box so that the information is saved in a file accessible by Watchdoc;
    - **device:** Tick this box so that the information is saved on the device;
    - **all :** Check this box to have the information saved in a file accessible by Watchdoc and on the device.
  - **Level**: indicate the level of detail of the information recorded:
    - **profile:**level defined in the WES profile;
    - **debug:** Option to keep track of WES malfunctions;
    - **verbose:** All detailed traces left by the WES;
    - **info:** Traces left by the WES;
    - **warning:** Traces left by the WES when there is a default;
    - **error:** Traces left when an error is detected at the WES;
    - **fatal:** Traces of faults detected on the WES;
    - **none:** No trace.



Validate the configuration

1. Click on ⓥ to validate the WES configuration on the print queue.
2. After having configured the WES onto the queue, you must install it.

> ⓘ After **modifying** a WES profile already installed on a print queue, it is necessary to restart the queue so that it takes account of the profile modifications. To restart a queue, click on the "pause" and then "start" buttons in the queue list.

Install the WES on the queue automatically

Principle

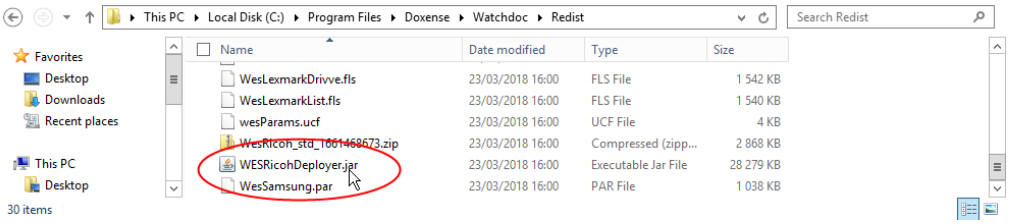
The WES Ricoh Smart Operation Panel is installed using the WESRicohDeployer.jar executable provided by Doxense® as a JAVA archive file (.jar) in the Watchdoc installation package.
This file can be run from the Watchdoc server or from any workstation that can network with the Watchdoc server and target devices. The server or workstation from which the executable is launched must support the Java® 8 min application.
In order for WESRicohDeployer to function correctly, it is necessary to use one of the following versions of the JRE (Java Runtime Environment) (Ricoh restriction):

- Amazon Corretto v8, v11, v17 or v19;
- Liberica v19.

If the installation of WES using the executable fails, you can resort to manual installation, described in the next chapter.

Run the executable

1. Access the Watchdoc server as administrator.
2. Go to the folder C:\Program Files\Doxense\Watchdoc\Redist\
3. Double-click on this **WESRicohDeployer.jar** file;



N.B. :As the Java 8 application on which WESRicohDeployer is based is relatively heavy, you can also install it not on the Watchdoc server, but on a workstation communicating with the server and the devices, from which WESRicohDeployer.jar will be launched:

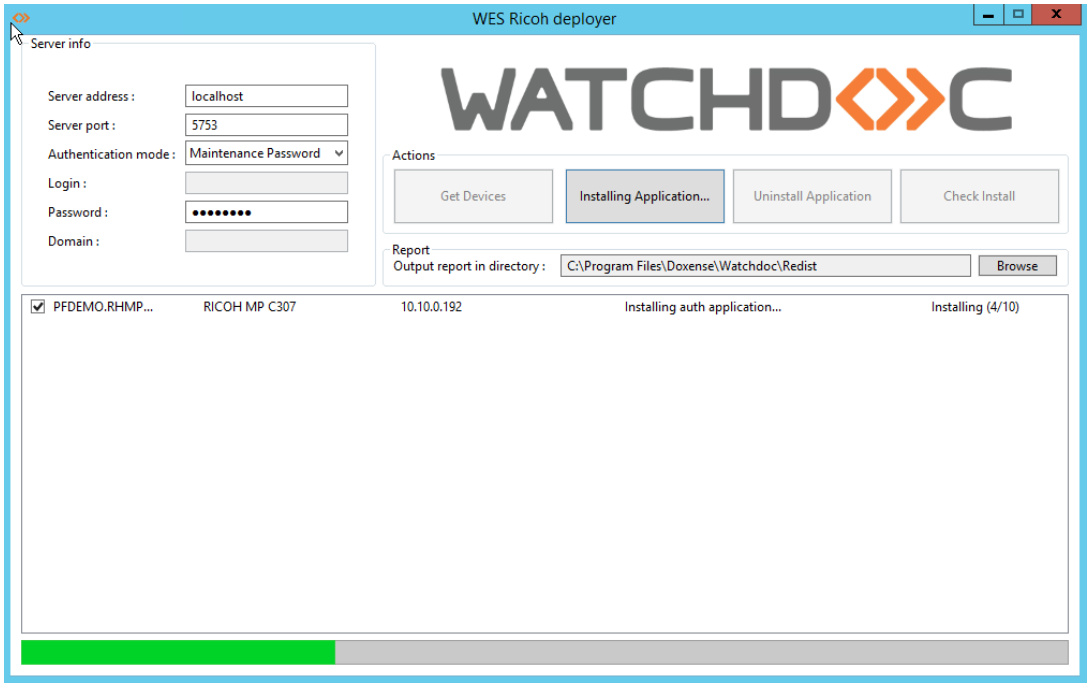
1. Check that the workstation is communicating on the network with the Watchdoc server and with the Ricoh® devices;
2. copy/paste the WESRicohDeployer.jar file on the workstation;
3. double-click on WESRicohDeployer.jar to launch the executable.

The WES Ricoh deployer interface that is displayed consists of 3 parts:

- the Server Info section contains fields relating to the Watchdoc server;
- the Actions section contains buttons to launch installation and uninstallation actions;

- the Report section includes a field in which you can specify the folder in which reports relating to WES installation and uninstallation operations will be saved;

The bottom section (blank at start-up) displays information about the actions launched and a progress cursor:



Configure access to the server

In the **Server Info** section, complete the following fields to identify and locate the server on which the WES is to be installed:

- **Server address**: enter the address (IP address) of the Watchdoc server;
- **Server port**: enter the port used to access the Watchdoc server;
- **Authentication mode** : from the list, select the authentication mode chosen to access the server.
  - **Maintenance Password**: select this mode if you want to access the server using a maintenance account and fill in the Password field.
  - **Login/Password**: select this mode if you wish to access the server using an administration account, then complete the fields relating to this account:
    - **Login**: enter the administration account login ;
    - **Password**: enter the password for the administration account;
    - **Domain**: enter the domain of the administration account.

Install the WES

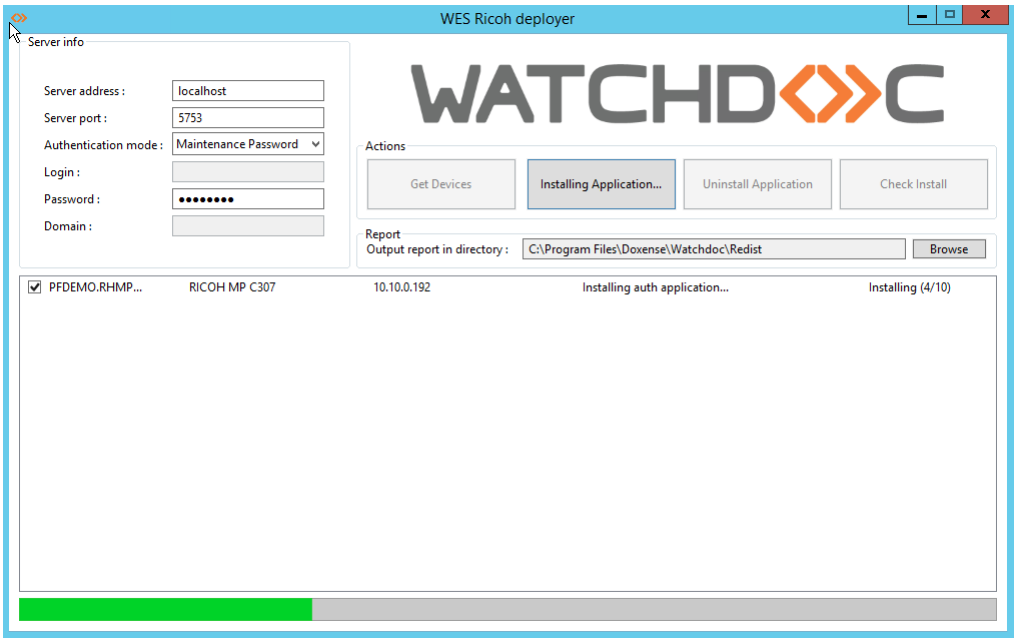
Once you have entered the data for the server

1. in the Actions section, click on the Get Devices button ;

➔in the lower section, all the Ricoh® devices installed on the server are displayed;

2. click on the Install Application button to start the WES installation on the detected devices;

3. a cursor indicates the progress of the operation;

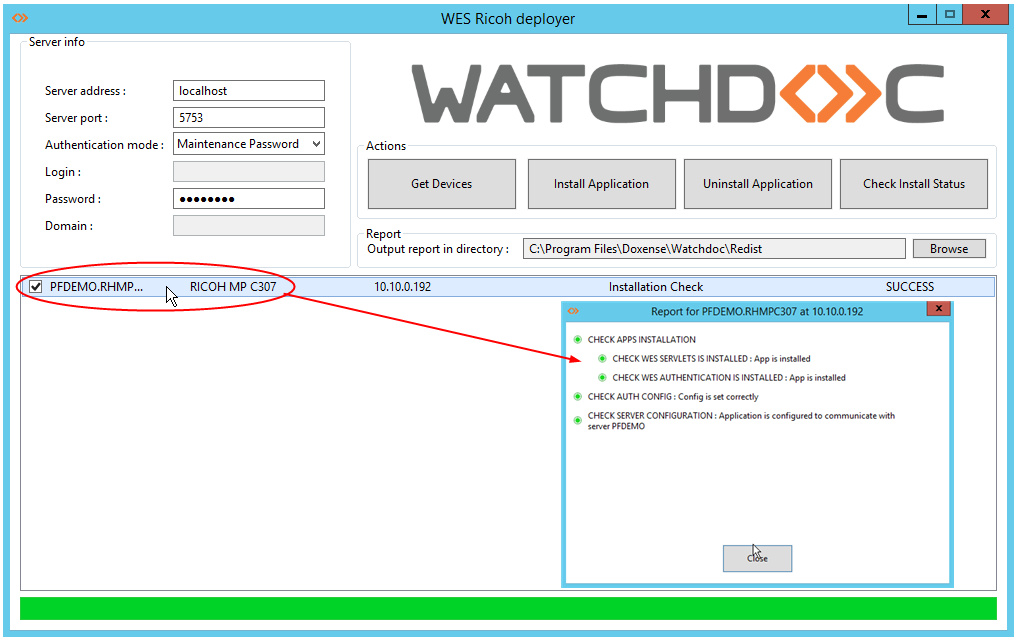


➔At the end of the operation, a message will appear indicating that the installation has been successful on the device(s): You can check that the WES is working on the device(s) by clicking on the **Check install** button.

Check the installation

To check that the WES has been installed on one of the devices:

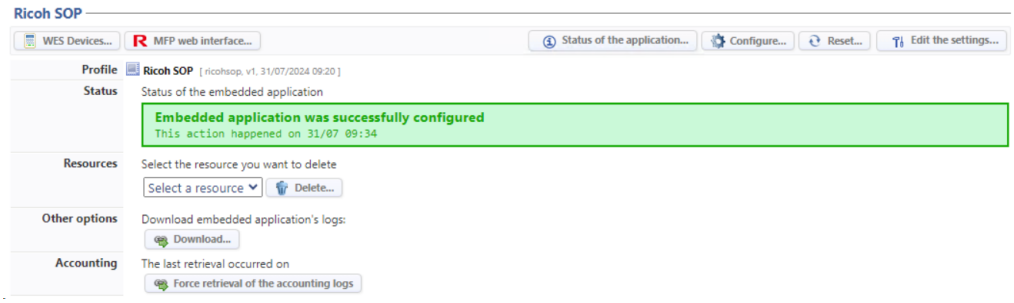
1. in the **Actions** section, click the **Get Devices** button ;
2. in the list of devices, tick the box for the device or devices whose installation you wish to check;
3. click on the **Check install status** button;
4. a message indicates that the check has been completed;
5. click on the line corresponding to the device to access the details:



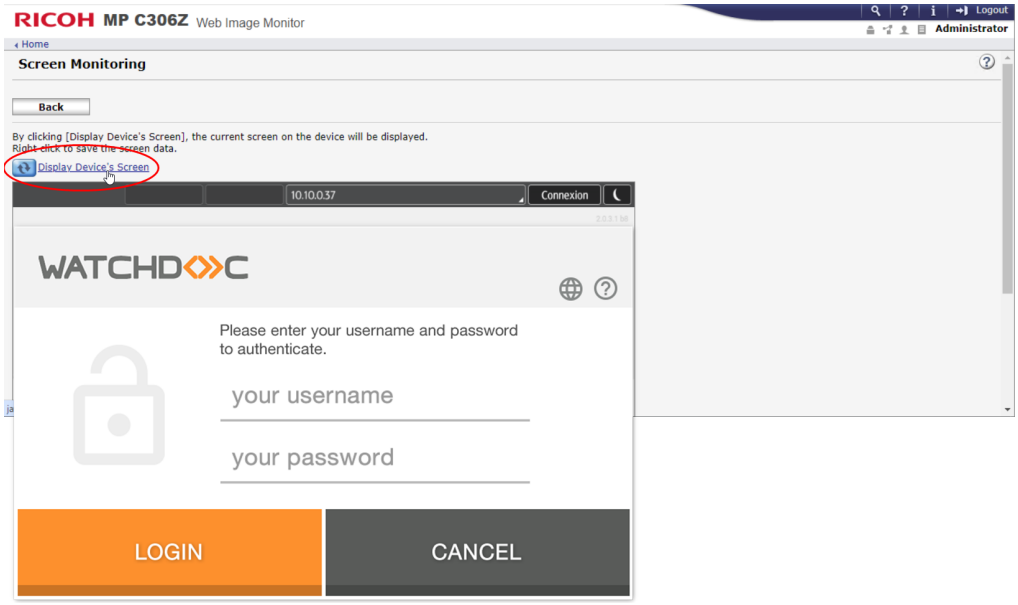
Finalise the installation in Watchdoc

From the Main Menu of the administration interface,

1. in the Operations section, click Print Queues :
2. In the list of queues, click on the queue on which you wish to install the Ricoh WES;
3. in the queue interface, click on the Properties tab;
4. In the WES Ricoh SOP section, click on the **Configure** button to install the application;



5. At the end of the installation, the status of the application is displayed:
6. From the device administration interface, you can use the screen simulator to check that the Watchdoc application is correctly installed:


RICOH MP C306Z Web Image Monitor
Logout
Administrator
Home
Screen Monitoring
Back
By clicking [Display Device's Screen], the current screen on the device will be displayed.
Right-click to save the screen data.
Display Device's Screen
10.10.0.37
Connexion
WATCHDOC
Please enter your username and password to authenticate.
your username
your password
LOGIN
CANCEL

Install the WES manually

Principle

If WES installation using the **WESRicohDeployer.jar** executable fails, you can install WES manually using the procedure described below. Manual installation involves the following steps:

1. activate SSL/TSL communication :
2. install WES from the Ricoh interface;
3. configure administrator authentication.

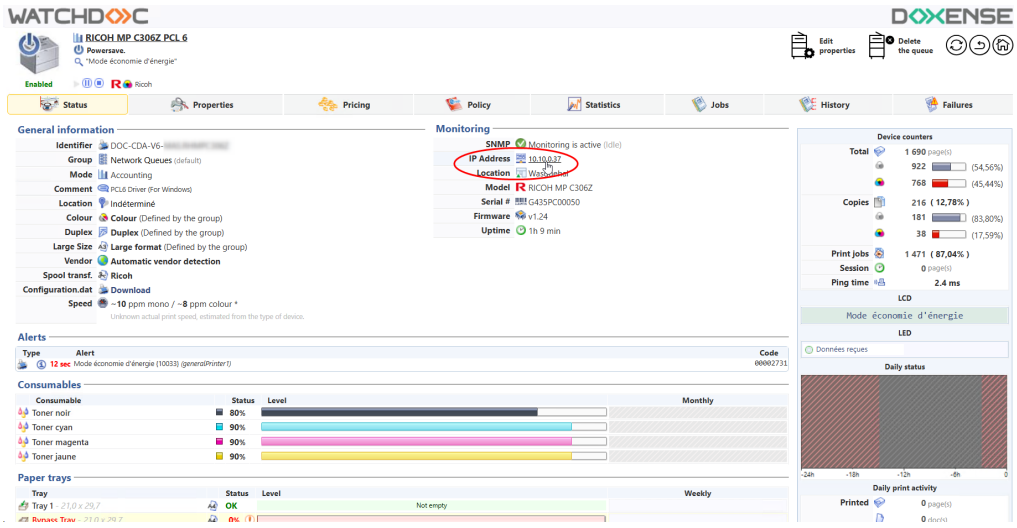
Access the device administration interface

WES is installed manually from **Web Image Monitor**, the Ricoh device administration website. You can access it in two different ways:

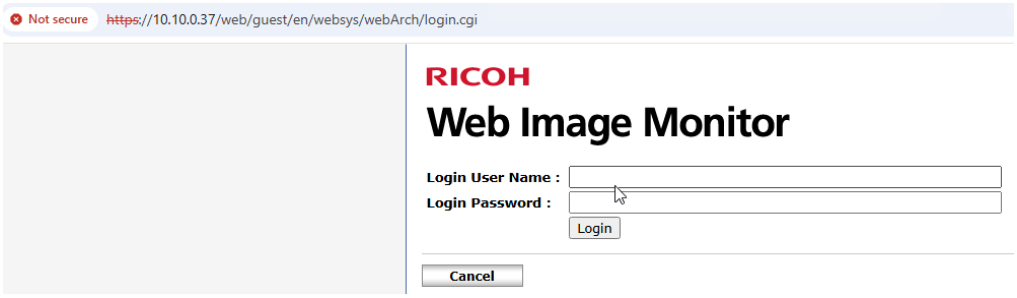
- by entering the website address directly into a browser;
- or via the Watchdoc administration website.

To access **Web Image Monitor** via Watchdoc:

1. in the Watchdoc administration interface from the **Main Menu**, **Production** section, click on **Printing Queues, locations, queue groups & pools** link;
2. in the list of printing queues, click on the Ricoh queue on which you wish to install WES:
3. in the queue configuration interface, under the Status tab, in the Monitoring section, click on the device **IP address**:



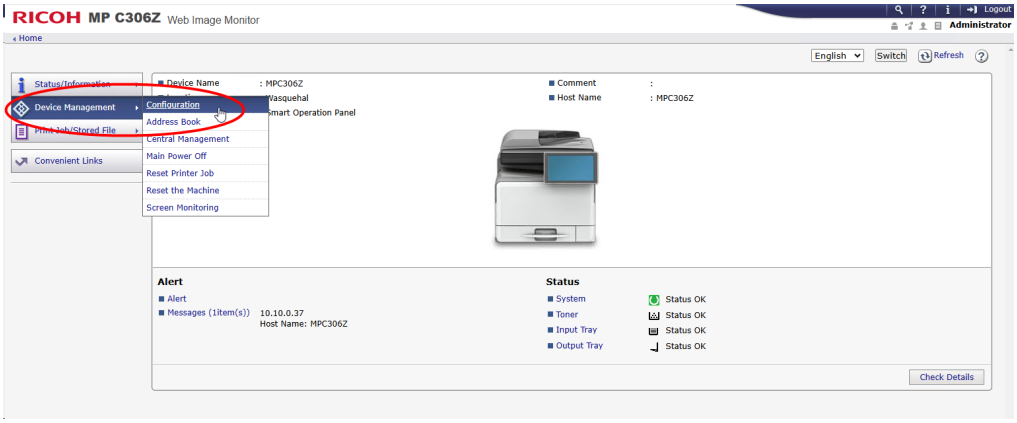
4. you access **Web Image Monitor**, the Ricoh device administration website.
5. Authenticate yourself as administrator:



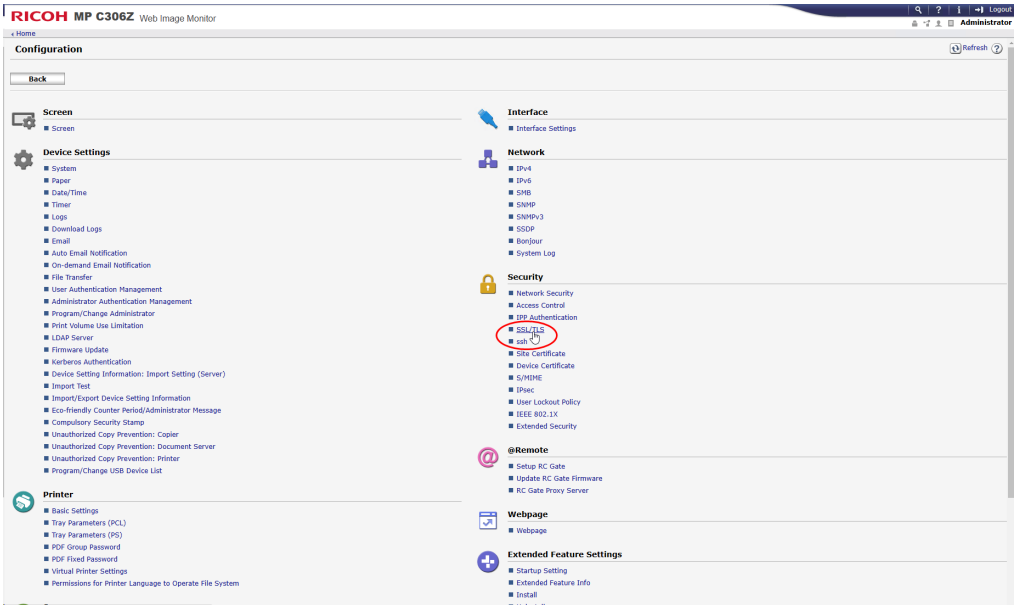
Enable SSL / TLS communication

To enable exchanges between the device and the WES, you first need to activate SSL/TLS communication:

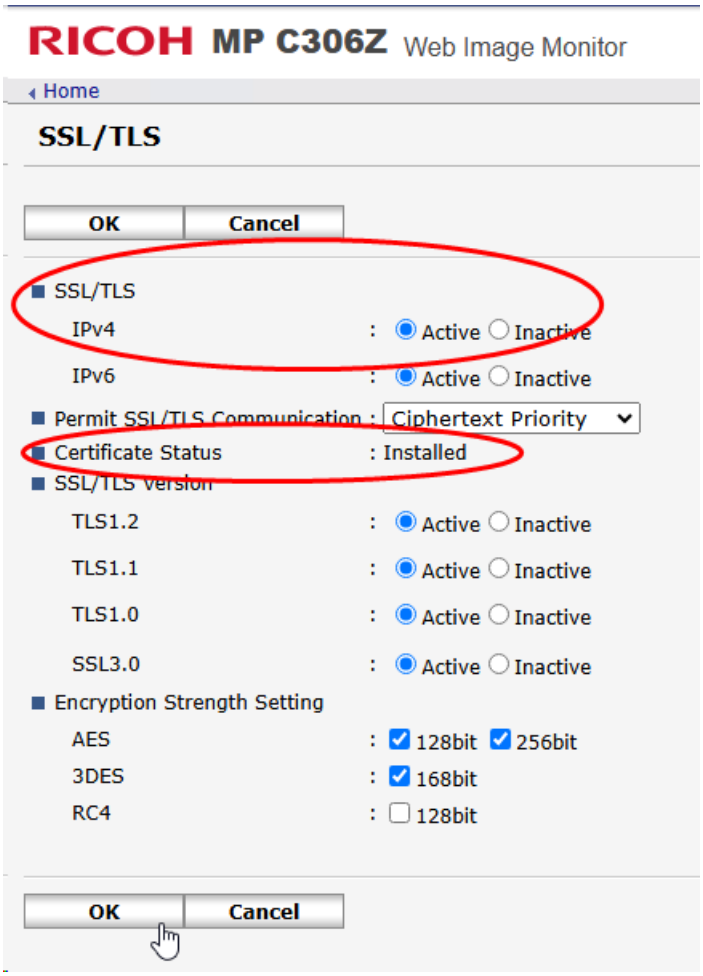
1. from the administration interface, go to **Device Management > Configuration:**



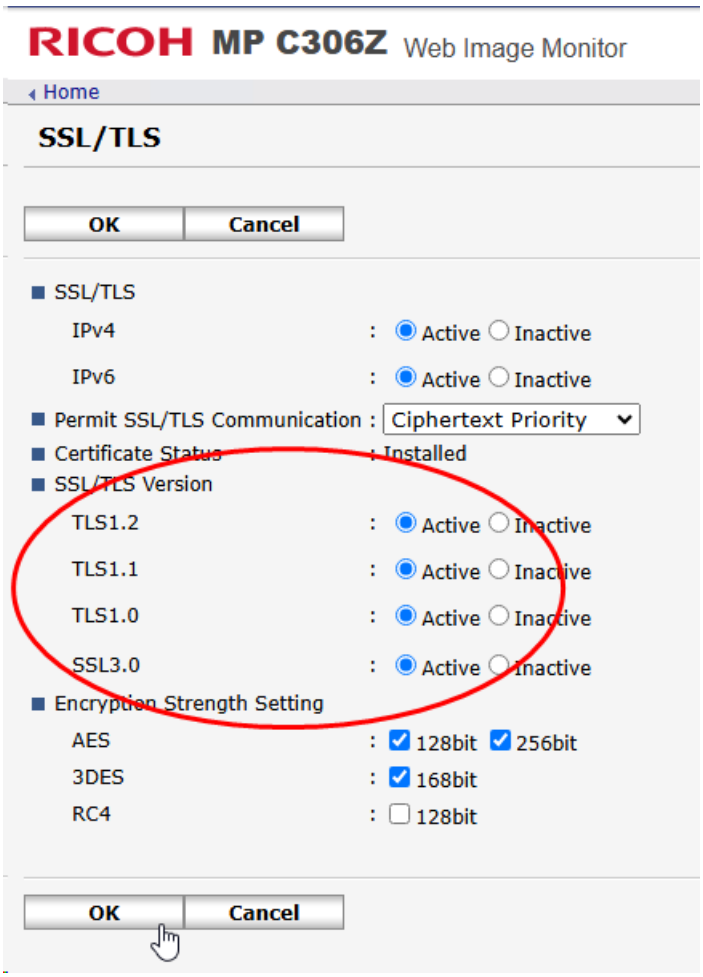
2. in the **Security** section, click on **SSL/TLS**:



3. in the SSL/TLS interface, check :
    - IPv4 parameter is enabled ;
    - the SSL certificate is installed.



- for generation 2.5 devices, check that all radio buttons in this section are enabled:

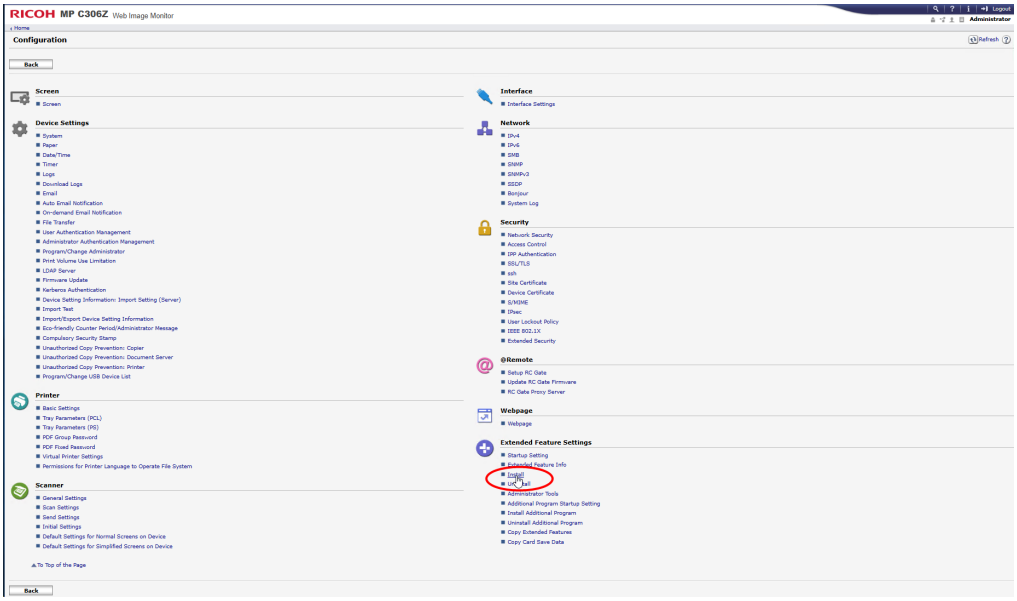


4. click on **OK** to validate the settings.

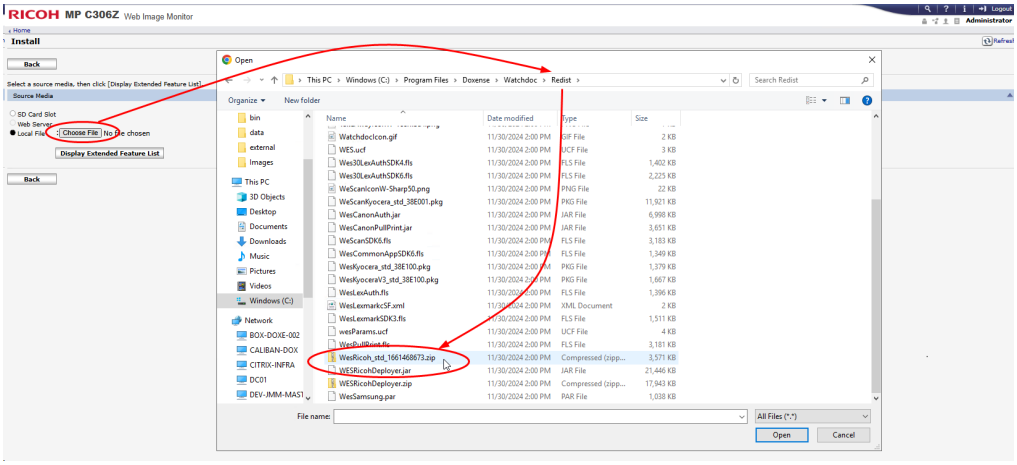
Install the WES from the Ricoh® device interface

Access the interface

1. from the **Configuration** interface, in the **Settings - Advanced functions** section, click on **Install**:



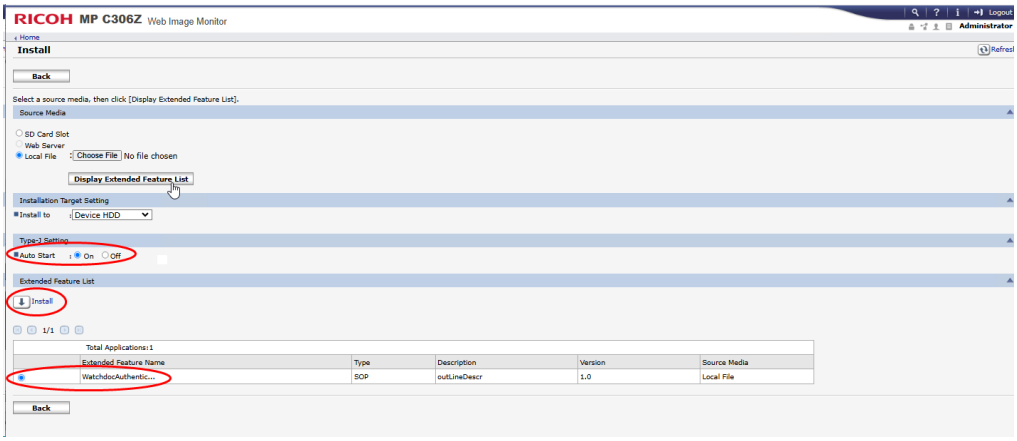
2. in the **Installer** interface, click on the **Local file** radio button, then click on Browse ;
3. in the selection window, browse your working environment to select the Ricoh WES installation file inProgramsDoxenseWatchdocRedist by default):



4. once the file has been selected, click on the Show advanced functions list button (N.B.: the display may take several seconds)
   ➔ new configuration sections appear in the interface.

Install authentication

1. In the **Installer** interface, in the **Type-J Configuration** section, check the **ON** radio button to enable **Auto-Start** ;
2. in the Advanced features list section, check the Watchdoc Authentication radio button,
3. then click **Install**;

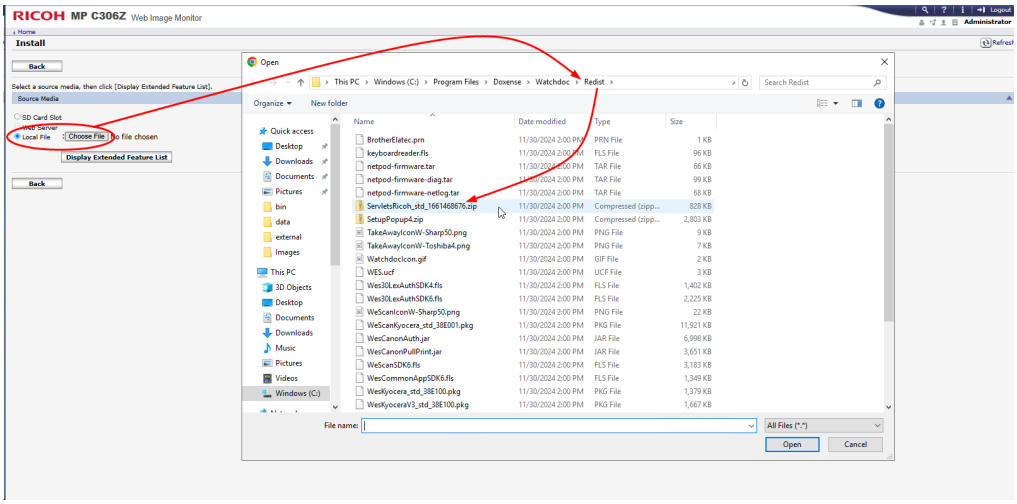


4. In the **Confirm** window, click on **OK**:

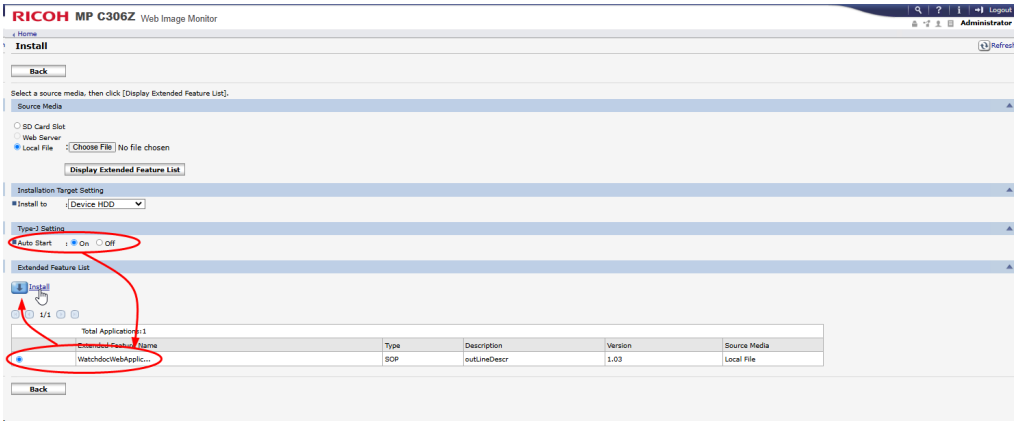
➔a confirmation message informs you that the **WatchdocAuthentication** advanced function is being installed and the **Install** interface reappears.

Install the servlet

1. In the **Install** interface, click again on the **Local file** radio button, then click on **Browse** ;
2. in the selection window, browse your working environment to select the compressed folder ServletsRicoh_std_[...] (in ...\Programs\Doxense\Watchdoc\Redist by default) :



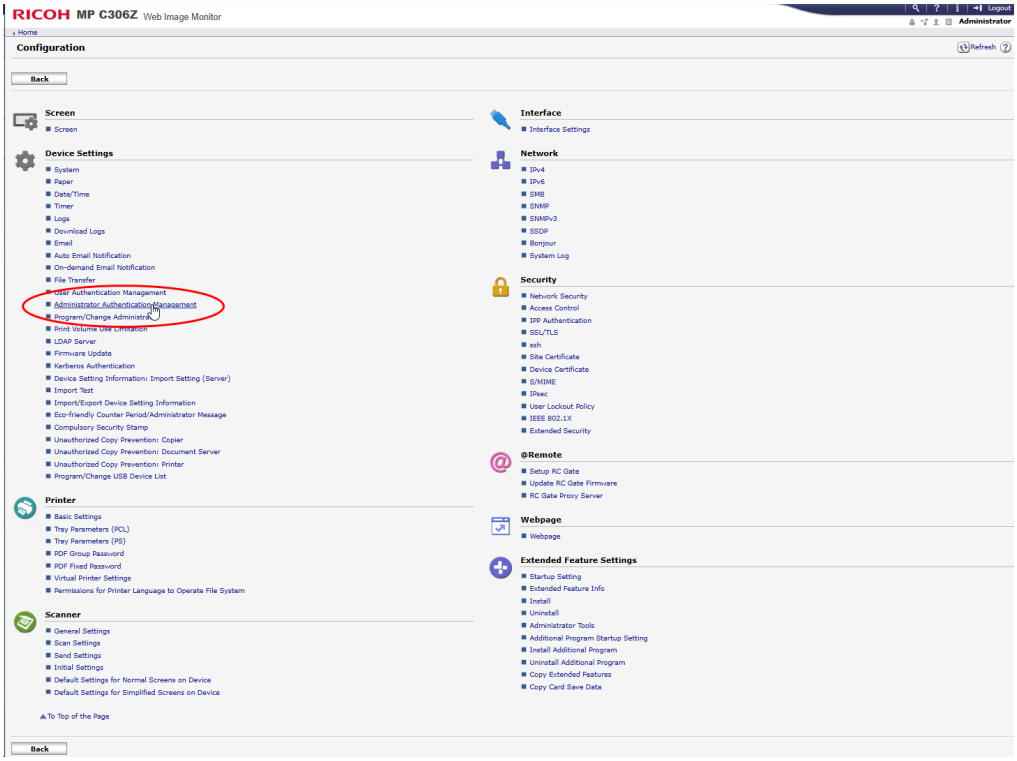
3. once the file has been selected, click on the **Displayed Extended Feature List** button;
4. in the **Extended features** list section, check the WatchdocWebAppInstallation radio button, then click on Install;



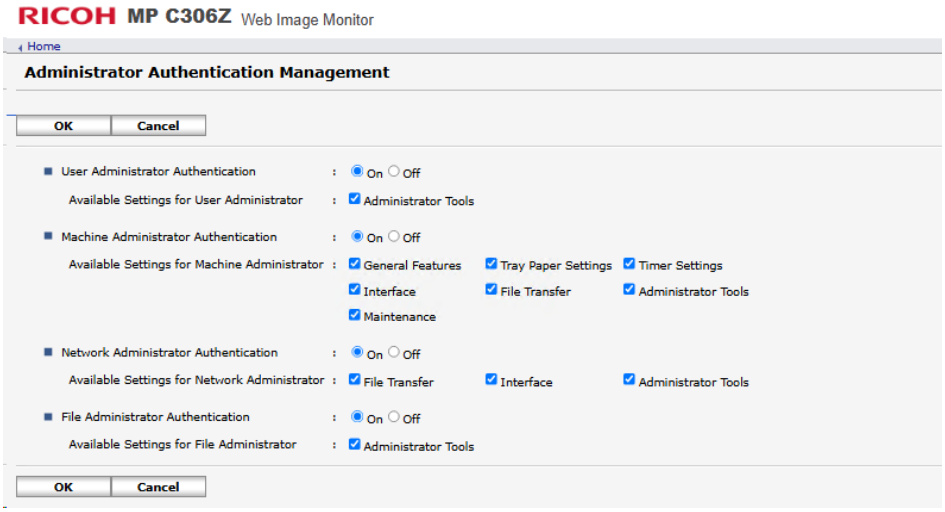
5. In the **Confirm** window, click on **OK** :
   A confirmation message informs you that the WatchdocWebAppInstallation advanced function is being installed..
6. click **OK** to confirm installation.
   You then return to the **Install** interface.
7. In the Install interface, click on the **Back** button to return to the general configuration interface.

Configure administrator authentication

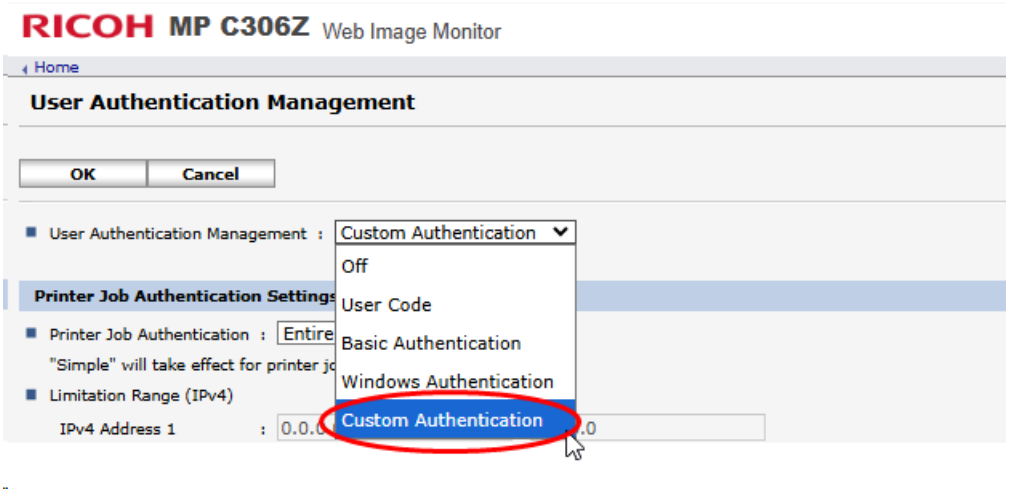
1. In the **Configuration** interface, **Device Setting Information** section, click on **Administrator authentication management**:



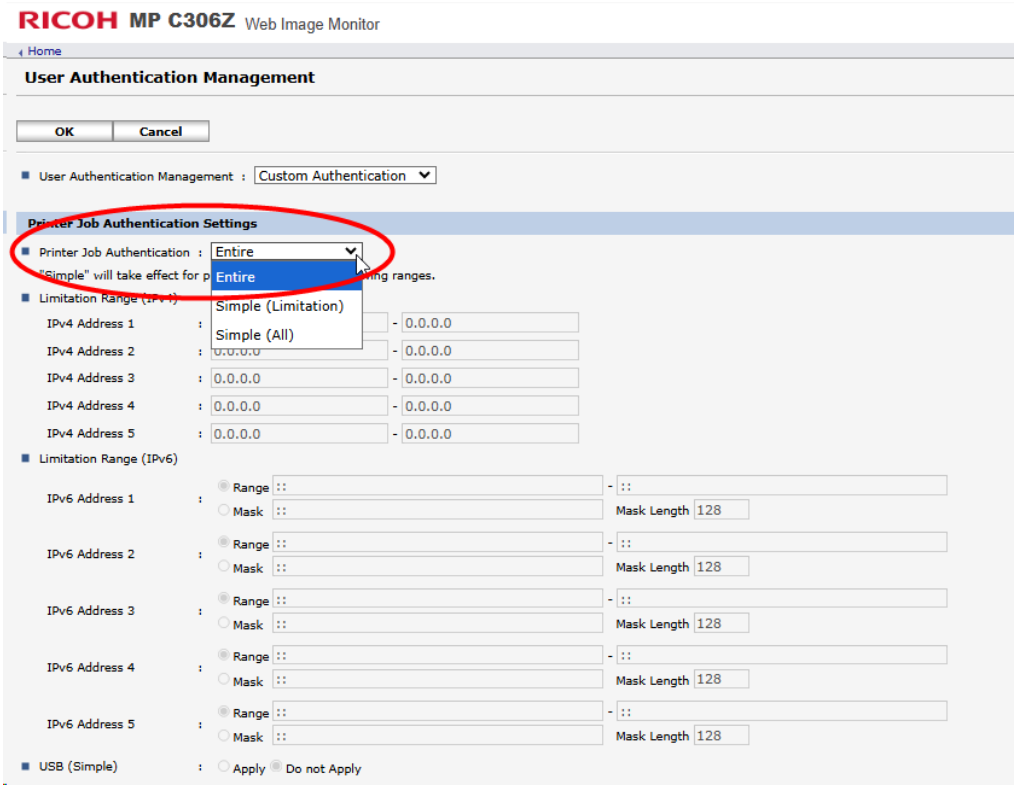
2. In the **Administrator authentication management** interface, check the **ON** radio buttons to activate :
    - user administrator authentication ;
    - administrator tools ;
    - machine administrator authentication ;
    - all parameters available to the machine administrator ;
    - network administrator authentication ;
    - all parameters available to network administrator ;
    - file administrator authentication ;
    - all parameters available to file administrator.



3. Click on **OK** to validate the settings;
4. You return to the general configuration interface.
5. Click on **User authentication management** parameter, select **Custom Authentication** from the list;
   N.B.: if the **Custom authentication** management type does not appear in the list, this means that SP modes are not correctly configured on the device (see **Configuring SP modes**).



6. click on **OK** to confirm your choice;
7. in the dans la section **Printer Job Authentication Settings** displayed, for the Printer Job Authentication setting, select **Entire:**

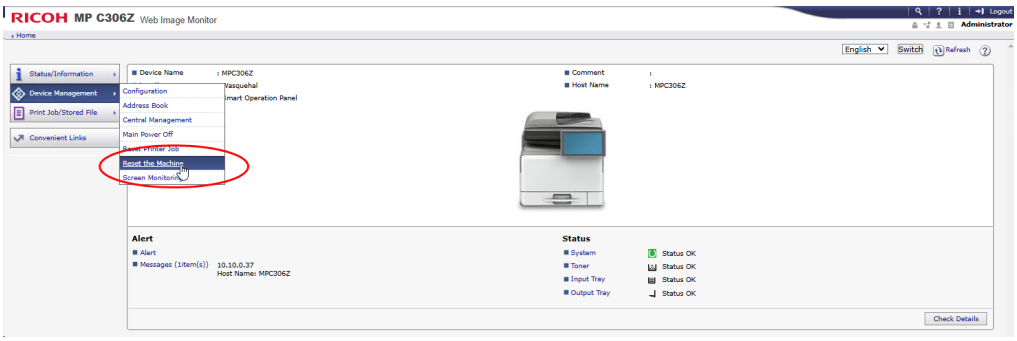


8. Keep the other parameters as default, then click on **OK** to validate the configuration.
   You will then return to the general configuration interface.

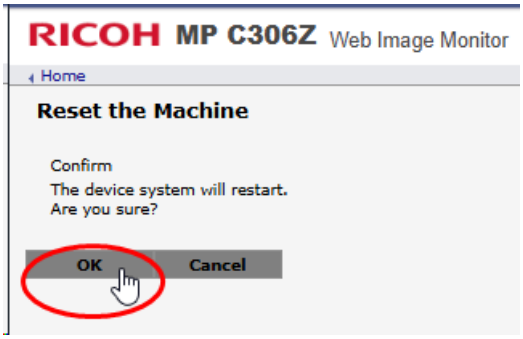
Reset device

Once these settings have been completed, the device must be reset:

1. from the **Image Monitor Web** interface > **Configuration**, click on the **Back** button ;
2. in the menu, click on **Device Management** > **Reset Device**:



3. in the **Reset device** interface, click **OK** to confirm the restart:

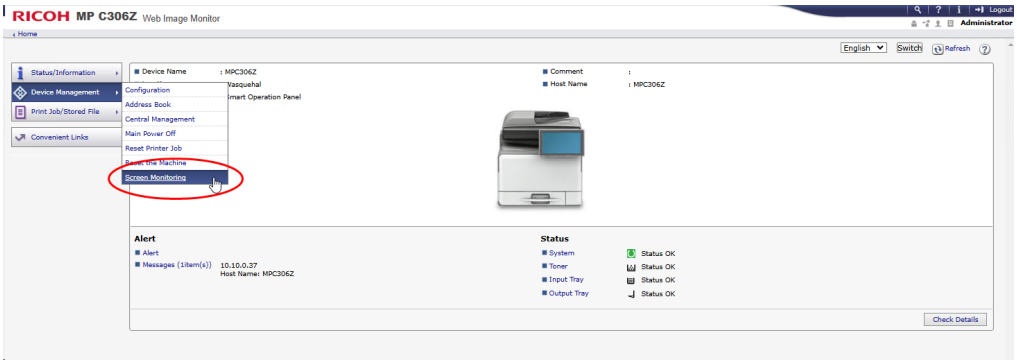


A message informs you that the device is inaccessible during the reboot and invites you to wait.

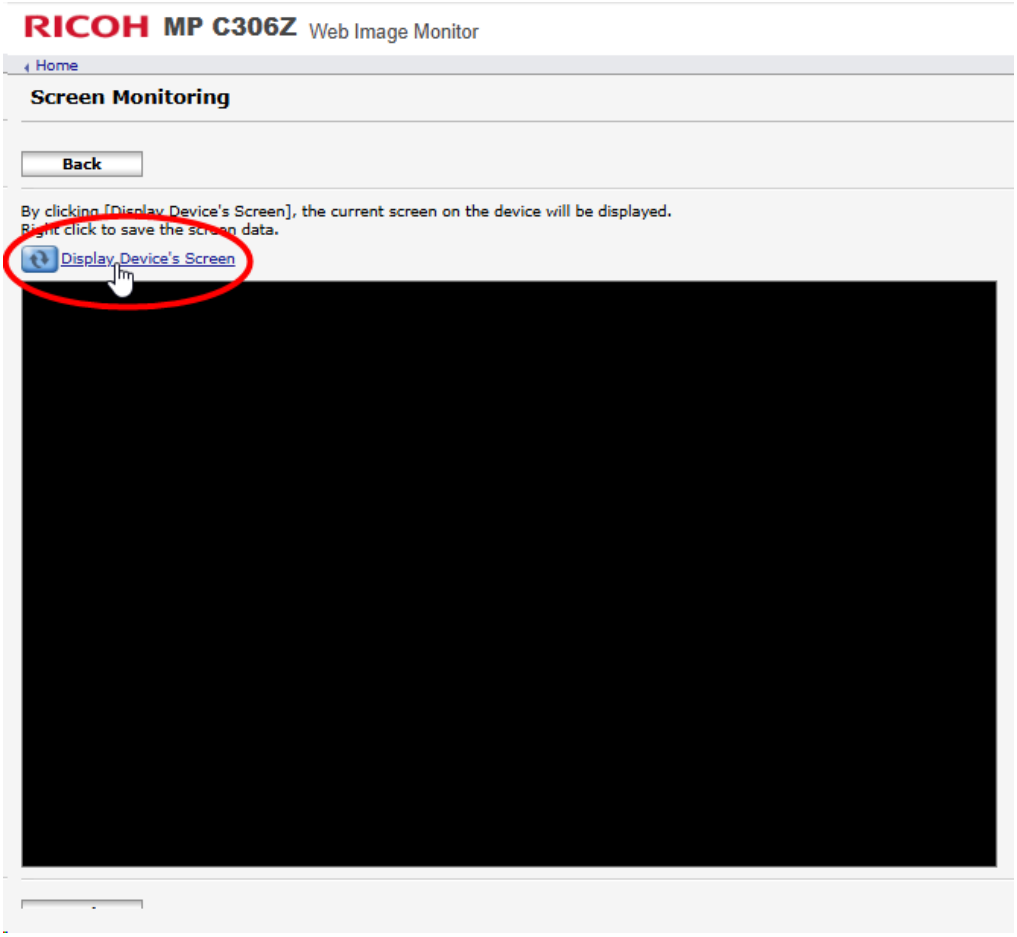
Check device status

You can check the device's status using the screen simulator. To access the simulator:

1. You can check the device's status using the screen simulator. To access the simulator :
   from the **Web Image Monitor** device administration interface, click on the Device Management>Screen Management menu;



2. in the **Screen Management** interface, the device screen is displayed. When the device restart is complete, the message displayed is “Settings modification complete”:
3. Click on the **Display device's screen** link to update it:



➔ A message informs you that the installation is continuing and awaiting a valid configuration:

4. Click the **View** device screen link again to update the device.
5. Return to the Watchdoc configuration interface to install the WES.

Troubleshoot the WES

General troubleshooting rules

- **What?** What procedure can be used to reproduce the incident?
- **When?** What date and time did the incident occur?
- **Where?** On which printer did the incident occur?
- **Who?** On which user account did the incident occur?
- **Watchdoc.log:** thank you for providing the Watchdoc.log file;a
- **config.xml file**: thank you for providing the Watchdoc.log file;
- **server/device communication logs**: please activate the trace files on each file.

Once this information has been gathered, you can send a resolution request from the Connect portal, the incident management tool dedicated to partners.

To obtain the best possible record of the data required for diagnosis, use the Watchdoc DiagTool® supplied with the Watchdoc installation program (cf. Creating a log report with DiagTool).

Scan, fax and photocopying are not in Watchdoc

If the scan, fax and photocopy jobs are not counted by Watchdoc, verify that the address (host name or IP) of the Watchdoc server configured in the device is correct:

1. Iin the configuration interface of the queue, in the WES section, click on the button **Application status** (displayed when the WES is properly installed);
2. Click the **Download** button to download the log files and WES configuration;
3. In the downloaded .zip file, open the Config.json file using a text editor and check the information corresponding to the address of the server (Address) and ports;
4. If the configuration of the address and / or ports is not correct, click on the Configure button on the queue configuration interface.
5. Verify that the procedure has resolved the problem.

Activating WES Traces

To diagnose a problem with WES applications, you need to activate the log files specific to WES communications :

1. in the Watchdoc web administration interface, from the **Main Menu**, **Production** section, click **Printing queues, queues groups & pools**;
2. In the list of queues, click on the name of the queue with the WES for which you want to activate the trace files;
3. in the queue management interface, click on **Properties**;
4. in the **WES** section, click on the **Edit the settings** button:
5. in the **WES>Diagnostics** section, tick the **Enable traces** box;
6. in the **Trace level** list, select:

- **Auto:** retains standard traces;
- **Include binary content:** retains detailed traces.

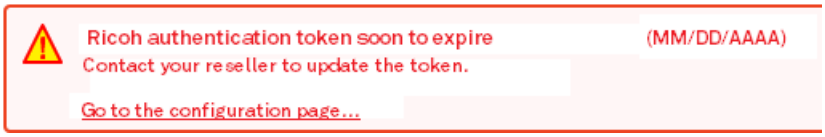
7. In the **Path field**, enter the path of the folder in which the trace files should be saved. If you leave the field blank, the trace files will be saved by default in the Watchdoc_install_dir/Logs/Wes_Traces/QueueId installation folder:

Activating the logs may slow down the server, so it is strongly recommended that you deactivate this option once the problem has been resolved.

Renewal of the Access Token before expiration

Context

When Watchdoc uses a Ricoh WES, it may occur that an alert message indicates that the access token will soon expire and invite you to contact your retailer:



Resolution

This issue can be solved by the update of Watchdoc.
If the Watchdoc update is not possible, the issue can be solved by the manual modification of the Watchdoc configuration file.

Since this procedure requires a service interruption, be sure to perform it when it will have the least impact on printing activity. Depending on the size of your print fleet, this service interruption can take between 15 seconds and 20 minutes.

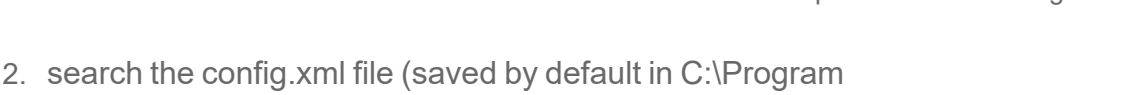
Procedure

To modify the Watchdoc configuration file:

1. log in to the server that hosts Watchdoc as an administrator and shut down the Watchdoc service;

2. search the config.xml file (saved by default in C:\Program Files\Doxense\Watchdoc\Data\config.xml);
3. copy the config. xml file to save it;
4. open the config. xml with a text editor and seach the tag <ricoh-web-api>.
5. If this tag doesn't exist, create it under the <instances><default-instance> tag; modify the tags included in this tag as follows:

<ricoh-web-api>
<remote>
<token>/yRUEU9p0bcbIoN5wA3BTxPAAITn+8LXqRCmNpzb7zHjvk6Qc
xQqZyKragYFtX9qgisDrak4lTi1EjQYncukK9cMwxi1jShy5fN9qCUy9HRd
L8qIYr4mU6aQrJhVVUwE8sWIRaaZG/3aZA07ybuJvUEoTf/OA66ja2I8Cf
+9N4oGvErB3D6ZZh3GJ+kYcUZ0</token>
<valid-until>20260123</valid-until>
</remote>
<browser>
<token>/yRUEU9p0bcbIoN5wA3BTxPAAITn+8LXqRCmNpzb7zHUG08F
n3losZyFihRFrLgsgisDrak4lTi1EjQYncukK4cxmrZHgFOSkv7Yl2KGKSJh
DL4Jw8dRfwat4g6pQkkV8sWIRaaZG/3aZA07ybuJvWtAIrYyDz2ZFxhihx
/d5srA+yWYP6Sbn8dufT8VstpiMtpQC6O/rDX3/tY1jGK6jw==</token>
<valid-until>20260123</valid-until>
</browser>
</ricoh-web-api>


In the <token> tag, there must be no spaces in the character string; if there are spaces, remove them.

6. As in the following example:

5. save the config.xml file;
6. restart the Watchdoc service;
7. in the Watchdoc administration web site, check that the access token alert message no longer displays.

Unable to find the ‘Doxense.Web assembly, Version=5.4.0.0, culture=neutral, PublicKeyToken=94de63351b6ea861’.

Context

When the Ricoh WES is installed, the following error is displayed when the **Configure** button is clicked:

```
Unable to find the 'Doxense.Web Version=[n°_version],
Culture=neutral, PublicKey Token=94de63351b6ea861'
```

Resolution

Install the Ricoh WES manually.
Do not use the WESRICOHDEPLOYER

Information to ask the technician
Have the login details for the print device's web portal.
Ask the technician on site to activate SP Modes and confirm as many times as possible using the hash key #.

- 5-113- 002 = 0
- 5-401-230 = 00000001
- 5-401-240 = 1000
- 5-420-041 = OFF
- 5-490-001 = Allowed