Kofax Copitrak
Xerox Application Installation Guide

Version: 3.1.99

Date: 2023-06-13

KOFAX

Table of Contents

Preface

This guide provides information on how to install the Copitrak SP5 Xerox Altalink and Versalink Applications on a CSS Server. These applications use IIS to communicate with the MFP and make Copitrak functionality available on the device's touchscreen, they work in place of the Copitrak Embedded software and were developed especially for the new Altalink and Versalink devices - while preserving support for legacy Copitrak-enabled Xerox MFPs.

Related documentation

Product documentation for Kofax Copitrak 3.4.0 is available here:

https://docshield.kofax.com/Portal/Products/Copitrak/3.4.0-csb5nx1k32/Copitrak.htm

Training

Kofax offers both classroom and online training to help you make the most of your product. To learn more about training courses and schedules, visit the Kofax Education Portal on the Kofax website.

Getting help with Kofax products

The Kofax Knowledge Portal repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Portal to obtain answers to your product questions.

To access the Kofax Knowledge Portal, go to https://knowledge.kofax.com.

> ℹ️ The Kofax Knowledge Portal is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Kofax Knowledge Portal provides:
- Powerful search capabilities to help you quickly locate the information you need.

  Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.

  To locate articles, go to the Knowledge Portal home page and select the applicable Solution Family for your product, or click the View All Products button.

From the Knowledge Portal home page, you can:

- Access the Kofax Community (for all customers).

  On the Resources menu, click the **Community** link.

- Access the Kofax Customer Portal (for eligible customers).

  Go to the Support Portal Information page and click **Log in to the Customer Portal**.

- Access the Kofax Partner Portal (for eligible partners).

  Go to the Support Portal Information page and click **Log in to the Partner Portal**.

- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

  Go to the Support Details page and select the appropriate article.

Prerequisites

To set up and configure the Copitrak SP5 Xerox Altalink, Versalink, C70 and PrimeLink Application, the following prerequisites are required:

- A supported Xerox Altalink, Versalink, C70 and/or PrimeLink device (verify your model(s) at https://knowledge.kofax.com/MFD_Productivity/00_Supported_Devices/Supported_Devices)
- Fully configured CSS server (build 700) SP2 with Copitrak DFI and SQL server installed
- IIS Manager installed (only required if Copitrak embedded system is to be installed on an Operating System other than a CSS server)
- The following Windows features turned ON: .NET Extensibility, ASP.NET, ISAPI Extensions and ISAPI Filters

  ℹ This section is relevant only if you plan to install Copitrak embedded system on an operating system other than a CSS server.

- Installer package including:
  - Installer file: EmbeddedXerox.exe

    ℹ This installer fully supports the old Legacy app and the older, pre-Altalink/Versalink/C70/ PrimeLink Xerox Work Centres.

  - Configuration file: terminal_XEROX_setup.xml
- Optional: Java Version Update 7 if you want to debug supported legacy devices pre-dating Altalink/Versalink/C70/PrimeLink.

Installation overview

After you have ensured that your system meets the preliminary requirements, you can start installing the Copitrak application for Xerox Altalink/Versalink/C70/PrimeLink. (If you have an earlier version of the Copitrak embedded application for Xerox, uninstall it first.) All required components of the solution are deployed by a single installer named EmbeddedXerox.exe. Use this executable to install the following on the CSS server (There are no components installed on the MFPs. The devices contact the CSS server to render pages for navigation):

- Microsoft WSE 3.0 (installed with a graphical interface)

  > ℹ If you have Microsoft WSE 3.0 already installed, the Xerox installer will skip the installation of this component.

- CopitrakCaApp - the Copitrak Convenience Authentication Application responsible for validating all users and account numbers (installed silently)
- CopitrakAdmin - this web application is used to configure the other applications in order that they connect correctly to the database and the CSS server (installed silently)
- CopitrakEIPGUI - the main configuration tool for the solution (installed silently)
- CopitrakPsApp - the Copitrak Presentation Service Application (selectable during installation) used for supported legacy devices as well as account validation
- CopitrakAltalinkPsApp - the Copitrak component for Xerox Altalink devices (selectable during installation)
- CopitrakVersalinkPsApp - the Copitrak component for Xerox Versalink devices (selectable during installation)

Once all required components and applications are successfully installed using the EmbeddedXerox.exe executable, you are ready to perform configuration steps via the web administration interfaces of your MFP devices as well as the GUI application.

The server-based embedded terminal communicates with three Xerox services:
- CA = Convenience Authentication
- PS = Presentation Services
- JBA = Job Based Accounting

This document follows the process outlined above:

1. Steps to be performed before installation

2. Installation process

3. Configuration tasks after installation is complete

Before installation

After you have verified the prerequisites, proceed as follows:

1. Go to the **Copitrak** folder on your desktop, and double-click the **CSS Manager** shortcut to launch the **Copitrak System Software Login** page in your default browser. Provide your password, and click **Login**.

2. On the **System Configuration** pane, select **Lists** > **Sites** > **Terminal setup**.

3. Under the **Terminal Setup** tab, create a new terminal with your MFP's name. Add **ID** and select **Unit Class** from the dropdown menu.

4. Go to the **Copitrak** folder on your desktop, and double-click the **Config File Manager** shortcut to launch the **Copitrak Configuration Manager Login** dialog box. Provide your password, and click **Login** to continue.

5. Select **Terminal/User Options**.

6. In **Configuration File Manager**, select **Terminal Group**, and click **Copy Default Group**.

7. Rename **Terminal Group** to **Terminal Group Xerox**.

8. Rename the terminal_setup.xml to terminal_XEROX_setup.xml.

9. Open the terminal_XEROX_setup.xml file in a text editor, and replace the default value of **setting name="Server_Host"** with the IP address of the CSS server. Save the file.

10. Copy the modified terminal_XEROX_setup.xml file to the DFI configuration folder at **C:\inetpub\wwwroot\CopitrakDFI\Config**.

11. Skip step 11-14 if you are installing Copitrak embedded application on a CSS server. Otherwise, go to **Control Panel** > **Programs** > **Turn Windows features on or off**, and turn on the following four Windows features:
    - .NET Extensibility
    - ASP.NET
    - ISAPI Extensions
    - ISAPI Filters

12. Click **Next** to the **Server Roles** section of the **Add Roles and Features Wizard**, and select **Web Server (IIS) Support**.

13. Ensure the **Include management tools (if applicable)** checkbox is marked and click **Add Features**.

14. Click **Next** when **Web Server (IIS) Support** checkbox is marked.

15. Click **Next** to the **Confirmation** section, and click **Install**.

16. Click **Close** when the Wizard prompts you to do so, and the rest of the installation process completes in the background.

Installation process

1. Launch the EmbeddedXerox.exe to start the installation process.
2. In the **Welcome** screen, select the applications to be installed.
   - Copitrak Ps App: for older versions of Xerox devices
   - Copitrak Versalink Ps App: for Versalink devices
   - Copitrak Altalink Ps App: for Altalink devices
3. Click **Install**.

The process will first launch the Microsoft WSE 3.0 Installation Wizard, if you do not have it already installed on your system.

Install Microsoft WSE 3.0

1. Click **Next** in the **Microsoft WSE Installation Wizard Welcome** screen.
2. Click the radio button to accept the terms in the license agreement, and click **Next**.
3. Select **Runtime** as the **Setup Type**, and then click **Next**.
4. Click **Install**.
5. Click **Finish** after the installation is complete, and then close the readme file that opens in your default web browser.

Install Copitrak applications

After the installation of Microsoft WSE completes, the installer resumes installing Copitrak Applications.

1. Once the installation is finished, a dialog box appears notifying successful installation. Do not click **OK** in the dialog box.
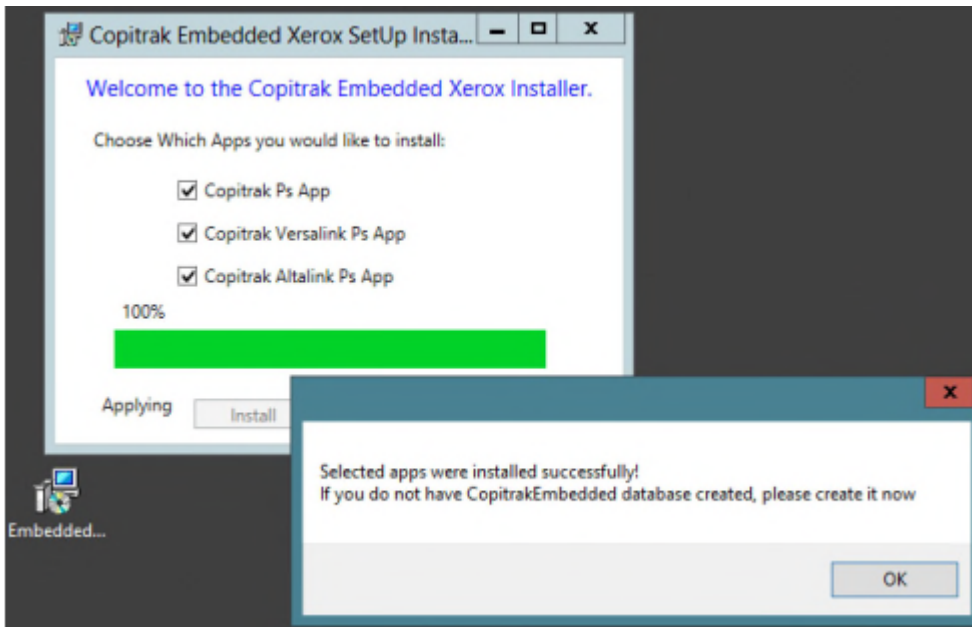
2. Open the **Microsoft SQLManagement Studio**, and log in using your credentials.

3. Create an empty database named **CopitrakEmbedded**. To do this, right-click **Databases** in **Object Explorer**, and select **New database**, and then click **OK**.

4. Navigate to **C:\ERS\EmbeddedXerox** and run the two SQL scripts `db.sql` and `db2.0.sql` in this order. These script files will create tables in the database. Make sure you click **Execute** for both script files in SQL Management Studio, othewise the tables are not created. Make sure you see the **Command(s) completed successfully** message.

5. Click **OK** on the installation successful message.

Verify connection with CopitrakAdmin

After you click **OK** in the Installation Successful message, you need to adjust security settings for the installed Copitrak Applications in a web browser. The following section uses a default Internet Explorer example.

1. A browser window is launched for the **CopitrakAdmin** page in your default browser (typically Internet Explorer). Click **Continue to this website (not recommended)**.

2. Verify that the page at *https://localhost:44328/Admin.aspx* shows the **CopitrakAdmin** page. Leave this browser window open.

   Use this interface to:

   • test the connection and verify that the applications are installed successfully, and connection is available.

   • change database credentials as well as Copitrak server IP.

3. Click **Test** to ensure that the applications are installed correctly. To proceed with adding security exception to each of pages with the installed applications, click **Yes** on each of

the **Security Alert** dialog boxes that appear as many times as the number of the installed applications.

After you click **Submit**, the **Connection successful!!!** message indicates that the security exception is added to each application. Applications are installed properly and are ready to be configured.

A **Security Alert** dialog box appears for each installed application including:

- CopitrakCaApp - installed automatically and silently
- CopitrakEIPGUI - installed automatically and silently
- CopitrakPsApp - selectable during installation
- CopitrakAltalinkPsApp - selectable during installation
- CopitrakVersalinkPsApp - selectable during installation

4. Once a successful connection has been verified, applications are ready to be configured as follows:

   a. Enter Database User ID.

   b. Enter Database Password.

   c. Enter Copitrak Server IP and click **Submit**.

> ℹ️ If you do not provide User ID, Password, and Server IP, an error message informs you about the missing input.

When all the fields required are entered correctly, the configuration completes successfully with a notification message.

5. Optionally, go the **C:\inetpub\wwwroot** and verify if the config files for all the installed applications are updated. Open the installation folder for each application, and open the Web.config file in a text editor to check if the CSS Server IP and the user ID/password reflect your recent changes.

6. Update the terminal_setup.ini file in **C:\inetpub\wwwroot\CopitrakDFI\Config** with the **Xerox** string.
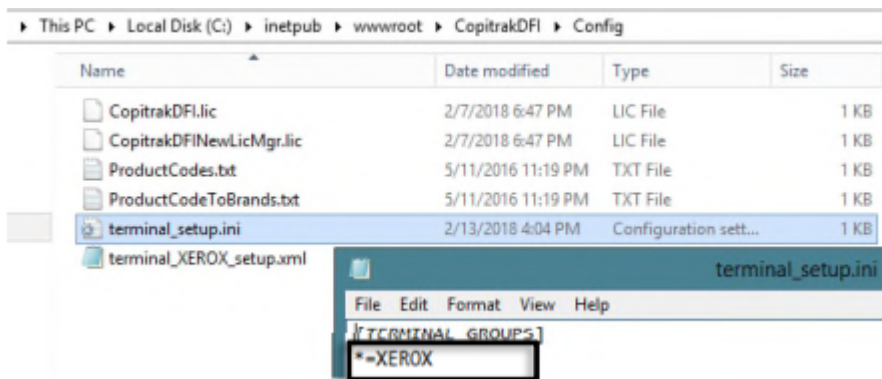
7. Verify if **setting name="ps_app_show_welcome_page"** value is set to **Yes** in terminal_XEROX_setup.xml file.

After finishing the above process, you are ready to move on to configuration.

If you have any third-party firewall system installed on your CSS server, make sure you add the ports required by Copitrak to the firewall exception. The Embedded Xerox installer does this automatically for the native Windows Server firewall.

Port numbers required by Copitrak applications:
- Copitrak**Ca**App: **44379**
- Copitrak**Admin**: **44328**
- Copitrak**Ps**App: **44313**
- Copitrak**Altalink**PsApp: **44394**
- Copitrak**Versalink**PsApp: **44366**

To verify the port numbers, do the following:

1. Go to **Control Panel** > **System and Security** > **Windows Firewall**.

2. Click **Advanced settings**.

3. Select **Inbound Rules**, right-click any of the Copitrak applications, and then select **Properties**.

4. Click **Protocols and Ports**. The port number is displayed in the **Local port** section.

Basic configurations

This chapter describes how to configure the Copitrak Application to work with the MFP. The high-level overview of the configuration process is as follows:

1. Configure your MFP using its web administration page
2. Add MFP
3. Register CopitrakPsApp on the Xerox MFP
4. Set CopitrakApp as default on your MFP

The steps in this section are performed using the Copitrak EIP GUI application and your Xerox Device's web administration interface.

Device configuration (web administration interface)

This section provides instructions to configure your devices to work with the MFP.

Xerox Altalink devices

Create a security certificate unless there is a default security certificate available for your Altalink device. Afterwards, proceed as follows:

1. Open a web browser (default web browser in this guide is Internet Explorer), and type the device's IP address in the browser's address bar. If you receive a **Certificate Error** message, click **Continue to this website (not recommended)**.
2. Click **Login** to log in as Administrator to the device. The user name and password are usually admin/1111.
3. Select **Properties** on the Xerox admin interface.
    a. Navigate to **Security** > **Certificates** > **Security Certificates**, and click **Create New Xerox Device Certificate** if the **Default Xerox Device Certificate** does not fulfill your needs.
    b. Click **OK** on the Javascript warning message.
    c. Modify any fields according to your needs, and click **Finish**.
    d. Wait until the certificate is generated.
    e. Depending on your browser, choose to proceed to the device web administration page (IP address of the device) if you receive an insecure connection warning.
4. Navigate to **Connectivity** > **Setup**, and make sure **HTTP** and **LDAP** are enabled.

⚠ **HTTP** is enabled by default if you navigate on the web administration page, since the Altalink device uses HTTP protocol for communication with the web server. If you click **Edit...** in the **HTTP** row, set **Configuration** to **Disabled** and then hit **Save**, the device will be no longer able to communicate with the web server. Should this happen, contact Xerox technical support to resolve the issue.

To edit any of the given properties, click the **Edit** button 🖊 on the right side of the property to be configured.

5. Make sure you enable **HTTPS** in **HTTP** section. To do so, click **Edit...** in the **HTTP** row, and select **Enabled** under **Connection** and **Yes (All HTTP requests will be switched to HTTPS)** under **Force Traffic over Secure Connection (HTTPS)**. Click **Save**.

6. Set the device to communicate with the CSS server. Select **Login/Permissions/Accounting** > **Login Methods** under **Properties**.

   a. In **Login Methods**, click **Edit** to enter the **Edit Login Methods** section.

   b. In **Edit Login Methods**, set **Control Panel & Website Login Methods** to the following:
      • Control Panel Login: Xerox Secure Access Unified ID system
      • Website Login: Username/Password Validate on the Network

   c. Click **Save**.

In **Configuration Settings**, under **Login Methods**, the following three properties must be configured:

• Xerox Secure Access Setup
• Authentication Servers
• LDAP Servers

7. Under **Configuration Settings**, in the **Xerox Secure Access Setup** row, click **Edit...** under the **Actions** column to configure the property.

   a. If your Xerox device has not been configured, click **Manually Configure** under the **Manual Configuration** section of the **Xerox Secure Access Setup** page. Otherwise, click **Manually Override Settings**.

   b. On the **Manual Override** page, enter the IP address of the CSS server and the port number.

      The port number for the CopitrakCaApp is **44379**. This is highly important for the application to function properly.

      The application authentication path is the default: **/SmartAuthServerImpl.asmx**.

      ℹ The CSS server IP address is the IP of the configured Copitrak server, but the port number of 44379 remains the same for all installations.

   c. Click **Save**.

   d. Click **Close**.

8. Under **Configuration Settings**, in the **Authentication Servers** row, click **Edit...** under the **Actions** column to launch the configuration page.

   a. Select **LDAP** as **Authentication Type**.

   b. Create the LDAP authentication server with any chosen name. The IP address must be the IP of the CSS server, and you need to select **Exchange** in the **LDAP Server** drop-down list.

   c. Click **Apply**, and then click **Close**.

   d. Click **Close** again to get back to the **Configuration Settings**.

9. Under **Configuration Settings**, in the **LDAP Servers** row, click **Edit...** under the **Actions** column to launch the configuration page.

   a. Similar details are needed as for the authentication servers. The used authentication server is LDAP. See step 8a-8d to edit the server details.

   b. Change the IP address to the CSS server IP, and set the port number to 44379.

   c. Click **Apply**, and then click **Close**.

   d. Click **Close** again to get back to the **Configuration Settings**.

Accounting methods configuration

Configure Accounting Methods (JBA configuration) for the transactions to be recorded.

1. Under **Properties**, select **Login/Permissions/Accounting** > **Accounting Methods**, and then click the green icon (or the **Edit...** button).

2. Under **Edit Method**, select **Network Accounting** from the **Current Accounting Method** drop-down list, and then click **Save**.

3. Under **Configuration Settings**, click **Edit...** to configure **Accounting Workflow** and **User Accounting Prompts**.

4. Under **Accounting Workflow**, select **Capture Usage** from the **Accounting Workflow** drop-down menu for all the five **Job Types** (Copy, Print, Scan, Email, Server Fax). Click **Save**.

5. Under **User Accounting Prompts**, set **Display Prompts** and **Mask Entries (***)** section to **Yes**, and select the **Prompt** option for all the three **Apps**, and then click **Save**.

> ⓘ Selecting the **Prompt** option for scans means that these scans will be tracked. If you set **Scans** to **No Prompt**, your scans will not be tracked.

6. Under **Configuration Settings** in **Accounting Methods**, click **Edit...** in the **Validation Policies/ Print Job exceptions** row. Set **Validation for Accounting Codes** to **Disabled**, and then click **Close**.

7. Go back to **Login/Permissions/Accounting** > **User Permissions**. Under **Configuration Settings**, click **Edit...** in the **User Permission Roles** row.

8. Under the **Non-Logged-In Users** tab, make sure that the **Description** says **Prevent non-logged-in users access to features**. Otherwise, click **Edit...** to block access to everything for non-logged-in users to prevent such users from performing any unauthenticated jobs.

On the **Manage user permissions (Non-Logged-in User)** screen, click **Apps & Tools**, and then select **Restrict Access to everything**. This will automatically change the apps role state to **Not Allowed** in the apps that are displayed under **Role State** drop-down menu. Click **Apply** to save the changes.

9. Once you are back to the **User Permissions** screen, click **User Permission Roles** again, and then select **Logged-In Users** tab.

If you are configuring it for the first time, you would not see any permission roles for the logged-in users. Click **Make Your Own Permission Roles**.

10. Fill in the **Role Name (Required)** and **Description** fields.

    Stick to a standard description to recall it easily. Click **View Quick Setup Options**. From the **Allow users...** option, select **Access to all apps**, and click **Create**.

11. Click the **Logged-In Users** tab and make sure it is set to **Allow logged-in users unrestricted access to all apps except admin tools**.

12. Navigate back to **Login/Permissions/Accounting** > **Login Methods** > **Xerox Secure Access Setup**, and click **Manually Override Settings**.

    Make sure you have **Automatically apply Accounting Codes from the server** selected in the **Accounting Information** section, since this option is usually disabled when **Accounting** is not set to **Network Accounting**.

Xerox Versalink devices

The Versalink administration interface is different from that of Altalink devices but overall, configuration steps are similar.

1. Open a web browser and enter the device's IP address in the browser's address bar. If you receive a **Certificate Error** message, click **Continue to this website (not recommended)**.

2. Click **Log In** to log in as administrator at the Versalink device's web administration page.

3. Select **System** > **Security**.

4. Under **Certificates**, select **Security Certificates** to open the **Security Certificates** dialog box.

5. Click **Create**, and select **Create Self-Signed Certificate**.

    The **Create Self-Signed Certificate** dialog box appears.

6. Optionally, you can enter "Copitrak" into the **Issuer** field. Other than that, do not modify any other parameters. Click **Create**.

7. Verify that the certificate has been created, then click **Close**.

8. Click **Close** in the **Security Certificates** dialog box.

9. Go to **Connectivity**. Under **Protocols**, turn on **HTTP** and **LDAP**.

    Also, make sure **HTTPS** is enabled for secure communication. Click **Edit...** in the **HTTP** row, and ensure that you have the following settings. Click **OK**.

10. Under **Permissions**, select **Login/Logout Settings**, and click **Select** in **Convenience** section if a different login method is selected. If **Convenience** is already selected, click **Edit**.

11. In the **Convenience Login** window, enter the CSS server IP address and the port number (44379). Specify **Path (/SmartAuthServerImpl.asmx)** and click **OK**.

    If a device restart is required due to changing the login method, click **Change** to restart your device. You will need to login again as Administrator to the device.

12. Under **Permissions**, go to **Login/Logout Settings**, and then select **Convenience** again by clicking **Edit**.

13. In the **Convenience Login** dialog box, do the following:

    a. Under **Alternate Login**, set **Allow users to login without their card?** to **Yes**.

    b. Set **Accounting Codes** to **Get codes automatically from server**.

    c. Under **Device Website Login Method**, select **Network** and then click **Edit** to configure it.

14. In the **Network Login** dialog box, select **LDAP**, and then click **Next**.
15. In the **LDAP** dialog box, click **LDAP Servers/Directory Services***.
16. In the **LDAP Servers/Directory Services** dialog box, enter the IP address of your CSS server and the port number for the CaApp such as **44379**.

    Leave everything else as their default settings. Click **OK** to come back to the **LDAP** dialog box, and click **Done**. If it prompts you for a restart, proceed with it to save your changes.
17. After logging in, go back to the **Convenience** screen in **Login/Logout Settings**, and then select **Convenience** to ensure you have made all the required changes and they are saved, especially if you did not restart on every prompt.

Once you complete the configurations, you should be able to log in to CopitrakApp on the MFP, unless you have some changes unsaved.

> ⓘ We recommend that you verify all your changes once you complete the above configuration steps.

Accounting methods configuration

1. Go to **Permissions** > **Accounting Method**.
2. If **Network** is already selected, click **Edit** to configure it.
3. Configure **Limits**, **Tracking Information** and **Information Verification** on the **Network Accounting** dialog box.
4. Under **Limits**, click **Setup**.
5. On the **Limits** dialog box, inactivate all the four job types under the **What to Limit** section using the switches. Click **OK**.
6. Go back to the **Network Accounting** dialog box, under **Tracking Information**, click **Edit**.
7. Ensure that the **Ask Users** and **Mask Input** options are switched on for both **UserID** and **AccountID**.

   Also, in the **When to Prompt** section, set **Always Prompt** for **Copy** and **Print**, and set **No Prompt** for **Scan** and **Fax**. To have your scans tracked, select **Always Prompt** next to **Scan**. **No Prompt** for **Scan** means that your scans will not be tracked.
8. Click **OK**.
9. Go back to **Network Accounting**, ensure that **Information Verification** is disabled, and click **OK**.

User permissions configuration

1. Navigate to **Permissions**, click **Roles**, and then select **Device User Roles**.
2. Click **Edit** in the **Basic User** section to configure what features logged-in users have access to.
3. In the **Edit Role** dialog box, make sure you specify **Access All** under **Control Panel Permissions** and **Everything Except Setup** under **Device Website Permissions**. Click **OK**.
4. Go back to **Permissions**, and click **Edit** under **Guest Access**. Select **Device User Role** to ensure that non-logged-in users are not able to access any jobs.
5. In the **Edit Role** dialog box, select **No Access** under **Control Panel Permissions** and select **Everything Except Setup** under **Device Website Permissions**. Click **OK**.

> ℹ️ Make sure that you save all the required changes, especially if you do not restart on every prompt.

Xerox C70 devices

1. Open a web browser and enter the device's IP address in the browser's address bar.
2. Log in as Administrator at the Xerox C70 device's web administration page.
3. Navigate to **Security** > **Certificate Management**, and verify that the device has a valid certificate. Create one if it does not exist.
4. Navigate to **Properties** > **Security** > **SSL/TLS Settings**, and make sure the settings are configured as below.
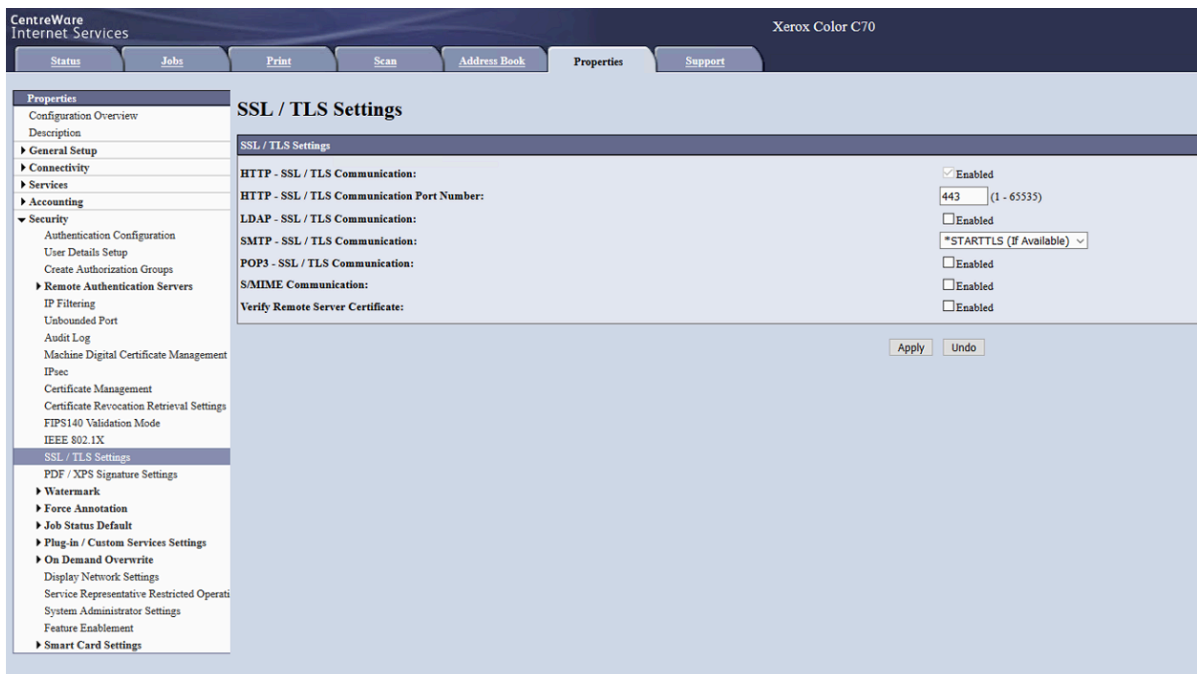
5. Navigate to **Properties** > **Security** > **Authentication Configuration > Step 1 of 2**, and make sure the settings are configured as below.
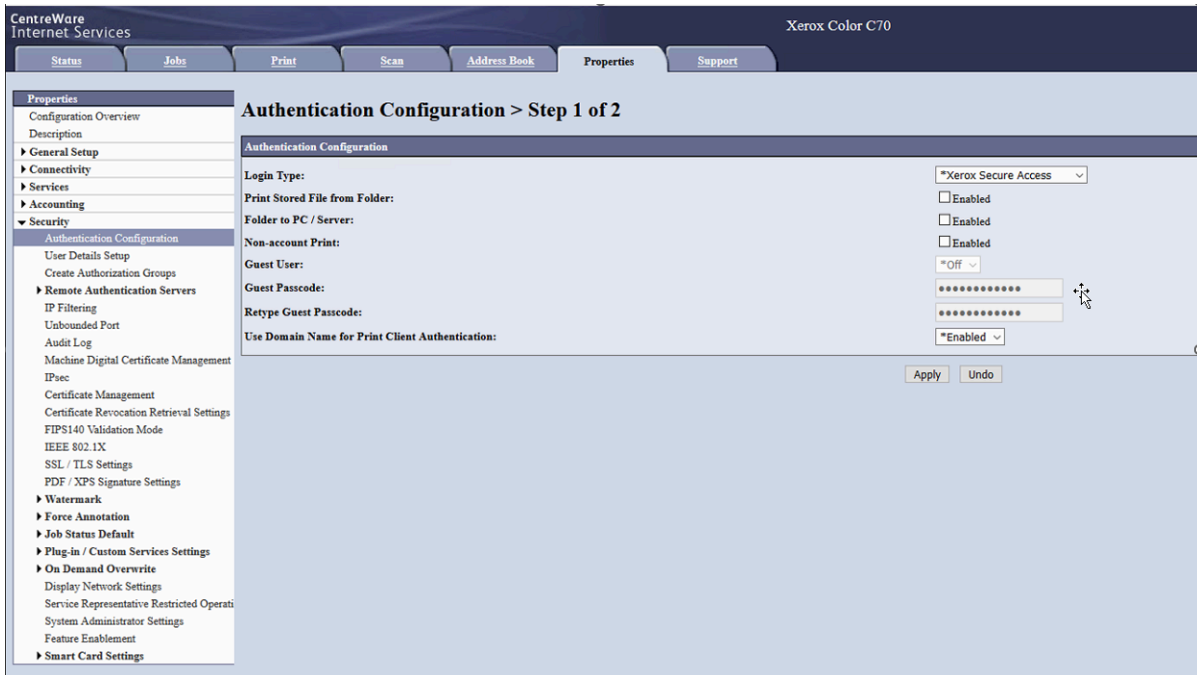
6. Click **Next**.
   You are prompted to **Authentication Configuration > Step 2 of 2**.
7. Under **Authentication - (Required)**, in the **Authentication System** row, click **Configure...**.
8. In the **Authentication System** row, select **Authentication Agent** in the drop-down menu.
9. In the **Assign UPN (User Principal Name)** row, select the **Enabled** check box, and click **Apply**.
10. Go back to **Properties** > **Security** > **Authentication Configuration > Step 2 of 2**, under **Access Control**, in the **Device Access** row, click **Configure...**.
11. Make sure the settings are configured as below.

12. Navigate to **Properties** > **Security** > **Remote Authentication Servers** > **Xerox Secure Access Settings**, and make sure the settings are configured as below.

13. Navigate to **Properties** > **Accounting** > **Accounting Configuration**.

14. Set the **Accounting Type** as **Network Accounting**, and select the **Enabled** check box for the **Auditron Mode** that you need such as Copy.
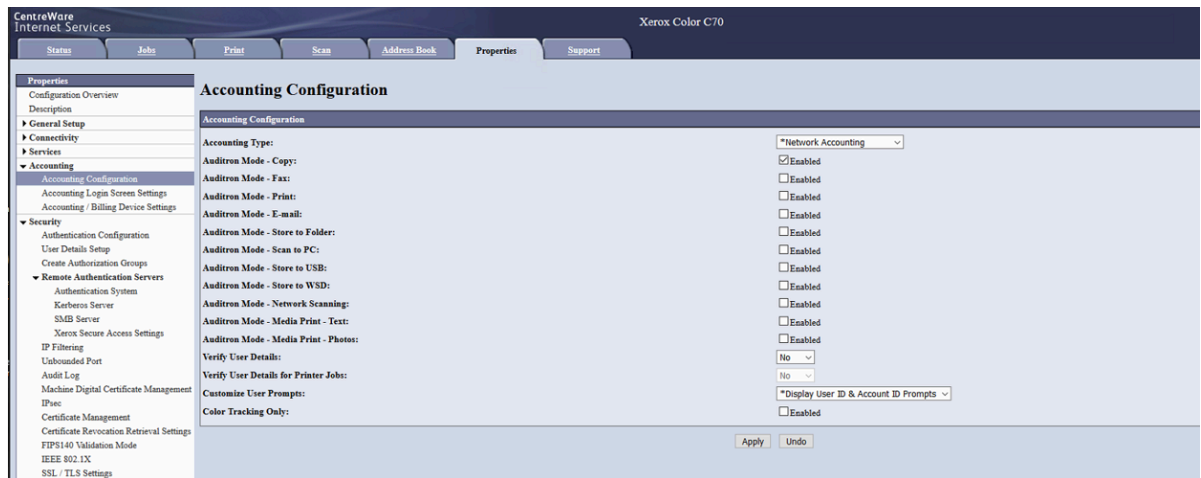
15. Navigate to **Properties** > **General Setup** > **Job Management** > **Extensible Services Setup**. In the **Extensible Services Registration** row, click **Edit....**

16. Make sure that the services are enabled as below.
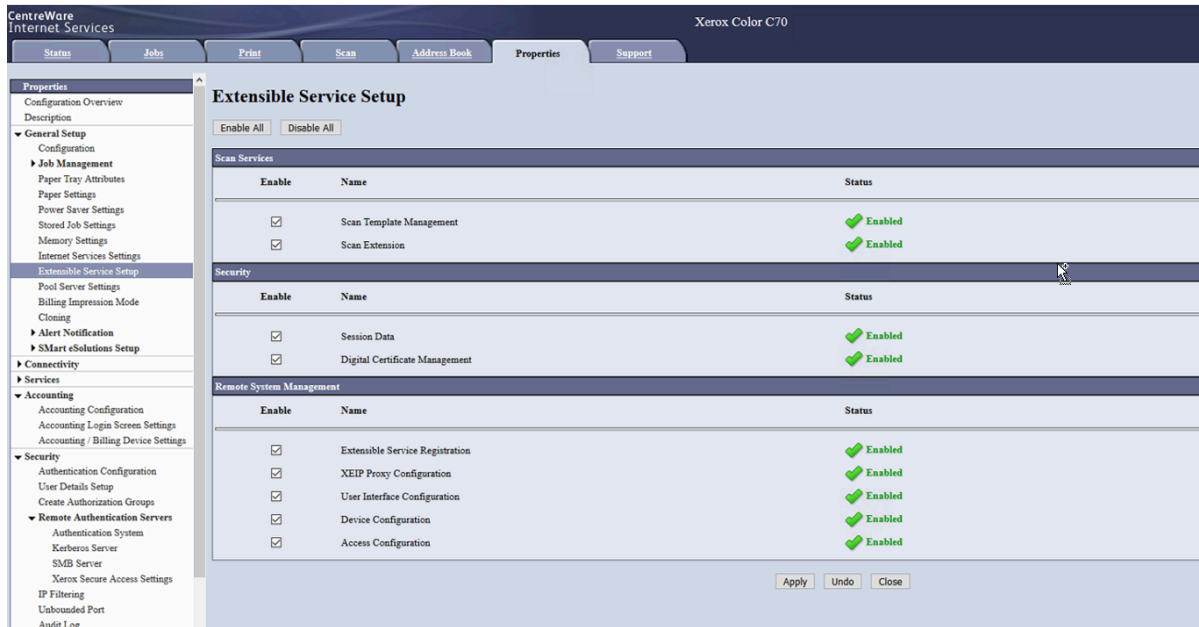
17. Open the Copitrak EIP GUI tool. In the main window of the Copitrak EIP GUI tool, select the device in the MFPs list, and click **Edit**.
    The **MFP Edit Form** appears.
18. In the **2. Web Services / DFI** section, click **Get Config** to verify the DFI connection.
19. In the **3. MFP CA MIBs** section, perform some advanced settings as below.
    • **Auth Protocol** - base: 101.136.1 - MIB Value: secure
    • **Auth Host Name** - base: 157.113.300 - MIB Value: blank
    • **Auth Host IP Addr** - base: 157.114.300 - MIB Value: Server IP : CA Port (For example: 192.168.5.200:44379)
      This is a required field.
    • **CA Server Path** - base: 157.118.300 - MIB Value: /SmarthAuthServerImpl.asmx
      This is a required field.
    • **CA Default Prompt** - base: 157.128.1 - MIB Value: blank
    • **CA Default Title** - base: 157.128.2 - MIB Value: Login to Copitrak
      This is a required field.
20. Click **Set All** to apply the settings on the MFP.
    A **Set All completed** message appears.

21. Click **OK** to complete the configurations.

Xerox PrimeLink devices

Before performing the configuration of Xerox PrimeLink devices, make sure that you complete the following:

- Enable **Extensible services browser** on the device.
- Install Xerox embedded application on the CSS server.
- All .config files are updated with SQL database connection string and CSS server IP address.

> ℹ️ Device will automatically reboot after some of the following steps.

1. Open a web browser and enter the device's IP address in the browser's address bar.
2. Log in as Administrator at the Xerox PrimeLink device's web administration page.
3. Navigate to **Security** > **Certificate Management**, and verify that the device has a valid certificate. Create one if it does not exist.
4. Navigate to **Properties** > **Connectivity** > **Protocols**, and ensure that HTTP protocol is enabled.
5. Navigate to **Properties** > **Security** > **Authentication Configuration**, and select **Xerox Secure Access** as the login type.
6. Navigate to **Properties** > **Security** > **Authentication Configuration** > **Device Access**, in the **Services Pathway** row, select **Locked** to lock the device, and then click **Apply**.

7. Under **Properties** > **Security** > **Authentication Configuration** > **Xerox Secure Access Configuration**, enable **Local Login** to make the keyboard available at the device.

8. Navigate to **Properties** > **Accounting** > **Accounting Configuration**. In the **Customize User Prompts** row, select **Display No Prompts** in the drop-down menu.

9. Run **eqsnmp.exe** located in **C:\ers\EmbeddedXerox** with the following sequence of parameters to finish configuring the Xerox PrimeLink device:

   • Set the IP Address and Port of the Auth server (CSS server):

   ```
   eqsnmp.exe -o set -c private -h [MFP IP Address] -x srv_addr -v [CSS
   Server IP Address].44379
   ```

   • Alternatively, set the Auth server by name and port instead of IP address:

   ```
   eqsnmp.exe -o set -c private -h [MFP IP Address] -x srv_host -v [CSS
   Server name].44379
   ```

   • Set the Path of the Auth server soap call (asmx in case you use CSS):

   ```
   eqsnmp.exe -o set -c private -h [MFP IP Address] -x srv_url -v "/
   SmartAuthServerImpl.asmx"
   ```

   • Turn on the Auth protocol for secure access:

   ```
   eqsnmp.exe -o set -c private -h [MFP IP Address] -x enable_56xx -v
   "secure"
   ```

   • Set Blocking screen title:

   ```
   eqsnmp.exe -o set -c private -h [MFP IP Address] -x default_title -v
   "Copitrak"
   ```

   • Set Blocking screen prompt:

   ```
   eqsnmp.exe -o set -c private -h [MFP IP Address] -x default_login -v
   "Please enter your ID"
   ```

Adding the MFP

1. In the main window of the Copitrak EIP GUI tool, click **Add** next to the **MFPs List** box on the right.
   The **Add MFP Form** window appears.

2. Enter the required MFP's IP, and click **Get S/N** to get the serial number.
   The serial number will automatically appear in the **Serial Number** field in the form. The **Unit ID** must be unique for each MFP and should be the same as the Unit ID of the MFP in DRS.

3. Click **OK**.

4. With your MFP selected, click **Edit** next to the **MFPs List**.
   The **MFP Edit Form** window appears.

5. Go to **2. Web Services / DFI** on the left side of the form.

6. Click **Get Config**.
   The text box will populate with the configuration from DFI.

7. Click **Save Config**.

8. Go to **4. MFP Accounting** on the right side of the form.

9. Click **Get Config**.
   The text box will populate with the configuration from the MFP.

10. Click **Save** at the top right side of the form.
11. Click **OK** in the dialog box.
12. Click **OK** in the **MFP Edit Form** window.

Registering CopitrakPsApp

1. Open the **Copitrak EIP GUI** application.
2. Navigate to **Setup Tools** > **Register PS App on MFP**.
3. In the **Registration Client** window, enter the Xerox MFP's IP address, and then enter the User Name and Password for the MFP. It is usually admin/1111.
4. Click **Connect**. Once the MFP is connected, its URL appears in the **Service Url** field.
5. Click **List Registrations** to view the list of applications on the Xerox MFP.
6. Click **Create New** to register the new CopitrakPsApp on the MFP.
   The **Registration Detail Form** window appears.
7. In the **Registration Detail Form**, click **Load** to select the registration templates for either Altalink or Versalink devices.
8. Select one of the XML files in **C:\ERS\EmbeddedXerox\ConfigXml** that corresponds to the Altalink or Versalink devices.

   You can use either of the templates for C70 devices. For PrimeLink devices, use Versalink template.

   Key values in the **Registration Detail Form** will be automatically filled in from selected XML file.
9. In the **Service Url** and **Description Url** fileds, replace "CSS-IP-Address" with the actual IP address of your CSS server where the embedded application for Xerox is installed.
   For example, on a CSS server at 10.17.6.71, the Service URL is `https://10.17.6.71:44366/Default.aspx`, and the Description URL is `https://10.17.6.71:44366/desc.xml`.

   > ⓘ Ensure that the port numbers for the corresponding Copitrak applications are correct:
   > - Copitrak**Ca**App: 44379
   > - Copitrak**Admin**: 44328
   > - Copitrak**Ps**App: 44313
   > - Copitrak**Altalink**PsApp: 44394
   > - Copitrak**Versalink**PsApp: 44366

10. When you finish the required data, click **Create**.
    After the Copitrak application has been successfully registered, it appears in the list at the bottom of the **Registration Client** window.
11. Select the registered application, and click **Update**.
12. Click **Update** in the **Registration Detail Form** dialog box.
13. In the **Registration Client** window, click **Close**.

Making the CopitrakPsApp default

1. In the main window of the **Copitrak EIP GUI** tool, go to **Setup Tools**, and select **Set PS App as Default on MFP** from the drop-down menu.
   The **UI Configuration Client** window appears.
2. In the **UI Configuration Client** window, under **Device Connection**, fill out the fields **DNS or IP**, **User Name**, and **Password**.
3. Click **Connect**.
   A **Services** button appears under the **Pathway** column.
4. Click **Services**.
   The list of applications available on the MFP appears.
5. Select the application that you want to set as default on the MFP.
   In this example, it is CopitrakVersalinkPsApp.
6. Click **Set Default Application**.
   Now the Copitrak Application is the default one on the MFP.
7. Verify that it is highlighted in the list as the default application, and then click **Close**.

Making applications default on the MFP Admin Portal

Besides making the app default in the Copitrak EIP GUI App, you can do the same on the device web administration portal.

Versalink devices

1. On the device web administration page, select **Apps** from the left control panel.
2. Click **Preferences** above the list of **Installed Apps**.
3. Select **Copitrak** in the **Walkup Screen** drop-down menu to ensure that once users log in, they see the selected app first.

Altalink devices

1. On the device web administration page, navigate to **Properties** > **General Setup** > **Entry Screen Defaults**.
2. In the **Default Walkup Screen** section, select **Copitrak App** from the drop-down menu.
3. Click **Apply**.

Starting the service

When all the above configuration steps are completed, go to the **Copitrak EIP GUI** app and click **Start** to get the service running. The app icons are also visible on the configured device if the service is not started, but the registered app will not function.

To end the service, click **Stop**.

Ensure proper functioning of Remote Session on the MFP

1. Uninstall the previously installed MFP on the CSS server.
2. Download and run the Xerox Global Driver (UNIV_5.585.13.0_PCL6_x64.exe) from https://www.support.xerox.com/en-us/product/altalink-b8000-series/downloads?language=en&platform=wins2016x64.
   It will automatically take you to control panel option where you can specify the IP address of the MFP.
3. Add the MFP via the Copitrak EIP GUI tool as in Adding the MFP.
   While adding the MFP, specify the name as **Xerox Global Print Driver PCL6**.
4. Once the MFP is added, associate it with XEROX Unit ID in **My Vault / Desktop** via **Configuration File Manager**.
5. Go to **Control Panel** > **System and Security** > **Windows Firewall** > **Advanced settings**.
6. Select **Inbound Rules**.
7. Under **Actions** > **Inbound Rules**, select **New Rule…**.
   The **New Inbound Rule Wizard** window appears.
8. Add the following ports in this rule for TCP/IP: 44379, 44366, 44394, 44313.
9. Ensure that the IP addresses point to the CSS server in the various sections of MFP page such as Xerox Secure Access Setup, LDAP servers, etc.
10. Ensure the correct path is set as **/SmartAuthServerImpl.asmx**.
11. Ensure that the Copitrak EIP GUI app is configured correctly for the MFP.
12. Before launching the remote session on the MFP page, make sure that you start **Add CA Session** on the Copitrak EIP GUI app via **Setup Tools** > **Add CA Sess for 127.0.0.1**.
13. Launch the Remote Session on the MFP page, and enter the User ID to see the icons for **Copy** and **DRS**.

Details of the terminal_XEROX_setup.xml file

This chapter describes the different settings in this xml file.

XML configuration file (terminal_XEROX_setup_date.xml)

If you want to make a change in this file, go to the Copitrak EIP GUI app, access the **MFP Edit Form** for each device, and repeat the **Get Config** and **Save Config** steps. For details, see Adding the MFP.

> ℹ Do not comment out lines in the XML configuration file. This may result in the file not being downloaded correctly to the MFP.

System settings

This section provides information on further system settings and configurations.

Main page configuration

```
<setting name="Main_Page_Title" value="Copitrak1>

<setting name="Main_Page_Enabled" value="Copier is Enabled"/>
```

CSS server communications configuration

All server configurations settings such as Host Server IP address and port numbers are set up in the configuration app. See Installation process for details.

Timeouts

There are no XML configuration file settings for user inactivity timeouts. These timeouts are described in Extend Time and Next buttons.

Currency

```
<setting name="Currency" value="USD"/>
```

Miscellaneous prompts and messages

```
<setting name="UnitID_Prompt" value="Unit ID"/>

<setting name="UnitIP_Prompt" value="Unit IP"/>

<setting name= "ServerHost_Prompt" value="Server Host"/>

<setting name="ServerPort_Prompt" value="Server Port"/>

<setting name="Server Connect" value="Connecting To ERS Server..."/>

<setting name="Server_Down value="ERS Server Unreachable."/>

<setting name= 'Server_Wait" value="Waiting For Server Respond... "/>

<setting name=' 'ErrorInvalidHost" value="Invalid Server Host"/>

<setting name=' 'ErrorInvalidPort" value="Invalid Server Port"/>
```

Copy and scan tracking

The Authorize Cost Recovery settings in the INI file are used to enable or to disable the tracking of copies, scans and faxes. Each Authorize setting activates or deactivates Cost Recovery for the specified device function.

- If the `Authorize function` setting value is set to Yes, cost recovery is turned on and the user must go through the Copitrak login procedure before completing that task (scanning a document). A transaction will be generated for each job.
- If the `Authorize function` setting value is set to No, the function operates normally and there will be no cost recovery. The user can access the MFP function directly without logging in and no transactions will be generated.

Scan settings tracking

To disable scan tracking, use the corresponding prompting settings available for your device. (See Accounting methods configuration for Altalink devices and Accounting methods configuration for Versalink devices).

Additionally, set the values of the following settings to No:

```
<setting name="Authorize_Scan" value="No"/>

<setting name="Scantrak" value="No"/>
```

Extend Time and Next buttons

> ⓘ The features described in this section are available in production releases v1.1.305.2 or later - for supported devices pre-dating Altalink and Versalink MFPs.

The **Additional Functions** hard key on the Xerox MFP displays a screen with **Extend Time and Next** buttons. This screen also displays a countdown. When expired, the user is automatically logged out. These features along with the interface screen can be enabled or disabled using the following XML configuration settings.

Timeout refresh config (to display by-the-second time counter):

```
<setting name="Enabled_ExtendTimeVisible" value="Yes"/>
```

By default, the user will see the **Extend Time and Next** buttons on a separate screen when the **Additional Functions** button is pressed. To automatically logout, the user without showing the extend screen must set this setting to **No**.

```
<setting name="Enabled_LogoutWhenReactivated" value="yes"/>
```

Next and Extend button settings:

```
<setting name="Enabled_ExtendButtonVisible" value="no"/>

<setting name="Enabled_NextButtonVisible" value="no"/>

<setting name="Button_Next" value="Next"!>

<setting name=' Button_Extend" value="Extend"/>

<setting name=' Button_Logout" value="Logout"/>
```

User validation

The `User Validation` value may be one of the following:
- **Absolute (CF)**: the user ID must be validated by ERS, switches to open validation if there is a loss of communications with the ERS server.
- **Absolute**: the user ID must be entered, and must be validated by ERS or it will be rejected.
- **Open**: the User ID must be entered, but is unconditionally accepted without checking `<setting name="User_Validation" value="Absolute"/>`.

Buttons names and User prompts

The "User_Prompt" is set on the Xerox device.

```
<setting name="User_Reject" value="Invalid User ID, Try Again."/>
```

User access denied groups

Not implemented in this release.

Lawyer validation

A dialog box for requesting the `Lawyer ID` can be activated by setting the `Lawyer_Default` value to anything other than Default Lawyer. The selected value appears as default text in the dialog box.

```
<setting name="Lawyer_Validation" value="Absolute"/> Absolute or Open

<setting name="Lawyer_Prompt" value="Please Enter Lawyer Number"/>

<setting name="Lawyer_Reject" value="Invalid Lawyer Number, Try Again."/>

<setting name="Lawyer_AssumeUser" value="No"/>

<setting name="Title_LawyerID" value="Lawyer Number"/>
```

A typical 'no lawyer' validation configuration can be:

```
<setting name="Lawyer_Validation" value="Absolute(CF)"/>

<setting name="Lawyer_Default" value="Default Lawyers"/>

<setting name="Lawyer_AssumeUser" value="No"/>
```

To force validation, consider the following:

1. `Lawyer_Default` cannot be `Default Lawyer`
2. `Lawyer_AssumeUser` cannot be `Yes`

Recommended configuration:

```
<setting name="Lawyer_Validation" value="Absolute(CF)1>

<setting name="Lawyer_Default" value="Default Lawyer - no"/>

<setting name="Lawyer_AssumeUser" value="No"/>
```

Account validation and Account code entry

The `Account_Validation` value can be:
- **Absolute (CF)**: the account number must be entered and must be validated by ERS, switches to open account validation if there is a loss of communications with the ER5 server.
- **Absolute**: the account number must be entered and must be validated by ERS.
- **Open**: the account number is unconditionally accepted.

```
<setting name="Account_Validation" value="Absolute"/>
<setting name="Account_Prompt" value="Please Enter Account Code"/>
<setting name="Account_Reject" value="Invalid Account Code, Try Again."/>
<setting name="Account_Default" value="Default Account"/>
<setting name="Account_Override" value="Yes"/>
```

Buttons names and User prompts

```
<setting name="Button_Override" value="Override"/>

<setting name="Search_Prompt" value="Please Enter Super-Search Term..."/>

<setting name="Button_Favorites" value="Favorites"/>

<setting name="Button_Search" value="Search"/>

<setting name="Result_Success" value="Success"/>

<setting name="Result_Failure" value="Failure"/>

<setting name="Title_AccountID" value="Account Code"/>

<setting name="Title_Search" value="Search"/>

<setting name="Title_Last" value="Last Jobs"/>

<setting name="Title_Favorites" value="Favorite Jobs"/>
```

Job description entry

A description for the job can be requested when the user opens the **Description** window and after the input of a non-billable account during login.

`Description_Displayed` setting. The full set of values is:

Yes - display the description page for NB accounts only.

No - do not display the description page.

Always - display the description page for all (NB and non-N3) accounts.

```
<setting name="Description_Displayed" value="No"/>
```

If `Description_Displayed` is set to **Yes**, the software will check that the description is not empty.

```
<setting name="Description_Validation" value="No"/>

<setting name="Description_Prompt" value="Enter Description"/>

<setting name="Description_Reject" value="lnvalid Description, Try Again."/>

<setting name="Title_Description" value="Description"/>
```

Other prompts, buttons and messages

```
<setting name="Button_Last" value="Last"/>

<setting name="Button_Enter" value="Enter"/>

<setting name="Button_End" value="End"/>
```

Color detection and page sizes

The features described in this section are available in production releases v1.1.305.2 or later.

```
<setting name="Copy_Default value="COPY_DEFAULT"/>

<setting name="Copy_Type1" value="BW-LETTER"/>

<setting name="Copy_Type2" value="CLR-MONO-LETTER"/>

<setting name="Copy_Type3" value="CLR-TWIN-LETTER"/>

<setting name=Copy_Type4" value="CLR-FULL-LETTER"/>

<setting name="Copy_Type5" value="BW-LEGAL"/>

<setting name="Copy_Type6" value="CLR-MONO-LEGAL"/>

<setting name="Copy_Type7" value="CLR-TWIN-LEGAL"/>

<setting name="Copy_Type8" value="CLR-FULL-LEGAL"/>

<setting name="Copy_Type9" value="BW-LEDGER"/>

<setting name="Copy_Type10" value="CLR-MONO-LEDGER"/>

<setting name="Copy_Type11" value="CLR-TWIN-LEDGER"/>

<setting name="Copy_Type12" value="CLR-FULL-LEDGER"/>

<setting name="Copy_Type13:38,CHARGE_BLACK" value="BW"/>

<setting name="Copy_Type14:133,CHARGE_BLACK" value="SPECIAL2"/>


<setting name="Scan_Default ' value="SCAN_DEFAULT"/>

<setting name="Scan_Type1" value="SCAN-BW-LET"/>

<setting name="Scan_Type2" value="SCAN-MCLR-LET"/>

<setting name="Scan_Type3" value="SCAN-TCLR-LET"/>

<setting name="Scan_Type4" value="SCAN-FCLR-LET"/>

<setting name="Scan_Type5" value="SCAN-BW-LEGAL"/>
```

```
<setting name="Scan_Type6" value="SCAN-MCLR-LEG"/>

<setting name="Scan_Type7" value=SCAN-TCLR-LEG"/>

<setting name="Scan_Type8" value="SCAN-FCLR-LEG"/>

<setting name="Scan_Type9" value="SCAN-BW-LED"/>

<setting name="Scan_Type10" value="SCAN-MCLR-LED"/>

<setting name="Scan_Type11" value="SCAN-TCLR-LED"/>

<setting name="Scan_Type12" value="SCAN-FCLR-LED"/>
```