SIMPLIFIED SECURITY COMPLIANCE AT YOUR FINGERTIPS

A Quick Start Guide to Custom Administrator

xerox

Contents

1.   Introduction

The following instructions enable a device administrator to create Custom Administrator roles, assign users to those roles, and select from a list of permissible actions that the Custom Admin will have on both Xerox® ConnectKey® Technology-enabled Xerox® AltaLink® and certain VersaLink® Multifunction Printers.

Custom Administrators have rights that are determined by the System Administrator. The Custom Admin is allowed to create/manage logged-in user roles, but they cannot create/modify roles with admin permissions or device management roles.

You can access the administration and configuration settings from the *Tools* tab on the control panel or from the *Properties* tab in Xerox® Embedded Web Server. The control panel consists of a touch screen and buttons you press to control the functions available on the printer.

Xerox® Embedded Web Server is the administration and configuration software installed on the Xerox® Printer. It allows you to configure and administer the printer from a web browser.

The administrator password (the default option is the device serial number) is required when accessing locked settings in Xerox® Embedded Web Server or at the control panel. Most printer models have a default configuration that restricts access to some settings. Access is restricted for settings on the *Properties* tab in Xerox® Embedded Web Server, and settings on the Tools tab on the control panel touch screen.

2.   Procedure

Accessing the control panel as a System Administrator

1. On the printer's control panel, press the Log In/Out button.
2. Type **admin** and touch **Next**.
3. Type the administrator password (the default option is the device serial number), then touch Done.

Accessing Xerox® Embedded Web Server as a System Administrator

Note: Before you begin:

*   Locate your printer's IP address using the configuration report. For details, see *Printing the configuration report*.
*   Ensure that TCP/IP and HTTP are enabled. If you have disabled either of these protocols, enable them at the control panel before accessing Xerox® Embedded Web Server.

Note:

For devices that are not connected to the network, connect a .com capable computer to the device via a crossover cable and proceed with the instructions below.

To log in to Xerox® Embedded Web Server as the administrator:

1. Open a web browser on your computer. In the address field, type the **IP address** of the printer, then press **Enter** or **Return**.
2. Click **Login**, located on the top right of the page.
3. Under User ID, type **admin**.
4. Under password, type the administrator **password** (the default option is the device serial number).
5. Click **Login**.

Printing the configuration report

The configuration report lists all current settings of the printer. This report prints at startup by default.

1. In Xerox® Embedded Web Server, navigate to the **Configuration Report**.
2. To print the report, click Print Configuration Page.

Install firmware containing the Custom Administrator feature

The following procedure assumes the device administrator has downloaded and installed the firmware release, which contains the Custom Administrator functionality.

To determine if your MFP contains the Custom Administrator functionality, check the printed configuration report to ensure the installed firmware is at least 100.xxx.037.0383x for Altalink® MFPs. If it is not, obtain the firmware listed below, and follow the installation process.

Xerox® Products	System Software
Xerox® AltaLink® B8045/55/65/75/90	100.008.037.03831 or higher
Xerox® AltaLink® C8030/35	100.001.037.03830 or higher
Xerox® AltaLink® C8045/55	100.002.037.03830 or higher
Xerox® AltaLink® C8070	100.003.037.03830 or higher
Xerox® AltaLink® B8145/B8155/B8170	Initial Launch
Xerox® AltaLink® C8130/C8135/C8045/C8155/C8170	Initial Launch
Xerox® VersaLink® B415/B625	Initial Launch
Xerox® VersaLink® C415/C625	Initial Launch

Create a new Custom Administrator role

Note

The Custom Admin role administration can only be performed via the Web UI. Creating a Custom Admin role will delete the default **logged-in user** Role if no other custom roles have been previously created. See section 8.

To create a new Custom Admin role:

1. Login to the machine as **admin.**
2. Select **Properties** > **Login/Permissions/Accounting** > **User Permissions**.
3. In the User Permission Roles row, select Edit.
4. On the User Permission Roles page, select the Device Management tab.
5. Under the Device Management tab, select **Add New Role**.
   a) Type in a **Role Name** and **Description** (e.g., Custom Admin Role, some settings are read-only).
   b) Select **Create**.

Assign permissions to the Custom Administrator role

1. On the *Add Management Role* page, select the *Properties* tab.
2. If **Forbid All** is selected, this role will not have the rights to change any of these settings.
3. To give users in this role the rights to change a particular setting, set the pulldown in the status column to **Allowed**.

Assign users to the Custom Administrator role

1. On the *Add Management Role* page, select the *Assign Users* to Role tab.
2. Select **Add New User**.
3. On the Add New User page, define the corporate-wide **user** and **password**.
   a) Type in a **User Name** and **Friendly Name** (e.g., healthadmin, healthadmin).
   b) Type in a **New Password** and retype the password (e.g., 1111).
   c) Select **Save**.
4. On the *Add Management Role* page, select the *Assign Users to Role* tab:
   a) Select the check box in front of the new user (e.g., healthadmin).
   b) Select **Apply**.

Creating a logged-in user role (optional)

1. Login to the machine as *Admin* or *Custom Admin*.
2. Select **Properties > Login/Permissions/Accounting > User Permissions**.
3. In the User Permission Roles row, select **Edit**.
4. On the User Permission Roles page, select the Logged-in Users tab.
5. Under the Device Management tab, select **Add New Role**.
   a) Type in **Role Name** - "Logged-in User" and **Description** - "Allow logged-in users unrestricted access to all features except Tools."
   b) Select **Create**.
   c) Select **All Logged-in Users** radio button and **Apply**.
   d) Under the Services & Tools Tab, ensure you select **Allow access to everything except Tools (Standard Access)** is selected. Click **Apply**.
   e) Under the Web UI Tab, ensure you select **Allow access to all web pages except Properties (Standard Access)** is selected. Click **Apply**.

3.   Support information

The customer support forum can be found at http://forum.support.xerox.com

Contact us or our partners about our products, supplies, services, support, and programs. Our extensive network of representatives can help you find the information you need. https://www.xerox.com/about-xerox/contact-us

4. Supported Multifunction Printers (MFPs)

The following is a list of MFPs that support the use of the Xerox® Lockdown Security Solution:

1. Xerox® ConnectKey® Technology-enabled Xerox® AltaLink® B8000 Series high-volume MFPs.
2. Xerox® ConnectKey® Technology-enabled Xerox® AltaLink® C8000 Series high-volume MFPs.
3. Xerox® ConnectKey® Technology-enabled Xerox® AltaLink® B8100 Series high-volume MFPs.
4. Xerox® ConnectKey® Technology-enabled Xerox® AltaLink® C8100 Series high-volume MFPs.
5. Xerox® ConnectKey® Technology-enabled Xerox® VersaLink® B415, B625 MFPs.
6. Xerox® ConnectKey® Technology-enabled Xerox® VersaLink® C415, C625 Color MFPs.