VERSION 1.5
SEPTEMBER
2019

Common Access Card for Xerox® VersaLink® Printers

System Configuration Guide

Document Version 1.3 November 2017

BR22729

Contents

1 Introduction

Purpose

The Common Access Card (CAC) solution brings an advanced level of security to sensitive information. Using the CAC, organizations can restrict access to the walk-up features of a Xerox® device. This ensures that only authorized users are able to copy, scan, email and fax information.

Target Audience

This document is a guideline for the configuration and set up of the CAC solution.

NOTE

Not all options listed are supported on all printers. Some options apply only to a specific printer model, configuration, operating system, network, or print driver type.

Disclaimer

The information in this document is provided without warranty of any kind. In no event shall Xerox be liable for any damages whatsoever resulting from user use or disregard of the information provided in this document, including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox has been advised of the possibility of such damages.

2 Prerequisites

To ensure the successful configuration and subsequent operation of the device, the following conditions are required:

- Existing and properly operating Transmission Control Protocol/Internet Protocol (TCP/IP) network infrastructure
- Existing and properly operating Public Key Infrastructure
- Certificate-based authentication server and valid certificate chains for clients
- Supported USB Card Reader
- Supported Smart Card
- Administration rights to configure a Xerox® VersaLink® device
- The VersaLink device is connected to the TCP/IP network with a valid IPv4 address
- A workstation with a modern browser is connected to the same TCP/IP network with a valid IPv4 address

NOTE

3 DPI LOI CAC Installation Guide Instructions Reference

The United States Air Force Digital Printing and Imaging (DPI) team has created a formal Letter of Instruction (LOI) document regarding the installation of CAC on MFP products like VersaLink.

This section relates the LOI to the contents of this document,

The listed sections describe how this information can be configured on the VersaLink device.

Your installation may not require setting all the below values.

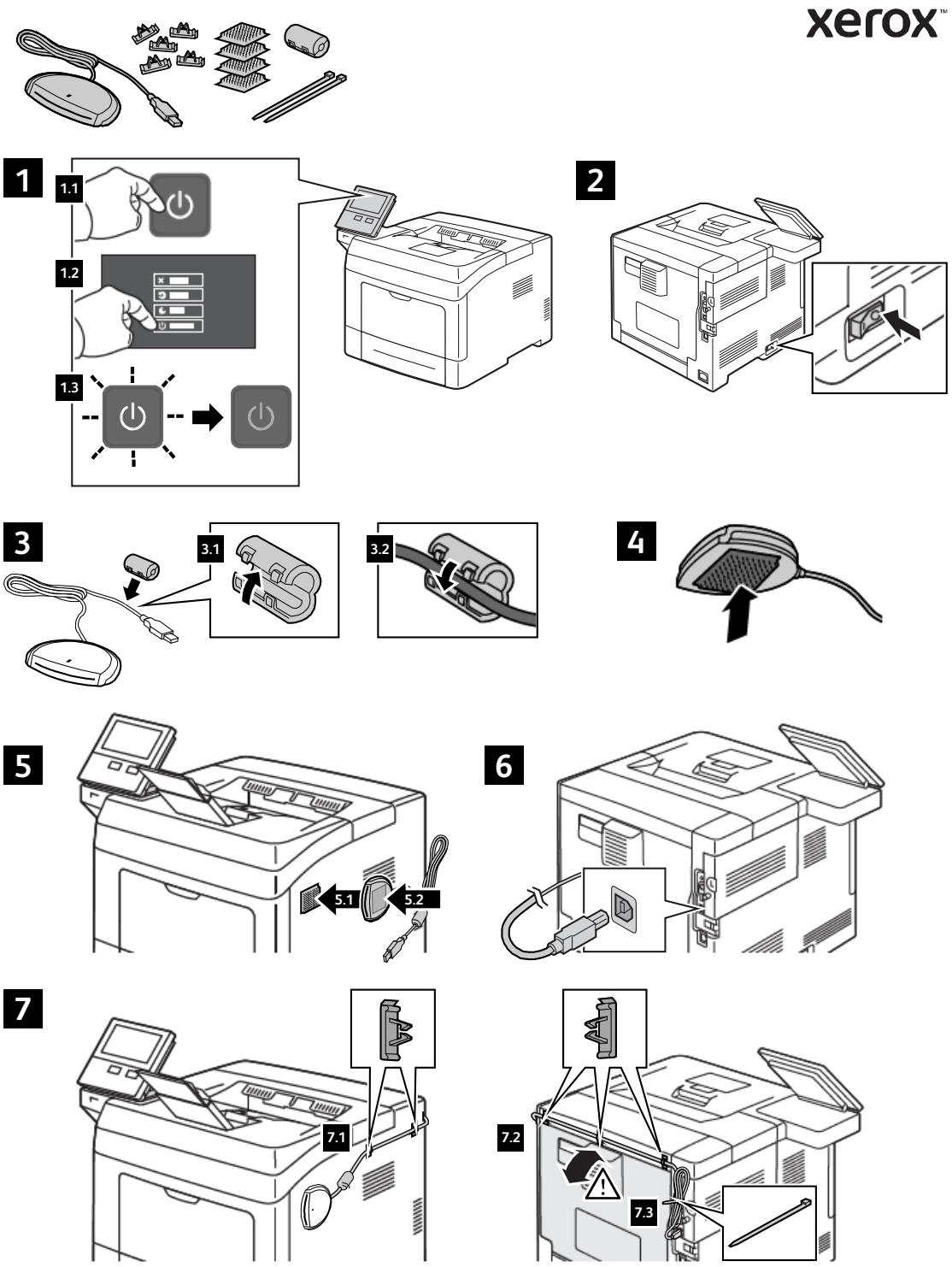
1) The type of information to be gathered before installation begins, such as:
   a) DNS Server Primary and Secondary **(Section 7.0 7-7)**
   b) Wins Server **(Section 7.0 7-7)**
   c) Domain Controller Network Addresses **(Section 8.0 8-19)**
   d) Domain Controller Certificates Root/User/Device **(Section 8.0 8-13)**
   e) LDAP Active Directory Network Address **(Section 7.0 7-8)**
   f) OCSP Network/Server information **(Section 7.0 7-8)**
   g) SMTP (scan to email) **(Section 9.0 9-22)**
   h) Kerberos Configurations **(Section 8.0 8-20)**
   i) Root Certificates **(Section 8.0 8-14)**
   j) Add any others not noted in the list

2) Steps the administrator should follow to complete installation and configuration of the MFP-CAC, based on the following:
   a) Using installation information from #1 above, identify the configuration steps
   b) Identify the Active Directory configuration within the MFP (ex: LDAP, Kerberos, etc) **(Section 9.0 9-21)**
   c) Identify how Certificates should be retrieved and installed **(Section 8.0 8-13)**
   d) Identify how SMTP (Scan to Email or Scan to File Share) should be configured **(Section 9.0 9-21)**
   e) Identify any additional steps needed to complete the installation **(Section 9.0 9-21)**

3) Other user administrator settings which should be considered after installation, based on the following:
   a) Identify how administrators should lock the device and require CAC Card/Pin Authentication before permitting access to scanning/printing features **(Section 9.0 9-21)**
   b) Identify how administrators should set the device to lock and clear user credentials after CAC Removal **(Section 9.0 9-21)**
   c) Identify any additional administrative settings needed to complete the installation **(Section 9.0 9-21)**

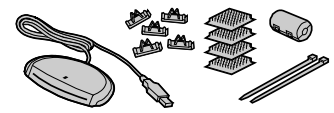
4 Hardware Installation

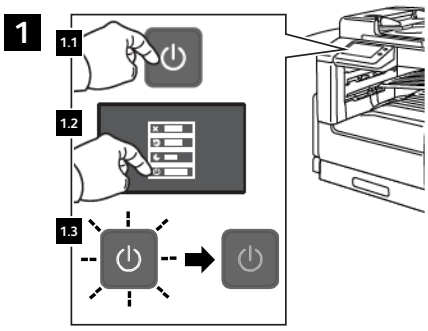
Refer to the diagram that most closely matches your device.

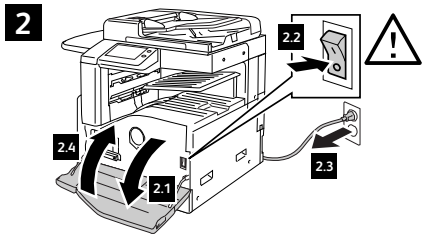


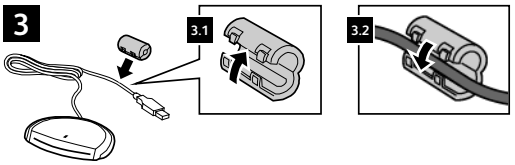
607E21290 Rev F

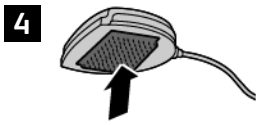
www.xerox.com/support

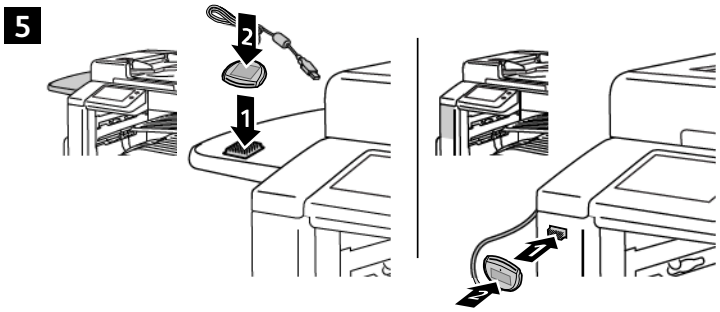










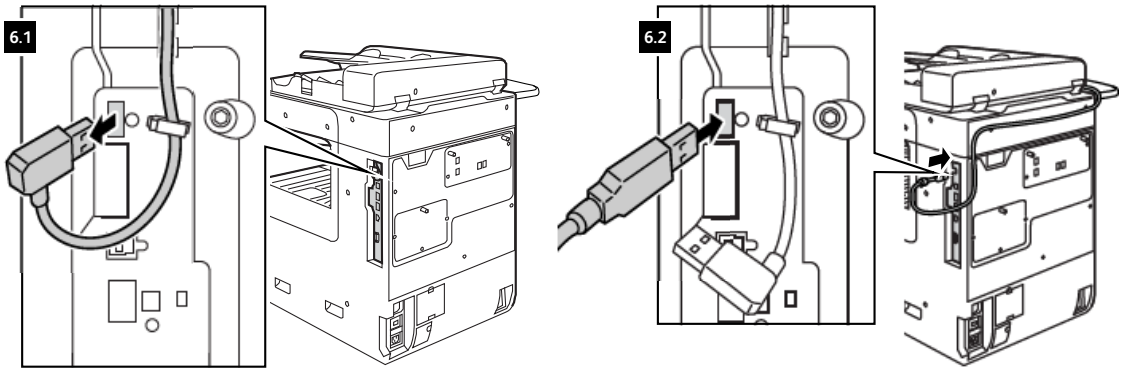


6

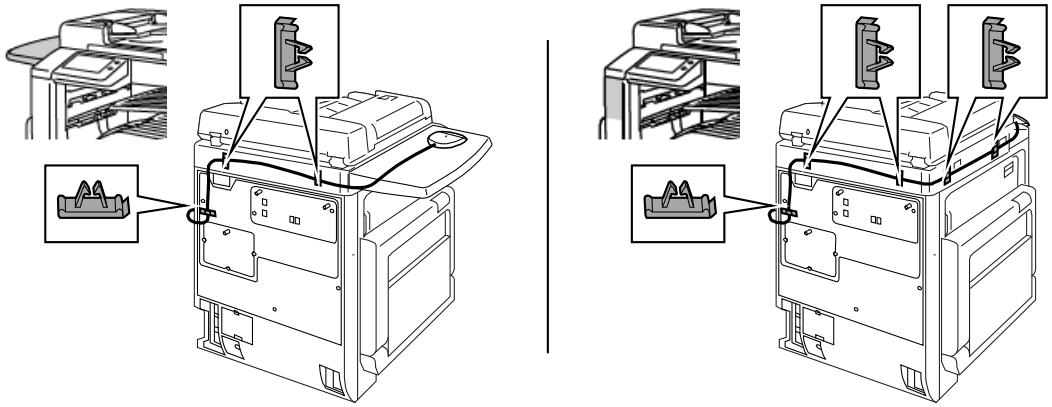
607E21040 Rev B

www.xerox.com/support

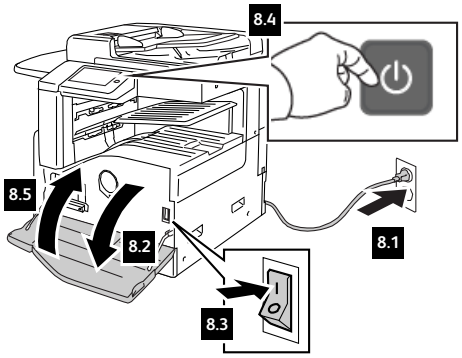
6



7



8



xerox™

5 Feature Overview

S/MIME

This product offers Secure/Multipurpose Internet Mail Extensions (S/MIME) that allows a System Administrator to configure the device to provide digital signature and encryption functionality, which requires the use of PKI certificates.

Secure Print Hold and Release

This product offers Secure Print Hold and Release that allows a System Administrator to configure the device to hide print jobs from unauthorized users, and only reveal and allow subsequent printing by users authenticated to the system.

NOTES

- Only the V3 Xerox® Print drivers for VersaLink products are CAC-enabled.
- Support for V4 Xerox® Print drivers and support for the Xerox® Global Print Driver® and Xerox® Mobile Express Driver® are not available at this time. For more information about supported print drivers, refer to Section 9 of this document.

6 Supported Card Readers

For each device that you want to configure to support the CAC, purchase a USB card reader. The following card readers are compatible with the CAC solution and your Xerox® VersaLink device:

- SCM SCR3310 version 2.0
- SCM SCR331
- NTTCom SCR3310-NTTCom
- Gemalto PC Twin
- Panasonic ZU-9PS

NOTES

- Other Chip Card Interface Device (CCID)-compliant card readers may function with the CAC solution for your VersaLink device, but other CCID card readers have not been validated.
- Certain card reader manufacturers may introduce hardware revisions that prevent card readers from working correctly.

7 Supported Card Types

The following card types are supported for use with your Xerox® VersaLink device and Common Access Card solution:

- Any Integrated Circuit (IC) card officially distributed by the U.S. Department of Defense
- CAC, Personal Identity Verification (PIV) and CAC 144K-compatible IC Smart Cards
- Gemalto Top DL GX4 144K used in system validation.

8 Additional Optional System Configuration

These steps are not required to enable CAC/PIV on VersaLink but may be required to integrate the device into your network environment.

Setting the DNS Server

The DNS server can be set manually using the following process:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **Connectivity**, then select **Ethernet**.
7. Select **DNS**, then **Edit**.
8. Disable **Use DHCP** or **Use DHCPv6-lite** or both depending on your network requirements.
9. Enter primary and alternate DNS servers for IPv4 and IPv6 as required.
10. To save your changes select **OK.**
11. To restart the device and apply the changes, click **Restart Now**.

Setting the WINS Server

The WINS server can be set manually using the following process:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **Connectivity**, then select **SMB**.
7. Disable **Wins Server Address Acquisition by DHCP.**
8. Enter primary and secondary WINS servers.
9. To save your changes select **OK.**
10. To restart the device and apply the changes, click **Restart Now**.

Configuring LDAP

If you have been directed to configure LDAP by a network administrator you can do so using the following process:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **Connectivity**, then select **LDAP**.
7. Enter the IP Address or hostname of the primary and optional backup LDAP servers.
8. Under **Advanced Settings** enter the **Search Directory Root** and the credentials required to bind to the LDAP server.
9. To save your changes select **OK.**
10. To restart the device and apply the changes, click **Restart Now**.

NOTE

If the device is configured for LDAP and the installation requirements have changed you can disable LDAP with the following procedure performed at the LUI:

1. Login to the device as Admin through the Local User Interface.
2. Select **Device** and then **Connectivity**.
3. Select **LDAP** and then **Enter Server Address.**
4. Clear the value from **Enter Server Address** and select **Ok.**
5. When prompted select **Turn Off**.
6. Select the **Home** button.
7. When prompted select **Restart Now.**

Configuring OCSP

If you have been directed to configure OCSP by a network administrator you can do so using the following process:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then select **Security**.
7. Select **Certificate Revocation Settings.**
8. Set **Level of Certificate Verification** to **High**.
9. Set **Certificate Revocation Check** to **Check by OCSP**.

10. Set **Send Query to Responder With** to **URL as Specified by Administrator**.
11. Enter your OCSP URL in the **Responder URL** field.
12. To save your changes select **OK.**
13. To restart the device and apply the changes, click **Restart Now**.

9 System Configuration

System Configuration Checklist

CAUTION

Complete the following steps in the order listed. Failure to do so can result in system software failure.

Status	System Configuration Step
☐	1. Accessing the Embedded Web Server
☐	2. Changing the Admin Password
☐	3. Enabling HTTPS
☐	4. Importing Root and Intermediate Certificates
☐	5. Enabling SNTP
☐	6. Enabling Plug-In Feature
☐	7. Downloading the CCID Terminal Service Plug-in File
☐	8. Checking the CCID Terminal Service Plug-In Version Number
☐	9. Updating the CCID Terminal Service Plug-in
☐	10. Deactivating and Activating the CCID Terminal Service Plug-In
☐	11. Installing an Updated CCID Terminal Service Plug-in File
☐	12. Enabling the CAC&PIV Smart Card Service Plug-in
☐	13. Changing system to Smart Card Authentication
☐	14. Enabling Smart Card Certificate Validation

Accessing the Embedded Web Server

You can configure the VersaLink device from the Embedded Web Server, using the IP address or the Domain Name System (DNS)-resolvable host name for the device.

When the device is first powered on in the default configuration, a Startup Page report prints with details about the device. The Startup Page includes the IPv4 address of the system on the TCP/IP network. Record the IP address for later use.

NOTE

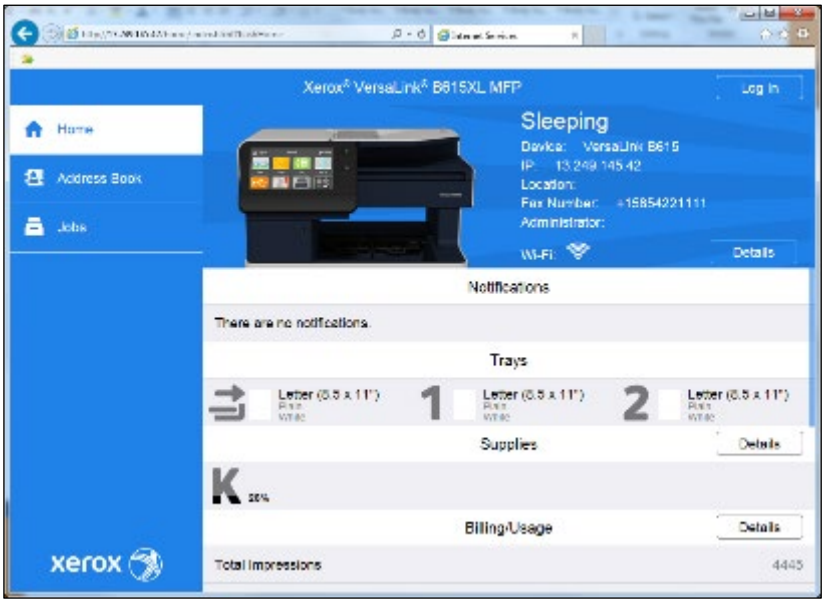
If the device is not configured to print a Startup Page, you can determine the IPv4 address of the system at the device control panel. At the device control panel, press the **Home** button, then touch **Device** > **About**. The IPv4 address is located under the Network heading.

To access the Embedded Web Server:

1. At your computer, open a new browser window.
2. In the address bar, enter the IP address or DNS-resolvable device host name, then press **Enter**.

   In this example, the IP address of the device being accessed is 13.249.145.42. The IP address of your device will be different.

3. The Embedded Web Server Home page for your device appears. In this example, the device being accessed is the VersaLink B615XL Multifunction Printer.



NOTE

The appearance of the Embedded Web Server Home page varies by product model, browser, and configuration.

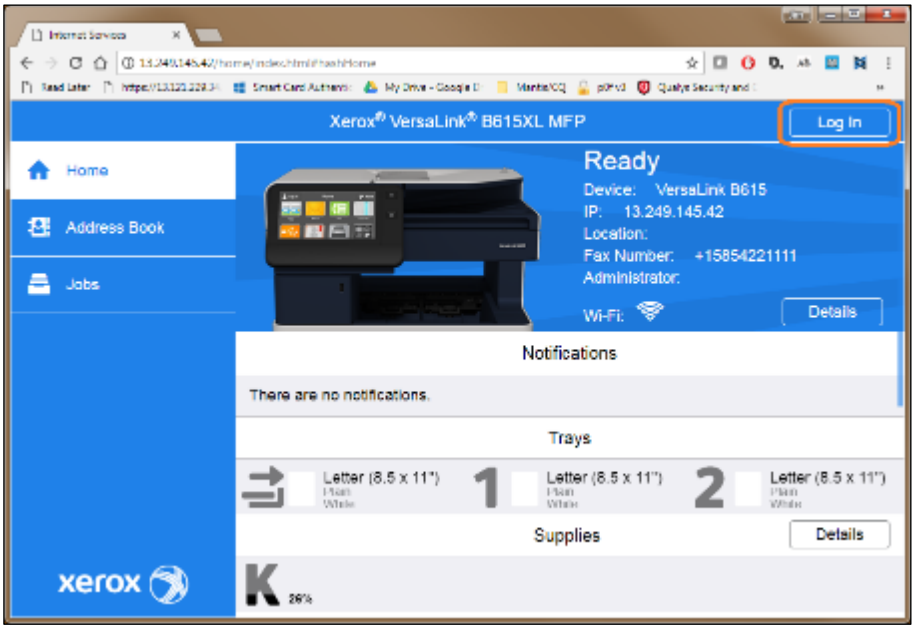
Changing the Admin Password

To protect the device against unauthorized changes, it is important to change the admin password for the device.

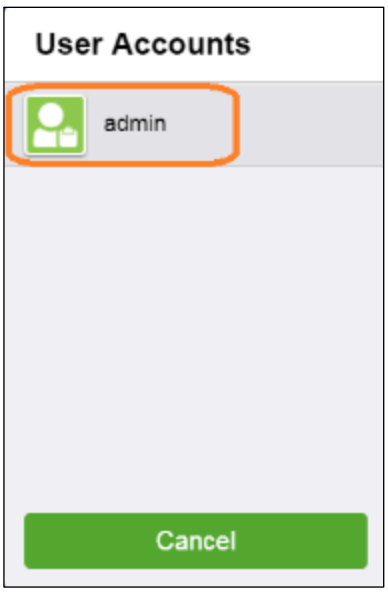
To change the admin password, log into the Embedded Web Server using the default System Administrator login credentials.

To log in as admin:

1. At your computer, open a new browser window.
2. In the address bar, enter the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.



4. From the list of user accounts, select **Admin**.



5. In the Password Required field, type **1111**, then click **Log In**.

To change the admin password:

1. On the Embedded Web Server Home page, click **Permissions**, then click **Login/Logout Settings**.
2. Click **Change Password**.
3. Enter the old Admin password, then enter the new password twice.
4. Click **OK**.

NOTE

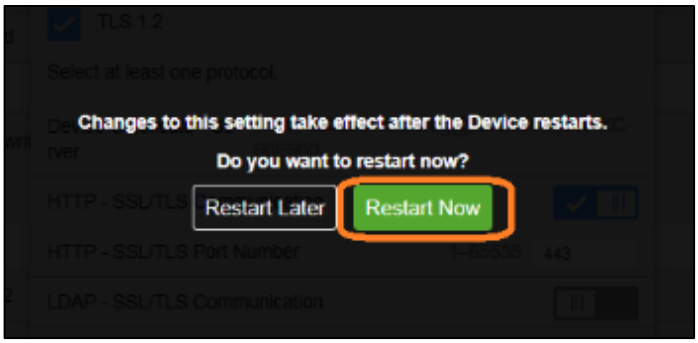
Ensure that you record the new admin password in a safe location for future use.

Enabling HTTPS

Enabling HTTPS is a requirement for the CAC configuration process. HTTPS ensures that the CAC certificates are encrypted and secured before being transmitted over the network. Without HTTPS, the certificate credentials are at risk of being stolen by an unauthorized observer.

To enable HTTPS in the Embedded Web Server:

1. At your computer, open a new browser window.
2. In the address bar, enter the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*. Click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then click **Security**.
7. For Network Security, select **SSL/TLS Settings**.
8. To enable HTTPS, from the list, select **HTTP – SSL/TLS Communication**, then click the toggle button.
9. To save your changes, click **OK**.
10. To restart the device and apply the changes, click **Restart Now**.



NOTE

After restarting the device, your browser may be unable to connect to the device over HTTP.

To confirm that HTTPS operation is enabled:

1. At your computer, open a new browser window.

2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. Accept the self-signed certificate of the device.

   NOTE

   The steps required to accept a self-signed certificate vary depending on your browser. For instructions on how to complete the certificate-importing process for your specific browser, contact your technical support team.

Importing Root and Intermediate Certificates

Certificate Requirements

- Only RSA Public Key Algorithm is supported
- Issuer DN 255 or fewer characters (UTF-8)
- Length of Public Key: 512, 1024, 2048, or 4096
- Supported Signature Algorithm: SHA, SHA224, SHA256, SHA384, or SHA512
- Formats: Public Key Cryptography standards (PKCS) #7 (.p7b,.p7c) or Distinguished Encoding Rules (DER) (.cer)

To import root and intermediate certificates:

14. At your computer, open a new browser window.
15. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
16. On the Embedded Web Server Home page, click **Log In**.
17. From the list of user accounts, select **Admin**.
18. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
19. On the Embedded Web Server Home page, click **System**, then select **Security**.
20. For Certificates, select **Security Certificates**.
21. From the Device Certificates menu, select **Trusted Root CA Certificates**, then click **Import**.
22. Click **Select**, then browse to the relevant .CER Certificate file. Leave the password field blank unless required by the certificate, then click **Import**.

    NOTE

    To import Intermediate Certificates, repeat steps 8 and 9. From the Device Certificates menu, for step 8, select **Intermediate CA Certificates**.

Enabling SNTP

Enabling Simple Network Time Protocol (SNTP) is a requirement for the CAC configuration process. SNTP ensures that the device system time is consistent with the authorization server. Failure to configure SNTP correctly can result in time-skew-related login failures.

To enable SNTP:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then select **Date & Time**.
7. For SNTP Settings, click **Edit**.
8. To enable Time Server Synchronization, click the toggle button.
9. Enter the customer-specified Time Server Address, then click **OK**.

   NOTE

   CAC Authentication against a Kerberos server is sensitive to time differences between the client and the server. It is critical that the correct time server for the customer environment is used by the device.
10. To restart the device and apply the changes, click **Restart Now.**

Enabling the Plug-In Feature

Xerox® VersaLink products allow customers to add functionality through various software, called plug-ins, which are obtained and installed after purchasing the device. Plug-ins allow the device to interface with a specific type of smartcard, such as CAC and or PIV, compared to .NET and other types of mag-stripe or proximity cards. Enable the Plug-In feature, then install the plug-in.

To enable the Plug-In feature in the Embedded Web Server:

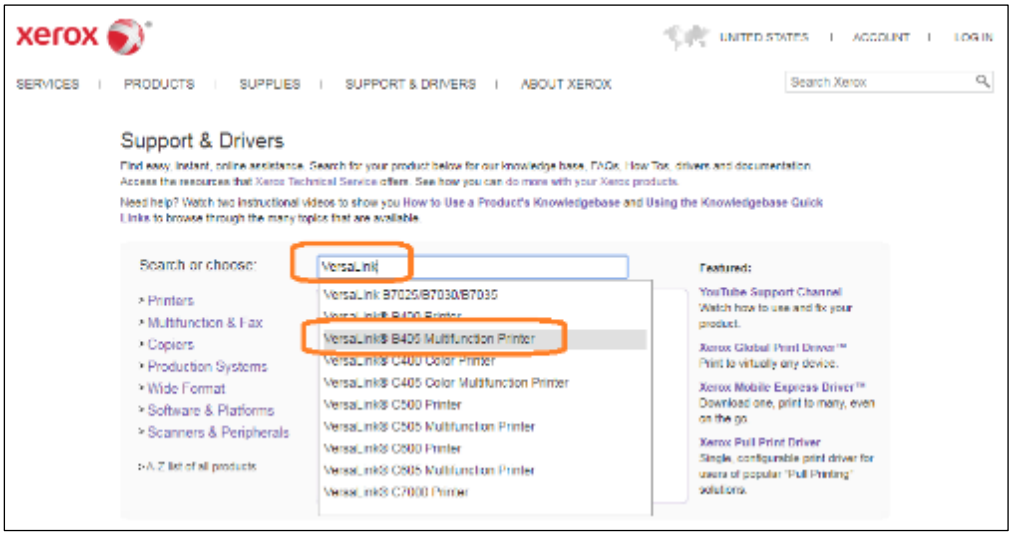
1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then select **Plug-In Settings**.
7. To enable the plug-in feature, click the toggle button.
8. To save the changes, click **Close**.
9. To restart the device and apply the changes, click **Restart Now.**

Downloading the CCID Terminal Service Plug-in File

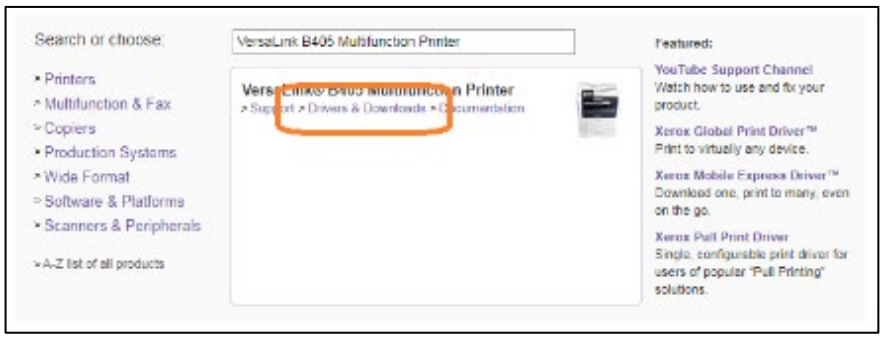
To connect the printer to an IC card reader, download and install the CCID Terminal Service plug-in.

To download the CCID Terminal Service plug-in file:

1. At your computer, open a new browser window, then navigate to http://www.xerox.com/drivers.
2. In the search or choose field, type **VersaLink**. From the list, select the required model. In this example, the device being updated is a Xerox® VersaLink® B405 Multifunction Printer.



3. Locate your device, then click **Drivers & Downloads**.



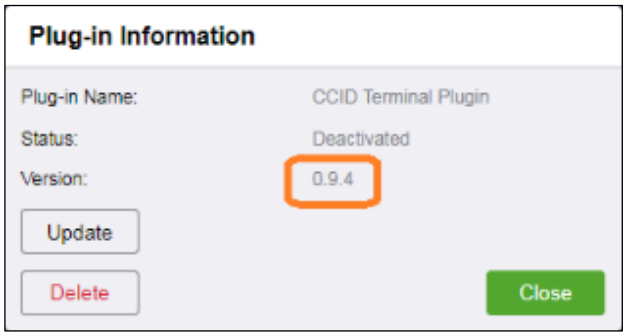
4. For Firmware, select **Card Reader Plug-ins**.
5. Download the .ZIP file. Extract the .ZIP file contents to an easily accessible location on your local system.
6. Open the extracted folder, then locate the file named **CCID_Terminal_Plug-in_vX.X.X_sig.jar**.
7. Record the version number of the file for later use. For example, the version number of **CCID_Terminal_Plug-in_v0.9.5_sig.jar** is 0.9.5.

Checking the CCID Terminal Service Plug-In Version Number

Before updating the plug-in on the device, check the version number of the newly downloaded plug-in. The newly downloaded plug-in version number must be higher than the plug-in version currently installed on the device.

To compare the version number of the newly downloaded plug-in against the version currently installed on the device:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then select **Plug-In Settings**.
7. Select **CCID Terminal Plug-in**.
8. Click **Details**.
9. Compare the version number of the currently installed plug-in with the version number of the newly downloaded file, as recorded in step 7 of *Downloading the CCID Terminal Service Plug-in File*. In this example, the version number of the plug-in currently installed is 0.9.4.



   - If the version number of the currently installed plug-in is **the same** or **higher** than that of the newly downloaded file, no further changes are required. Skip to the *Enabling the CAC&PIV Smartcard Service Plug-in* section in this guide.
   - If the version number of the currently installed plug-in is **lower** than that of the newly downloaded file, complete all remaining tasks in this guide.

Updating the CCID Terminal Service Plug-in

To update the CCID Terminal plug-in, change the status of the plug-in to deactivated. After you update the CCID Terminal Plug-in, re-activate it.

- To deactivate the plug-in, refer to *Deactivating and Activating the CCID Terminal Service Plug-In*.
- To install the updated file, refer to *Installing an Updated CCID Terminal Service Plug-in*.
- To activate the plug-in, refer to *Deactivating and Activating the CCID Terminal Service Plug-In*.

Deactivating and Activating the CCID Terminal Service Plug-In

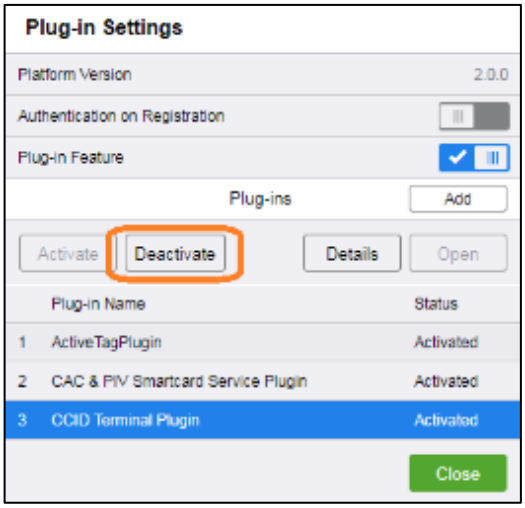
NOTE

This task is only required if the version number of the currently installed plug-in is **lower** than the plug-in downloaded from Xerox.com. If you have not already checked the version number of the currently installed plug-in, refer to *Checking the CCID Terminal Service Plug-In Version Number*.

To change the status of the plug-in:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then select **Plug-In Settings**.
7. Select the **CCID Terminal Plug-in**, then do one of the following:
   - To deactivate the plug-in, click **Deactivate**.
   - To activate the plug-in, click **Activate**.

   For example, the CCID Terminal Plug-in is activated and requires deactivation.



8. To save the changes, click **Close**.
9. To apply the changes and restart the device, click **Home**, then select **Support** > **Restart Device**.
10. A dialog box appears. To complete the restart process, click **Restart**.

Installing an Updated CCID Terminal Service Plug-in File

NOTES

- Before completing this task, ensure that the CCID Terminal Service plug-in is deactivated. For details, refer to *Deactivating and Activating the CCID Terminal Service Plug-In*.

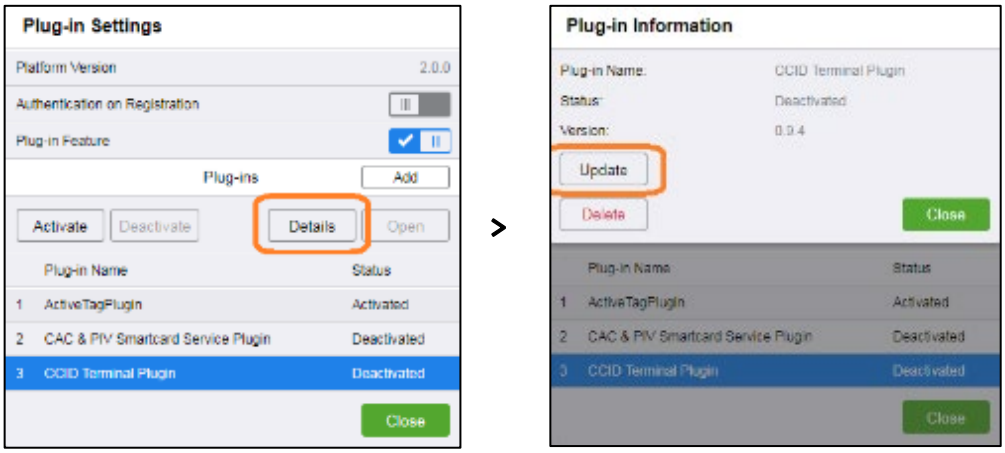
- This task is only required if the version number of the currently installed plug-in is **lower** than the plug-in downloaded from Xerox.com. If you have not already checked the version number of the plug-in, refer to *Downloading the CCID Terminal Service Plug-in File*.

To update the CCID Terminal Service Plug-in:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then select **Plug-In Settings**.
7. Select **CCID Terminal Plug-in**. Ensure that the status is set to **deactivated**.

   NOTE

   If the status of the plug-in is set to **activated**, for information on how to deactivate the plug-in, refer to *Deactivating and Activating the CCID Terminal Service Plug-In*.
8. Click **Details**, then select **Update**.



9. Click **Select**. Navigate to the location that you chose in step 5 of *Downloading the CCID Terminal Service Plug-in File*.
10. Locate the file named **CCID_Terminal_Plug-in_vX.X.X_sig.jar**.
11. Select the file, then click **OK** > **Close** > **Close**. The version in the Plug-In Information dialog is updated to match the downloaded version.
12. After you have ensured that the most up-to-date version is installed, reactivate the plug-in. For information on how to reactivate the plug-in, refer to *Deactivating and Activating the CCID Terminal Service Plug-In*.

NOTE

After you make plug-in changes, ensure that you close the Plug-In Settings dialog. If you leave the Plug-In Settings dialog open, it can cause errors.

Enabling the CAC&PIV Smartcard Service Plug-in

CAC and PIV cards are two types of IC cards that you can use to authenticate a user at the printer. To use a CAC or PIV card with the printer, enable the CAC&PIV Smartcard Service Plug-in.

To enable the CAC&PIV Smartcard Service Plug-in:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then select **Plug-In Settings**.
7. Select the **CAC&PIV Smartcard Service Plug-in**, then do one of the following:
   - If the status of the CAC&PIV Smartcard Service Plug-in is Activated, the task is complete. To return to the Embedded Web Server System page, click **Close**.
   - If the status of the CAC&PIV Smartcard Service Plug-in is Deactivated, continue with the remaining steps in this task.
8. Click **Activate**.
9. To save the changes, click **Close**.
10. To apply the changes and restart the device, click **Home**, then select **Support** > **Restart Device**.
11. A dialog box appears. To complete the restart process, click **Restart**.

Changing the System to Smart Card Authentication

After you have enabled the CAC&PIV Smartcard Service Plug-In, configure the printer to allow Smart Card authentication. After Smart Card Authentication users are required to log in at the device using a Smart Card, before they can use previously locked services.

To change the system to Smart Card authentication:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **Permissions**, then select **Login/Logout Settings**.
7. For **Smart Card**, click **Select**.
8. To enable domain controller validation, for **Validate**, click the toggle button.
9. To add a domain controller, click **Add.**

10. Enter the customer-specified domain server host name, domain server port, and domain, then click **OK**.
11. For Device Website Login Method, locate the Network option, then click **Select**.
12. Select **Kerberos (Windows ACS)**, then click **Next**.

    NOTE

    CAC authorization is always enabled through Kerberos. Do not select SMB or LDAP unless you have been explicitly instructed to by your network administrator.

13. For each Authentication and Domain for Smart Card users, enter the following customer-supplied Kerberos Authentication settings.
    - Domain or Realm name
    - Authentication Server Host Name or IP Address
    - Port number

    NOTES

    - For information about Kerberos, contact your system administrator.
    - If you want to use secondary alternate servers, click **Add Alternate Server**, then enter the details.
14. To save your changes, click **OK**.
15. To restart the device and apply the changes, click **Restart Now**.

Enabling the Smart Card Certificate Verification Option

NOTES

- Enabling Smart Card certificate verification is an optional step.
- This step should only be completed after you verify that users can successfully authenticate and log in using a Smart Card, and after all Root and Intermediate Certificates are imported to the device.

To enable Smart Card verification:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **System**, then select **Security**.
7. For Certificates, click **Smart Card Certificate Verification**.
8. Ensure that **On** is selected, then click **OK**.

10 Feature Configuration

Securing Against Non CAC/PIV Login

NOTES

- On VersaLink devices removing the CAC/PIV card will force a logout from the device, clearing user credentials. This is expected behavior when the device is configured for CAC/PIV login.

The device can be configured to only allow access using a CAC/PIV card by following these steps:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **Permissions**, then select **Guest Access Edit**.
7. Select **Device User Role**.
8. Under **Control Panel Permissions** select the **No Access** radio button.
9. Under **Device Website Permissions** select the **Home Only** radio button.
10. Select **Ok.**
11. In the top right corner select **Admin** and then **Log Out**.

At this time no functions of the device will be available to users who are not authenticated.

Obtaining and Installing the V3 Xerox® Print Driver

For information on obtaining, installing, and configuring print drivers for your Xerox® device, refer to your Xerox® device user guide.

NOTES

- Only the V3 Xerox® Print drivers are CAC-enabled for VersaLink products. Support for V4 Xerox® Print drivers and support for the Xerox® Global Print Driver® and Xerox® Mobile Express Driver® are not available at this time. For information on supported print drivers, refer to *Support at Xerox*.
- If you need help to determine if your device requires a PostScript or PCL driver, contact your system administrator.

Configuring the Client for Secure Print Release Jobs

Microsoft Windows workstations that will submit secure print release jobs must be configured following this process:

1. Ensure that the V3 Xerox® Print Driver has been installed.
2. Open the **Run** dialog using the start menu or Windows key.
3. Enter **Devices and Printers** and select the same from the search results.
4. Locate the Xerox printer and right click on the printer icon.
5. Select **Printing Preferences** from the context menu.
6. Select the **Advanced** tab from the dialog.
7. Expand the **Driver** category and ensure that **Enhanced Printing Features** is **Enabled.**
8. Select **Ok** to close the dialog.
9. Locate the same Xerox printer and right click on the printer icon.
10. Select **Printer Properties** from the context menu.
11. Select the **Administration** tab or the **Options** tab depending on print driver version.
12. Ensure that **Access and Verification (CAC/PIV)** is **Enabled**.
13. Select the **Configuration** tab.
14. Ensure that **Bi-Directional Communication Connection** is set to **Automatic.**
15. Select **Ok** to close the dialog.

Enabling Email Signing and Encryption

After the device is configured, to send S/MIME email, enable and configure SMTP and enable S/MIME.

NOTE

The device may already be configured for SMTP email delivery. Confirm the SMTP configuration, even if feature shows as enabled on the Embedded Web Server.

To enable and configure SMTP:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **Connectivity**, then select **SMTP**.
7. Ensure that **Email Submission** and **Email Notification** are both enabled.
8. Ensure that the details for **Device Email**, **SMTP Server Address** and **Outgoing SMTP Port Number** match the settings for the installed network.

   NOTE

   The SMTP and S/MIME values may have been set automatically when the system was installed. If you are unsure whether these values are correct, contact your local email administrator.

9. Ensure that the **Connection Security** and **Outgoing SMTP Authentication** settings are correct for the installed network.
10. To save your changes, click **OK**.
11. To restart the device and apply the changes, click **Restart Now**.

To enable S/MIME:

1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password that you created in step 3 of *Changing the Admin Password*, then click **Log In**.
6. On the Embedded Web Server Home page, click **Connectivity**, then select **S/MIME**.
7. To enable S/MIME, locate Enable, then click the toggle button.

   NOTE

   In the S/MIME window, you can optionally set encryption standards. Before changing any settings, consult your local email or security administrator.
8. To save your changes, click **OK**.

11 Workflow Examples

The following workflow examples assume that the printing device is configured for the customer network.

Secure Scan to Email

Secure Scan to Email allows users to scan and send a document, in an encrypted format, to an email address. The Secure Scan to Email feature prevents unauthorized users from intercepting and reading documents. Users can digitally sign the email as proof that they are the sender.

Requirements
To use Secure Scant to Email, the following are required:

- Enable the Email Signing and Encryption features. For instructions on enabling the Email Signing and Encryption features, refer to *Enabling Email Signing and Encryption*.

To use the Secure Scan to Email feature with Smart Card authentication:

1. At the device control panel, press the **Home** button, then touch **Log In**.
2. Insert the CAC card into the card reader.
3. Using the touch screen device keyboard, enter the CAC Passcode, then touch **Enter**.
4. Touch **Scan To**, then select **Email**.
5. Using the touch screen device keyboard, enter the recipient email address, then touch **Enter**.

   NOTE

   You can send scanned files to multiple recipients. To add additional email recipients, touch **Add Destination**.
6. Configure the filename, file type, and Common Features settings as required, then touch **Scan**.

   NOTE

   On VersaLink the Email 'From' address can be obtained from multiple locations.
   On VersaLink you can specify the “From” address through the EWS under Apps->Email->Scan To Apps General Settings->”From” Field.

   The device will use the first Email determined in this order:
   1) Email from the Smart Card.
   2) Email from the Login process if enabled through EWS.
   3) User specified ‘From’ if allowed through EWS.
   4) Device Email if not other address is specified.

Secure Print Hold and Release

To use the Secure Print Hold and Release feature with Smart Card authentication:

1. At the device control panel, press the **Home** button, then touch **Log In**.

2. Insert the CAC card into the card reader.
3. Using the touch screen device keyboard, enter the CAC Passcode, then touch **Enter**.
4. Touch **Jobs**, then select **Personal & Secure Jobs**.
5. Highlight the job that you want to print, then touch **Print**.

12 Troubleshooting and Support

Troubleshooting Tips

Attempting to Update an Active Plug-In
Before you update a plug-in, ensure that the plug-in is deactivated.

Attempting to Change the State for Multiple Plug-Ins
After changing the state of any plug-in, and before you change the state of any additional plug-ins, restart the device.

Support at Xerox

For support with any Xerox® product, go to the Xerox website: https://www.xerox.com/support

For information on your local sales and Technical Customer Support team, go to the Xerox® web site: https://www.xerox.com/office/worldcontacts

More Information

You can obtain more information about your Xerox® printer from these sources:

Resource	Location
Installation Guide	Packaged with the printer.
Recommended Media List	United States: www.xerox.com/rmlna European Union: www.xerox.com/rmleu
Local sales and Technical Customer Support	www.xerox.com/office/worldcontacts
Printer registration	www.xerox.com/office/register
Direct online store	www.direct.xerox.com/

13 Security Information

Security at Xerox

For the latest security information about your Xerox® product, go to http://www.xerox.com/security.

For the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox® software and hardware, go to http://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html