



Common Access Card for Xerox[®] VersaLink[®] Printers

System Configuration Guide

© 2017 Xerox Corporation. All rights reserved. Unpublished rights reserved under the copyright laws of the United States. Contents of this publication may not be reproduced in any form without permission of Xerox Corporation.

Copyright protection claimed includes all forms of matters of copyrightable materials and information now allowed by statutory or judicial law or hereinafter granted, including without limitation, material generated from the software programs which are displayed on the screen such as styles, templates, icons, screen displays, looks, and so on.

Xerox® and Xerox and Design®, Global Print Driver®, VersaLink®, and Mobile Express Driver® are trademarks of Xerox Corporation in the United States and/or other countries.

PostScript® is a trademark of Adobe Systems Incorporated in the United States and/or other countries.

Windows® is a trademark of Microsoft Corporation in the United States and other countries.

Document Version 1.3 November 2017

BR22729

Contents

| | | |
|---|--|------|
| 1 | Introduction..... | 1-1 |
| | Purpose..... | 1-1 |
| | Target Audience..... | 1-1 |
| | Disclaimer..... | 1-1 |
| 2 | Prerequisites..... | 2-2 |
| 3 | Feature Overview..... | 3-3 |
| | S/MIME..... | 3-3 |
| | Requirements..... | 3-3 |
| | Secure Print Hold and Release..... | 3-3 |
| 4 | Supported Card Readers..... | 4-4 |
| 5 | Supported Card Types..... | 5-5 |
| 6 | System Configuration..... | 6-6 |
| | System Configuration Checklist..... | 6-6 |
| | Accessing the Embedded Web Server..... | 6-7 |
| | Changing the Admin Password..... | 6-8 |
| | Enabling HTTPS..... | 6-9 |
| | Importing Root and Intermediate Certificates..... | 6-10 |
| | Enabling SNMP..... | 6-10 |
| | Enabling the Plug-In Feature..... | 6-11 |
| | Downloading the CCID Terminal Service Plug-in File..... | 6-12 |
| | Checking the CCID Terminal Service Plug-In Version Number..... | 6-13 |
| | Updating the CCID Terminal Service Plug-in..... | 6-13 |
| | Deactivating and Activating the CCID Terminal Service Plug-In..... | 6-14 |
| | Installing an Updated CCID Terminal Service Plug-in File..... | 6-14 |
| | Enabling the CAC&PIV Smartcard Service Plug-in..... | 6-16 |
| | Changing the System to Smart Card Authentication..... | 6-16 |
| | Enabling the Smart Card Certificate Verification Option..... | 6-17 |
| 7 | Feature Configuration..... | 7-18 |
| | Obtaining, Installing and Configuring V3 Xerox® Print Driver..... | 7-18 |
| | Enabling Email Signing and Encryption..... | 7-18 |
| 8 | Workflow Examples..... | 8-20 |
| | Secure Scan to Email..... | 8-20 |
| | Secure Print Hold and Release..... | 8-20 |

| | | |
|----|----------------------------------|-------|
| 9 | Troubleshooting and Support..... | 9-21 |
| | Troubleshooting Tips..... | 9-21 |
| | Support at Xerox | 9-21 |
| | More Information..... | 9-21 |
| 10 | Security Information..... | 10-22 |
| | Security at Xerox | 10-22 |

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

This document does not address the proper configuration of the network, Public Key Infrastructure (PKI), or server authentication systems.

3 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.

Requirements

To use the secure Scan to Email feature, purchase and install the optional Hard Disk Drive (HDD) kit.

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.

4 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.

5 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.

6 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 |
|--------------------------|---|
| <input type="checkbox"/> | 1. Accessing the Embedded Web Server |
| <input type="checkbox"/> | 2. Changing the Admin Password |
| <input type="checkbox"/> | 3. Enabling HTTPS |
| <input type="checkbox"/> | 4. Importing Root and Intermediate Certificates |
| <input type="checkbox"/> | 5. Enabling SNTP |
| <input type="checkbox"/> | 6. Enabling Plug-In Feature |
| <input type="checkbox"/> | 7. Downloading the CCID Terminal Service Plug-in File |
| <input type="checkbox"/> | 8. Checking the CCID Terminal Service Plug-In Version Number |
| <input type="checkbox"/> | 9. Updating the CCID Terminal Service Plug-in |
| <input type="checkbox"/> | 10. Deactivating and Activating the CCID Terminal Service Plug-In |
| <input type="checkbox"/> | 11. Installing an Updated CCID Terminal Service Plug-in File |
| <input type="checkbox"/> | 12. Enabling the CAC&PIV Smart Card Service Plug-in |
| <input type="checkbox"/> | 13. Changing system to Smart Card Authentication |
| <input type="checkbox"/> | 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.

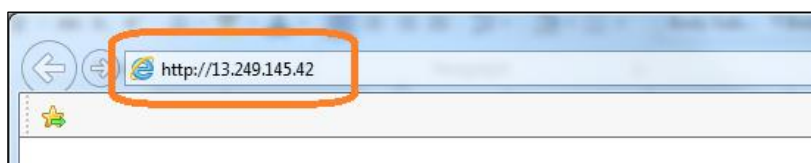
When the device is first powered on in the default configuration, a Startup Page report prints with details about the device. The Startup Page includes the IPv4 address of the system on the TCP/IP network. Record the IP address for later use.

NOTE

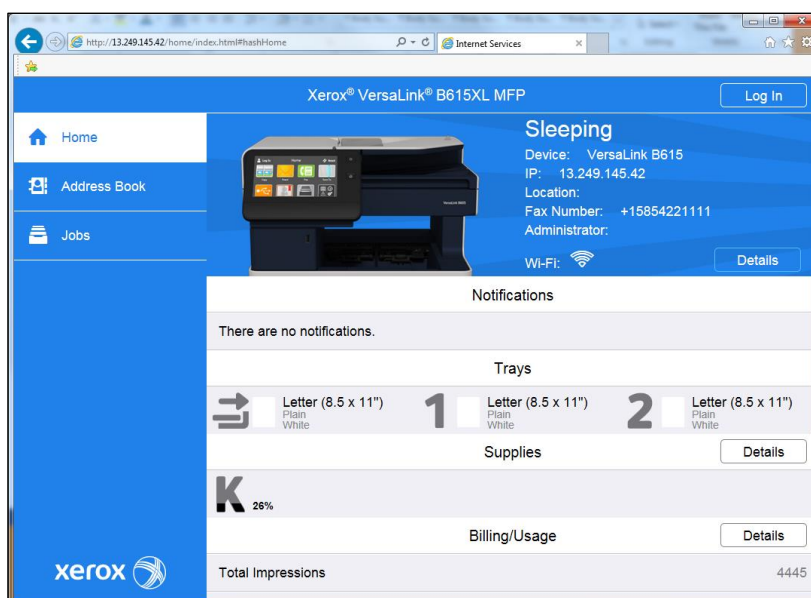
If the device is not configured to print a Startup Page, you can determine the IPv4 address of the system at the device control panel. At the device control panel, press the **Home** button, then touch **Device > About**. The IPv4 address is located under the Network heading.

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.

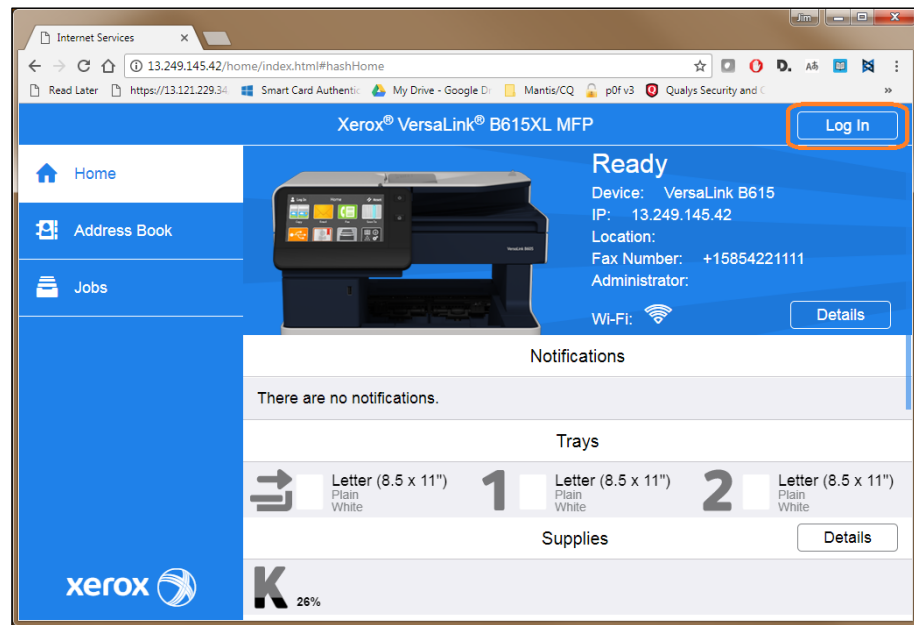
Changing the Admin Password

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

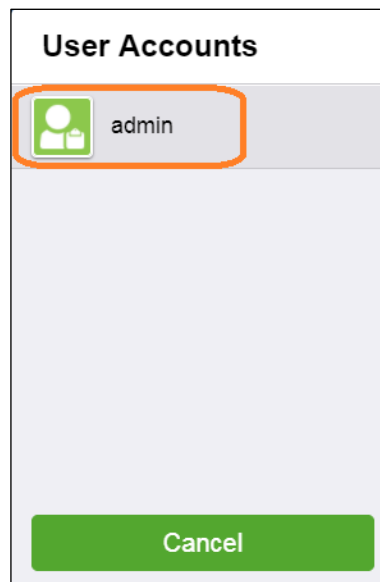
To change the admin password, log into the Embedded Web Server using the default System Administrator login credentials.

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

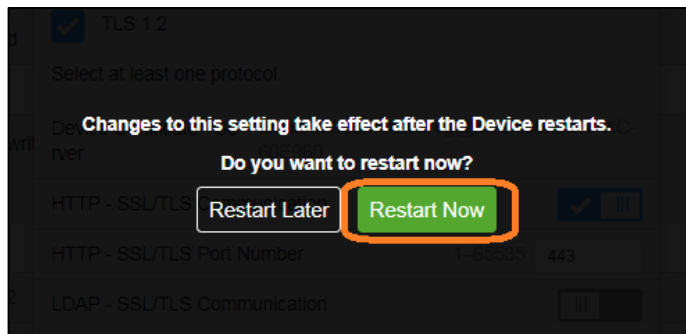
Ensure that you record the new admin password in a safe location for future use.

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:

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, select **Security Certificates**.
8. From the Device Certificates menu, select **Trusted Root CA Certificates**, then click **Import**.
9. 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:

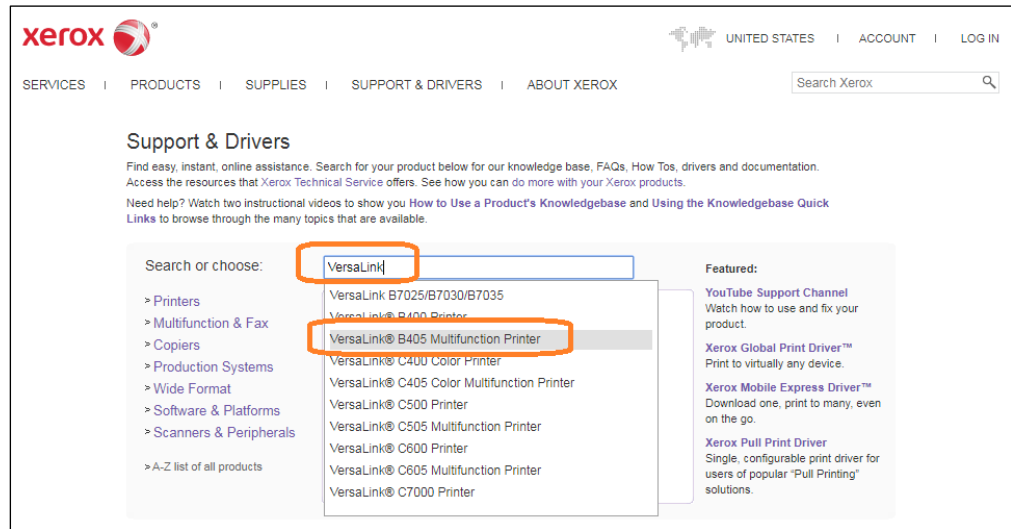
1. At your computer, open a new browser window.
2. In the address bar, type **https://** followed by the IP address or DNS-resolvable device host name, then press **Enter**.
3. On the Embedded Web Server Home page, click **Log In**.
4. From the list of user accounts, select **Admin**.
5. Enter the password 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

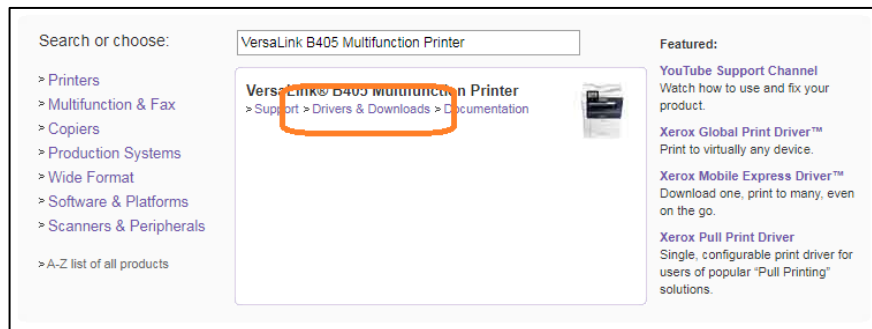
To connect the printer to an IC card reader, download and install the CCID Terminal Service plug-in.

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**.



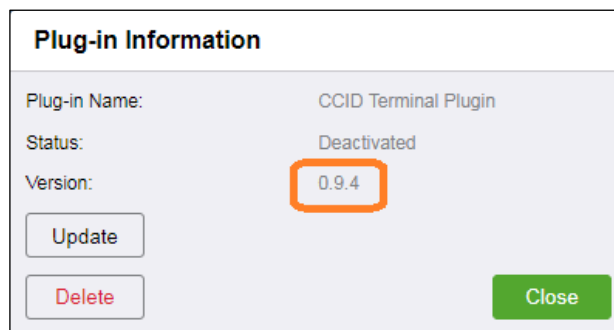
4. For Firmware, select **Card Reader Plug-ins**.
5. Download the .ZIP file. Extract the .ZIP file contents to an easily accessible location on your local system.
6. Open the extracted folder, then locate the file named **CCID_Terminal_Plug-in_vX.X.X_sig.jar**.
7. Record the version number of the file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

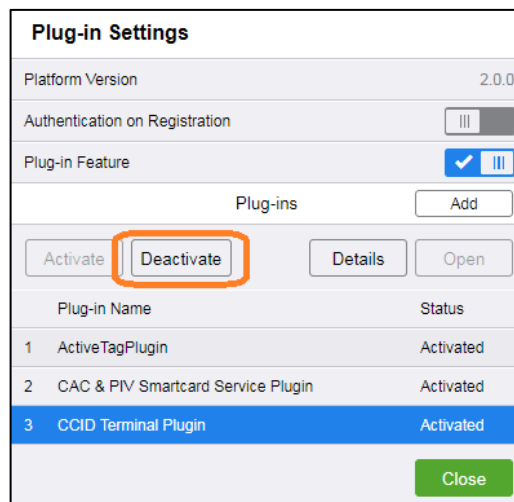
NOTE

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](#).

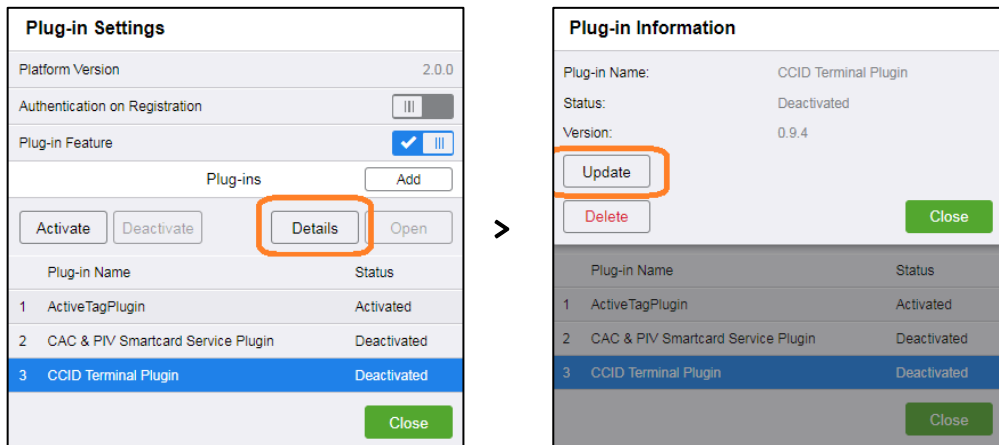
To update the CCID Terminal Service Plug-in:

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.XX_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**.

7 Feature Configuration

Obtaining, Installing and Configuring 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.

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**.

8 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 Scan 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](#).
- Purchase the Hard Disk Drive kit, then install the drive on your Xerox® device.

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**.

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**.

9 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/rmlau |
| 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/ |

10 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>