HP SmartCard SIPRNet and NIPRNet Solutions for US Government using HP FutureSmart firmware

Administrator's Guide

Copyright and License

© Copyright HP Development Company, L.P.

Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Part number: F8B30A and CC543B

Edition: 3, 2/2016

Trademark Credits

Microsoft®, Windows®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Applicable product: F8B30A and CC543B

Table of contents

1 Introduction 1

2 Getting started with HP SmartCard SIPRNet or NIPRNet Solution 2

Supported Products 2

Install the HP SmartCard NIPRNet or SIPRNet Solution 2

Obtain tools for configuring the printer 3

Update the firmware 3

3 Configure the printer settings using the Embedded Web Server 4

Access the Embedded Web Server (EWS) 4

Set the date and time 5

Verify the network settings 6

Configure the sign-in method to enable SmartCard authentication 7

Configure certificate management 11

Configure the Scan/Digital Send settings 14

Address Book settings 14

E-mail settings 15

Save to Network Folder settings 18

4 Device Resets 21

Restore Factory defaults 21

Preboot Menu 24

Appendix A Licenses 26

Heimdal Kerberos 27

OpenLDAP 28

OpenSC 30

OpenSSL 34

SHA-2 36

Appendix B Warranty Service 37
HP Limited Warranty Statement 37
Customer self-repair warranty service 38

1 Introduction

The HP SmartCard NIPRNet Solution for US Government and the HP SmartCard SIPRNet Solution for US Government are designed to optimize security in imaging and printing environments for various Department of Defense (DoD) agencies and military branches of the US government.

This guide is intended for administrators responsible for managing security in their network environment, and provides instructions on how to install and configure settings on HP products with FutureSmart firmware version using the HP SmartCard SIPRNet or NIPRNet Solution for US Government.

2 Getting started with HP SmartCard SIPRNet or NIPRNet Solution

Get started by installing the HP SmartCard SIPRNet or NIPRNet Solution on HP products with HP FutureSmart firmware version. This chapter provides instructions on the following topics:

- Supported Products
- Install the HP SmartCard NIPRNet or SIPRNet Solution
- Obtain tools for configuring the printer
- Update the firmware

Supported Products

For a list of HP products compatible with the HP SmartCard SIPRNet Solution for US Government, go to Supported products for SIPRNet Solution (c04896003), and for products that are compatible with the NIPRNet Solution, go to Supported products for NIPRNet Solution (c04896573).

Install the HP SmartCard NIPRNet or SIPRNet Solution

Purchase one of the following Smart Cards, and then install it on the printer.

- HP SmartCard US Govt NIPRNet Solution: CC543B #201
- HP SmartCard US Govt SIPRNet Solution: F8B30A #201

For installation instructions of the HP SmartCard NIPRNet Solution for US Government or the HP SmartCard SIPRNet Solution for US Government, go to: Installation Guide. (c04797700)

Figure 2-1 HP SmartCard NIPRNet Solution

Figure 2-2 HP SmartCard SIPRNet Solution

Obtain tools for configuring the printer

The **Tools** directory in the HP CAC website provides the files required for configuring a printer with the HP SmartCard SIPRNet or NIPRNet Solutions.

Obtain the following files in the Tools directory:

- KerbosInfoCert2.exe OR KerbosInfoCert2.vbs: To view the configuration information.
- FutureSmartBackupRestore 2.0.0.3.exe: To obtain the FutureSmart Restore tool

Follow these steps to obtain the files in the **Tools** directory:

1. Go to https://ftp.usa.hp.com/hprc.
2. Read the **HPRC Terms of Use & Service**, and then click **Accept**.
3. Type in your Account name and password, and then click **Login**.

NOTE: Passwords must be changed annually to the next consecutive number.

4. Click the **Tools** directory.
5. Select the following files, and then click **Save**.
   - KerbosInfoCert2.exe OR KerbosInfoCert2.vbs

     Make sure to print this page to verify the Kerberos Client settings information when configuring the device.
   - FutureSmartBackupRestore 2.0.0.3.exe

Update the firmware

To download the latest firmware, go to HP Support, and then select **Software and Drivers**.

For instructions to download and update the firmware, go to Update the firmware using a USB flash drive or the Embedded Web Server (EWS).

NOTE: After downloading the firmware, make sure to note the following information in the **Configuration Page**:

Product Name, Model number, Device Serial Number, and the Firmware Level.

3 Configure the printer settings using the Embedded Web Server

After installing the HP SmartCard NIPRNet or SIPRNet Solution on the printer, open the HP Embedded Web Server (EWS) to configure the printer settings. The following topics provides instructions for configuring the printer settings using the EWS.

- Access the Embedded Web Server (EWS)
- Set the date and time
- Verify the network settings
- Configure the sign-in method to enable SmartCard authentication
- Configure certificate management
- Configure the Scan/Digital Send settings

Access the Embedded Web Server (EWS)

Follow these steps to open the EWS:

1. From the Home screen on the printer control panel, touch the Network button to display the IP address or host name.
2. Open a Web browser, and in the address line, type the IP address of the printer exactly as it displays on the printer's control panel. Press the Enter key.

NOTE: If the Web browser displays a message indicating that accessing the website might not be safe, select the option to continue to the website. Accessing this website will not harm the computer.

NOTE: To prevent unauthorized changes in the printer configuration settings, IT administrators might set a password in the EWS.

3. Depending on how the HP EWS is configured, it might be necessary to log in using the administrator's password to access and configure printer settings.

NOTE: If passwords are set in the EWS, only the **Information tab** will be available to the users.

Set the date and time

The device date and time must be synchronized to within five minutes of the date and time on the Kerberos server. If the time difference is greater than five minutes, the HP Smart Card authentication attempts will fail.

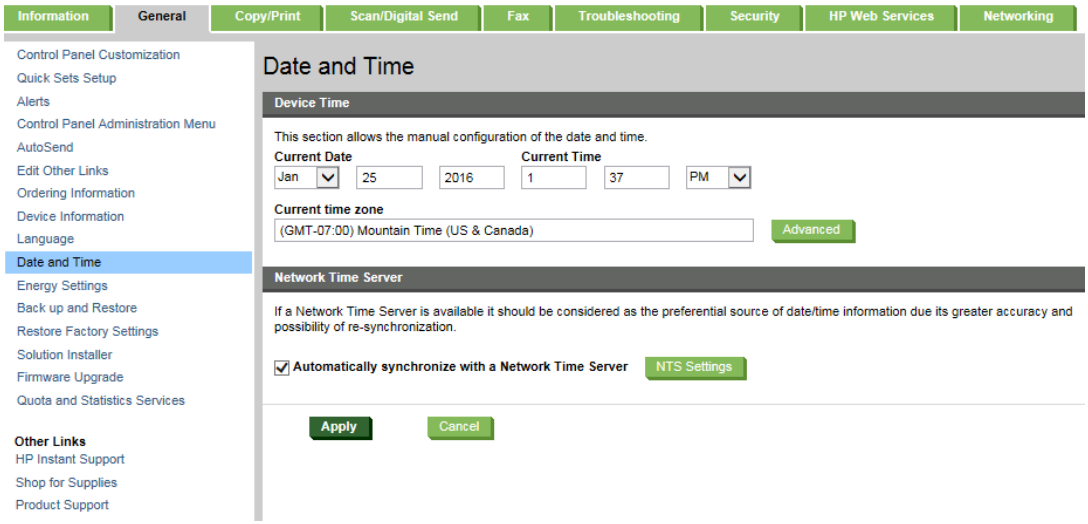
1. Open the EWS.

   For instructions, see Access the Embedded Web Server (EWS) on page 4

2. On the top navigation tabs, select the **General** tab.

3. In the left navigation pane, select **Date and Time**.

Figure 3-1 Date and Time



4. Set the date and time in the **Device Time** or in the **Network Time Server** section.

   Follow these steps to set the date and time in the **Device Time** section:

   a. Type the day and year for the **Current Date** and the time for the **Current Time**.

   b. Click **Advanced**, select the correct **Time zone** from the drop-down list, select the desired options in the **Daylight Savings Time Settings** section, and then click **OK**.

   Follow these steps to set the date and time in the **Network Time Server** section:

   a. Select the **Automatically synchronize with a Network Time Server** check box.

   b. Click **NTS Settings**, and then provide the server information, and then click **OK**.

5. Click **Apply** to save the changes.

Verify the network settings

Use the following information to verify the HP printer's TCP/IP network information.

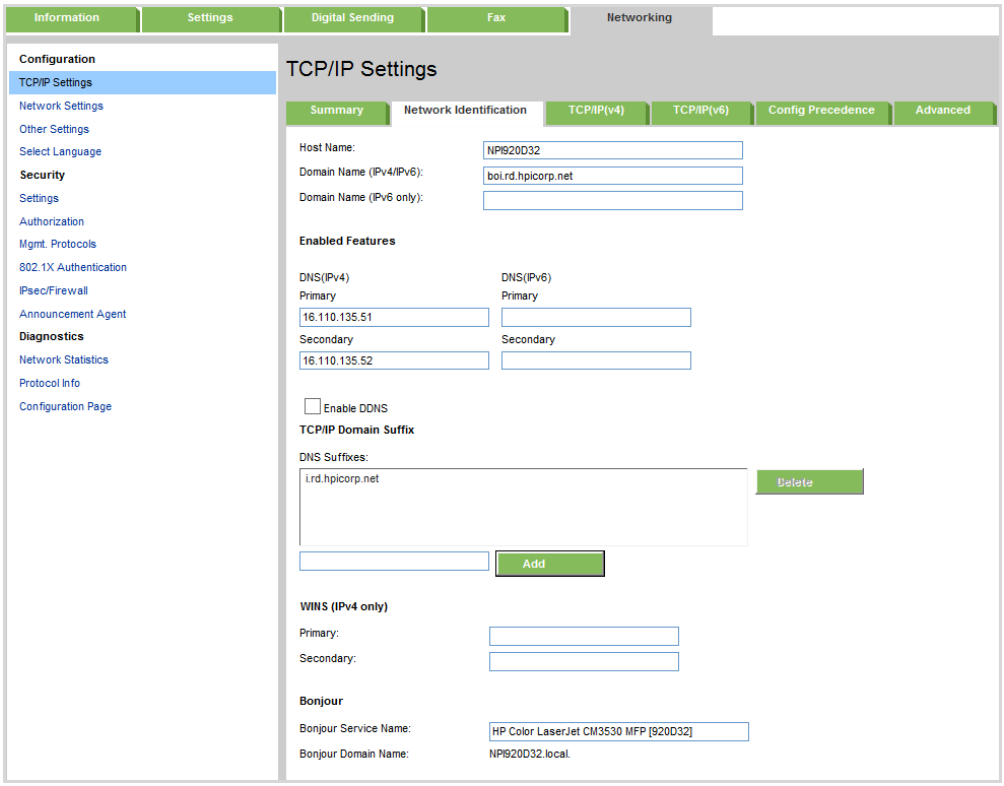
1. Open the EWS.

   For instructions, see Access the Embedded Web Server (EWS) on page 4

2. On the top navigation tabs, select the **Networking** tab.

3. On the left navigation pane, select the **TCP/IP Settings**, and then select the **Network Identification** tab.

Figure 3-2 TCP/IP Settings



4. Verify that the **Host Name** and **Domain Name (IPv4/IPv6)** are properly set.

5. Verify that the **DNS Primary** and **DNS Secondary** are correctly set.

6. If required, type additional DNS suffixes in the **DNS Suffixes** text box of the **TCP/IP Domain Suffix** section.

7. If applicable, type the WINS **Primary** and **Secondary** addresses in the **WINS (IPv4 only)** section.

8. Click **Apply** to save the changes.

Configure the sign-in method to enable SmartCard authentication

Use the **Access Control** page of the EWS to set up the **Smart Card** or the **SIPRNet Smart Card** in the sign-in method and domain information, to access functions at the device, and for E-mail settings.

NOTE: Verify that the printer is on and the HP SmartCard reader (NIPRNet or SIPRNet Solutions) is connected to the printer before beginning.

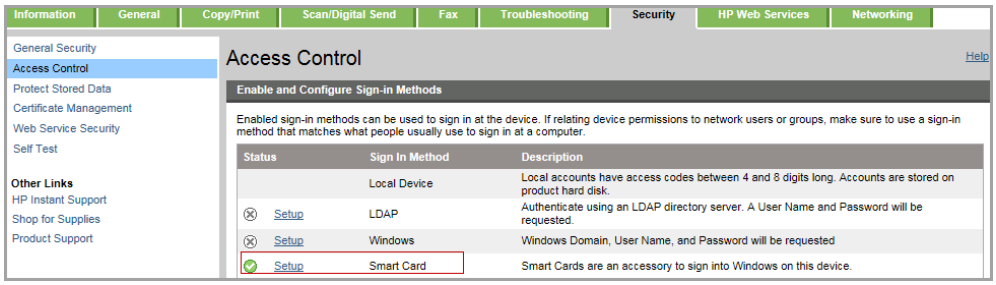
1. Open the EWS.

   For instructions, see Access the Embedded Web Server (EWS) on page 4

2. On the top navigation tabs, select the **Security** tab.

3. In the left navigation pane, click **Access Control**.

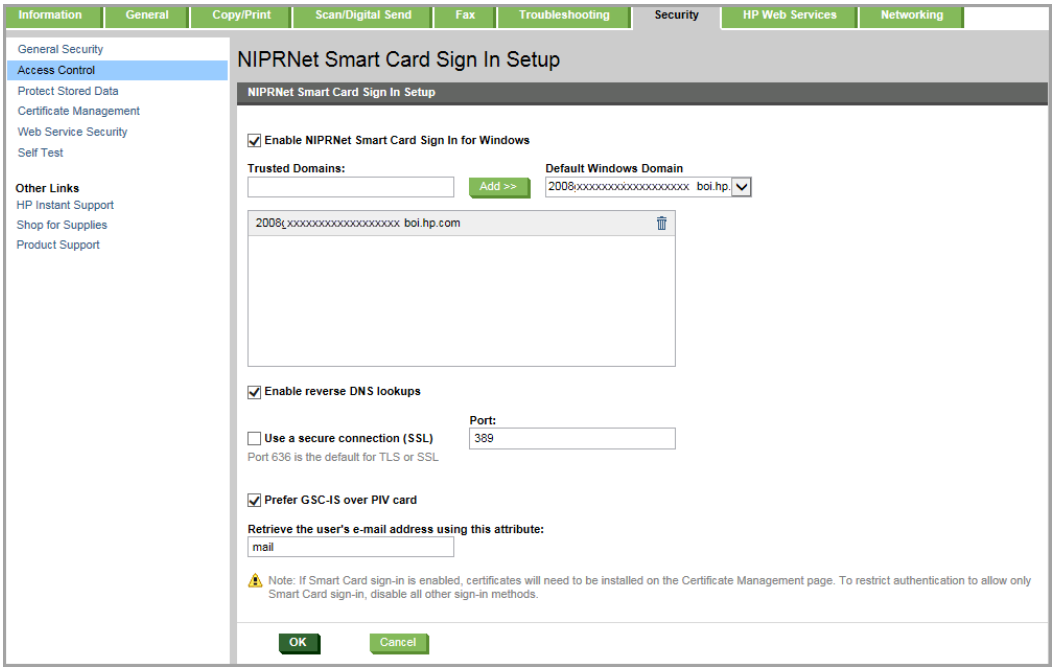
Figure 3-3 Access Control



4. Verify that the **Smart Card** (for HP SmartCard NIPRNet Solution) or the **SIPRNet Smart Card** (for HP SmartCard SIPRNet Solution) is listed in the **Sign In Method** column.

5. In the **Enable and Configure Sign-in-Methods** section, select **Setup** in the **Status** column where the Sign in method column is either the **Smart Card** entry to set up the HP SmartCard NIPRNet Solution for US Government, OR the **SIPRNet Smart Card** entry to set up the HP SmartCard SIPRNet Solution for US Government.

Figure 3-4 Smart Card Sign in Setup



6. On the **NIPRNet Smart Card Sign In Setup** or **SIPRNet Smart Card Sign In Setup** page, perform the following tasks to enable the SmartCard as a sign-in method:

   a. Select the **Enable NIPRNet Smart Card Sign In for Windows**, or **Enable SIPRNet Smart Card Sign In for Windows** check box.

   b. Type the fully qualified domain name (FQDN) of the domain controller in the **Trusted Domains** text box, and then click **Add**.

   c. If your environment has reverse DNS disabled, clear the **Enable reverse DNS lookups** check box.

   d. Depending on your HP MFP Authentication Reader, select the proper environment setting.

   - HP CAC: Select **Prefer GSC-IS over PIV card** check box.
   - PIV cards: Select to clear the **Prefer GSC-IS over PIV card** check box.

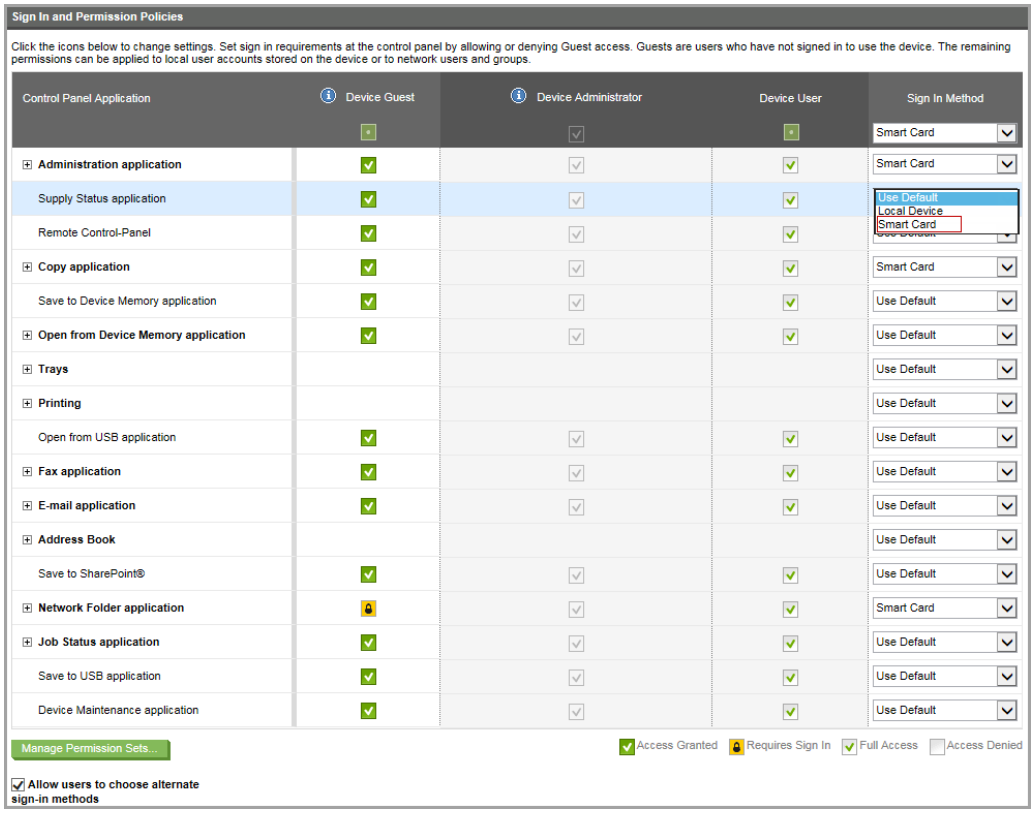
   e. Verify that the correct LDAP e-mail attribute is specified in the **Retrieve the device user's e-mail address using this attribute** (LDAP E-mail attribute) text box.

   f. Click **OK** to save the settings, or click **Cancel** to discard the changes.

7. After the page refreshes, review the **Enable and Configure Sign In Methods** section of the **Access Control** panel to verify that the **Status** for the **Smart Card** or **SIPRNet Smart Card** entry contains a green check mark. If not, perform the tasks in Step 6.

NOTE: If the **Smart Card** or **SIPRNet Smart Card** is not displayed on any of the drop-down lists as a **Sign In Method** in the **Sign In and Permission Policies** section, then the HP SmartCard (NIPRNet or SIPRNet) Solution for US Government might not be properly installed.

Figure 3-5 Sign in and Permission Policies



8. To restrict the **Sign In Method** to only the **Smart Card** or **SIPRNet Smart Card** , perform the following tasks on the **Enable and Configure Sign In Methods** section

   a. Select **Setup** in the **Status** column for the **Sign In Method** for entries that should be restricted (e.g. LDAP entry).

   b. On the Sign In Setup page (e.g. LDAP Sign In Setup), clear the **Enable** Sign In Method entry check box (e.g. Enable LDAP Sign In), and then select **OK**.

   NOTE: When the **Smart Card** or **SIPRNet Smart Card** option is selected from the **Sign in Method** drop-down list, all other functions are also restricted to the SmartCard authentication option.

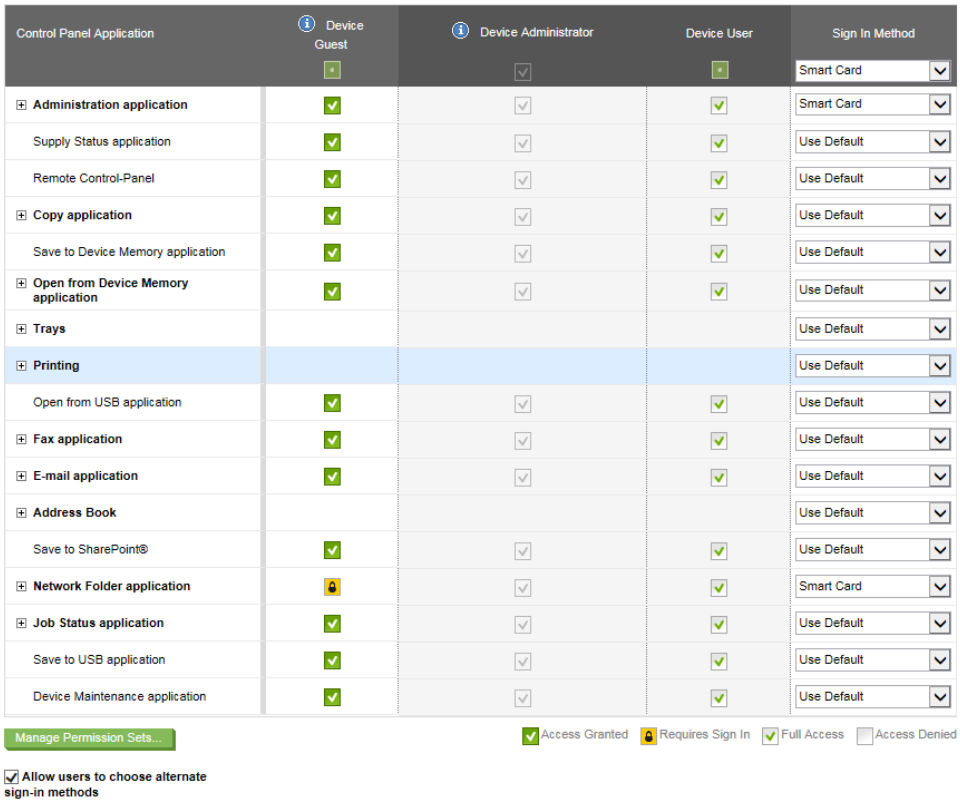
9. On the **Sign In and Permission Policies** section, perform the following tasks for each **Control Panel Application** that requires the HP SmartCard (NIPRNet or SIPRNet) Solution for the US Government:

   a. Select the **Smart Card** or **SIPRNet Smart Card** option from the **Sign In Method** drop-down list.

   b. In the **Device Guest** column, click the **Access Granted** icon ( ) and change it to the **Requires Sign In** icon ( ).

10. Click **Apply** to save the changes.

Figure 3-6 Smart Card option in the Sign In and Permission Policies



Configure certificate management

Set up security certificates on the **Certificate Management** page of the EWS:

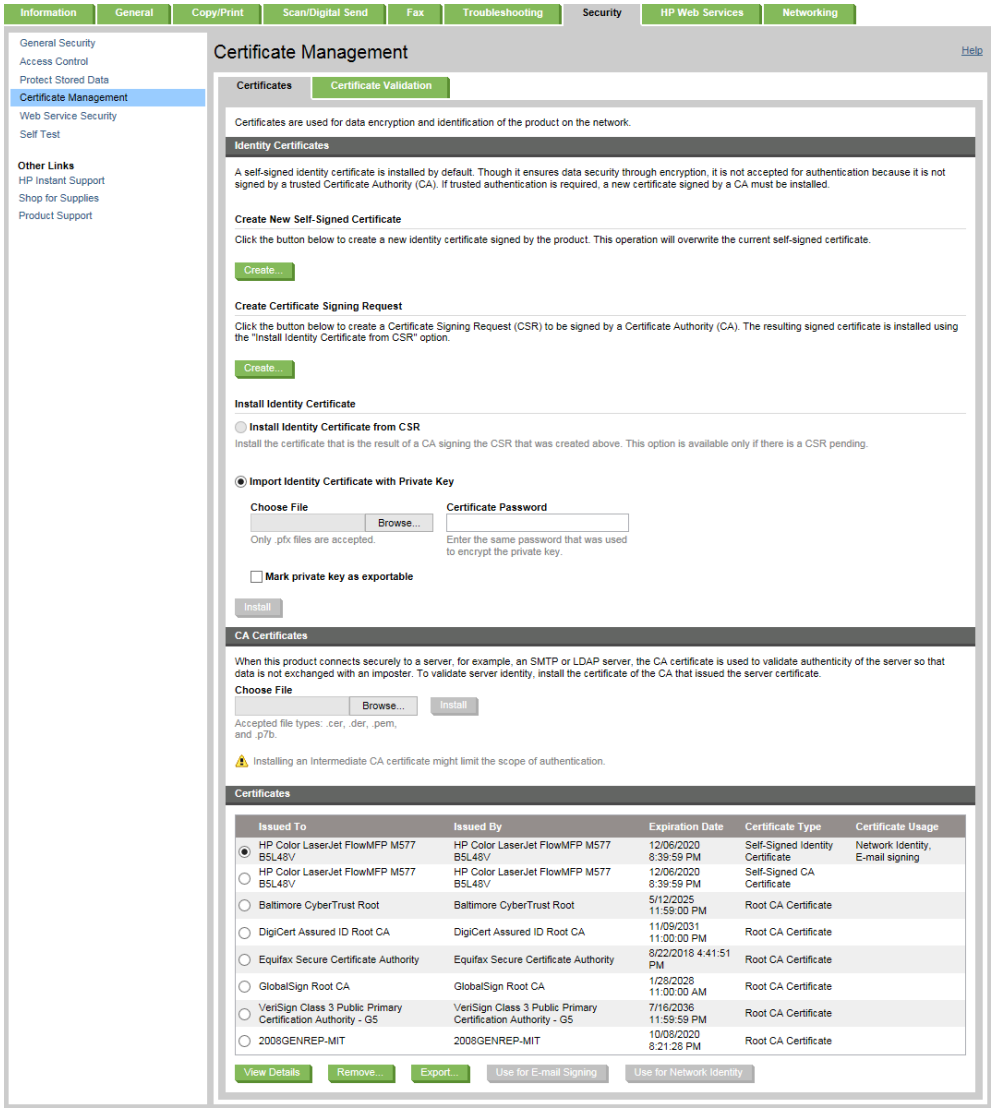
1. Open the EWS.

   For instructions, see Access the Embedded Web Server (EWS) on page 4

2. On the top navigation tabs, select the **Security** tab.

3. In the left navigation pane, click **Certificate Management**.

Figure 3-7 Certificate Management



4. Click the **Certificates** tab.

5. Install the root CA certificate, intermediate CA certificate, and the subordinate CA certificate of the Windows Active Directory domain controller.

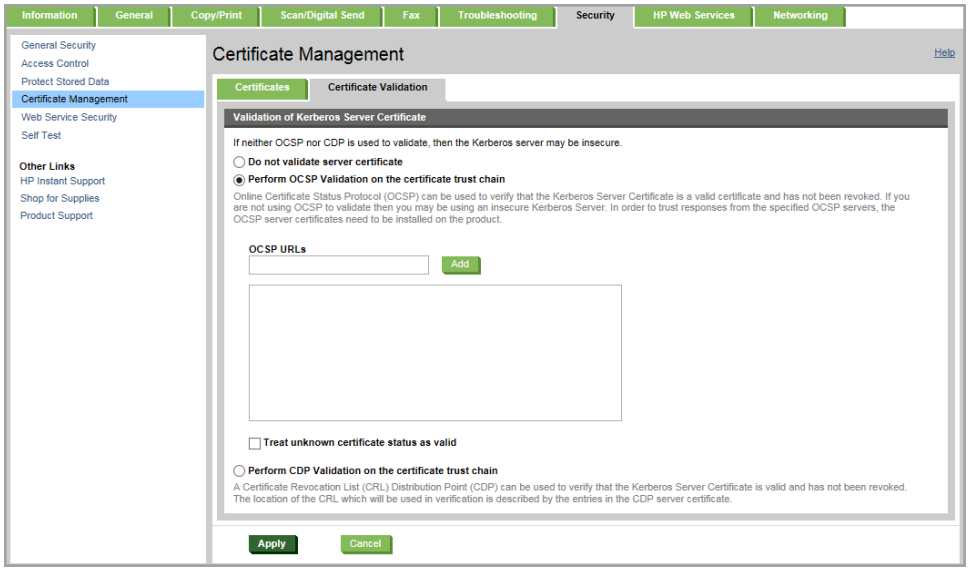
6. If OCSP is used for certificate-revocation checking, also install the root CA certificate, intermediate CA certificate, and the subordinate CA certificate of the OCSP server.

7. If OCSP is used for certificate revocation checking, complete the following steps:

   a. Click the **Certificate Validation** tab.

   b. Select the **Perform OCSP Validation on the certificate trust chain** check box to enable OCSP validation.

Figure 3-8 Certificate Validation

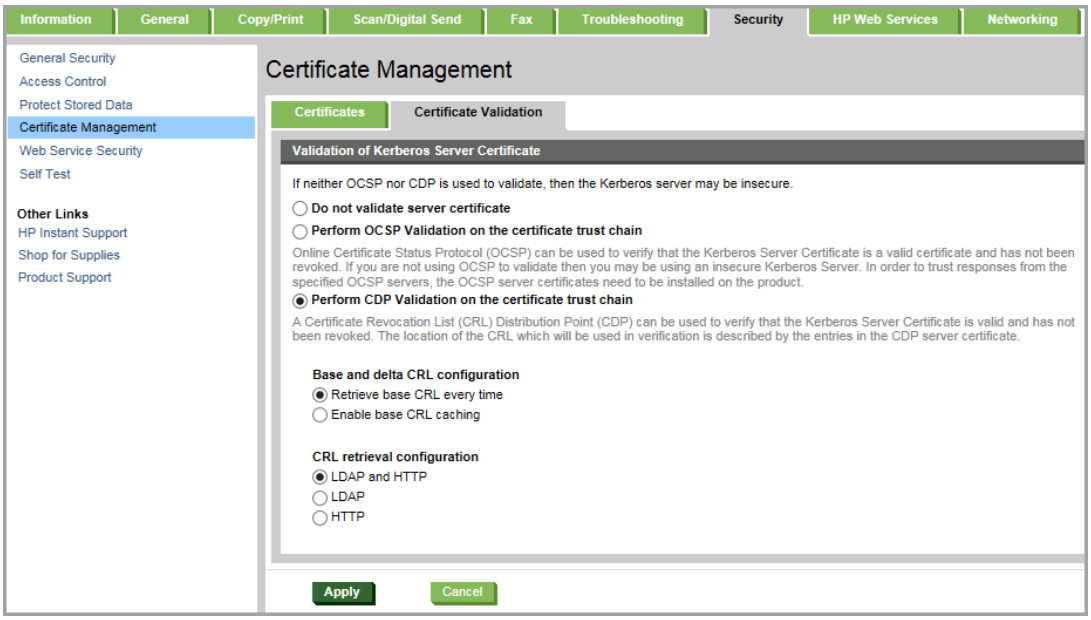


   c. Enter the URL(s) of the OCSP server(s) in the **OCSP URLs** field.

8. Click **Apply** at the bottom of the **Certificate Validation** section to save the changes.

9. If CDP is used for verification of the kerberos server certificate using a certificate revocation list, select the **Perform CDP Validation on the certificate trust chain** check box and complete the following.

Figure 3-9 Validation of Kerberos Server Certificate



NOTE: The retrieval options indicate which methods to use to retrieve the certificate revocation list (CRL).

a. Select the **Retrieve base CRL every time** check box (the default) to retrieve the list every time.

   -or-

   Select the **Enable base CRL caching** check box to allow selection of **Enable delta CRL support** and **Treat unknown CRL status as valid**.

b. Select one of the **CRL retrieval configuration** options to use. (**LDAP and HTTP** is the default.)

10. Click **Apply** at the bottom of the **Certificate Validation** section to save the changes.

Configure the Scan/Digital Send settings

Use the **Scan/Digital Send** tab of the EWS to configure the address book, e-mail, and network folder settings.

- Address Book settings
- E-mail settings
- Save to Network Folder settings

Address Book settings

Use the following steps to configure the **Address Book** settings.

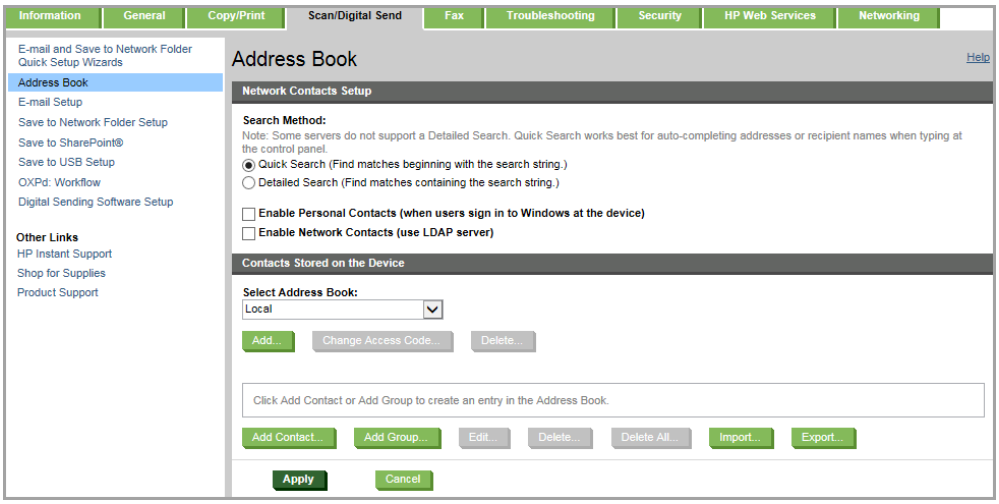
1. Open the EWS.

   For instructions, see Access the Embedded Web Server (EWS) on page 4

2. On the top navigation tabs, select the **Scan/Digital Send** tab.

3. In the left navigation pane, click **Address Book**.

Figure 3-10 Address Book



4. Select the **Enable Network Contacts (use LDAP server)** check box, and then click the **Add** button to start the wizard. The **Network Contacts Setup** page displays.

5. On the **Network Contacts Setup**, complete the following tasks to set up the network:

   a. In the **LDAP Server Address** field, type the FQDN of the domain controller.

   NOTE: This must be the same FQDN that was typed in the **Trusted Domains** field of the **NIPRNet Smart Card Sign In Setup** or the **SIPRNet Smart Card Sign In Setup** page.

   b. If applicable, in the **Port** field type the correct SSL or Global port number.

   - SSL Port: 636 or 3269
   - Global Catalog Port: 3268

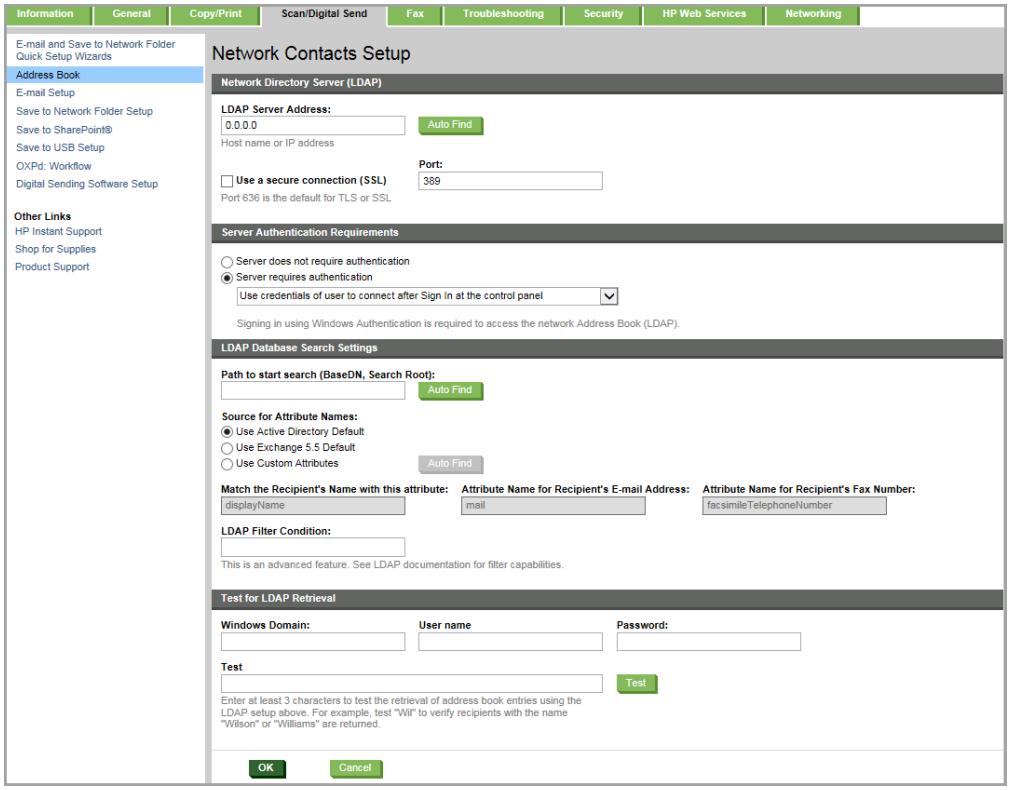
c. In the **Server Authentication Requirements** section, select the **Server requires authentication** radio button, and then select **Use credentials of user to connect after Sign In at the control panel** from the drop-down list.

d. In the **LDAP Data base Search Settings**, type the LDAP database search root in the **Path to start search (BaseDN, Search Root)** (OU=Installations,DC=SMARTCARDHQ,DC=DOD,DC=MIL, for example) field.

e. In the **Source for Attribute Names**, make sure that the **Use Active Directory Default** button is selected, unless the search attributes are different.

   For example, some sites require user principal name (userPrincipalName) instead of mail for the e-mail attribute.

Figure 3-11 Network Contacts Setup



6. Click **OK** to save any changes.

E-mail settings

Use the following steps to configure the **E-mail Setup**.

1. Open the EWS.

   For instructions, see Access the Embedded Web Server (EWS) on page 4

2. On the top navigation tabs, select the **Scan/Digital Send** tab.

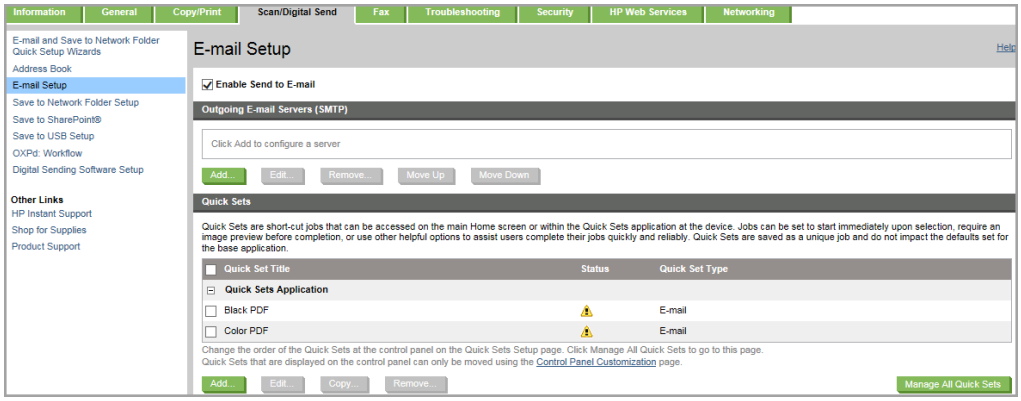
3. In the left navigation pane, click **E-mail Setup**.

4. On the **E-mail Setup** page, perform the following tasks to set up the email:

a. Select the **Enable Send to E-mail** check box.

b. In the **Outgoing E-mail Servers (SMTP)** section, click **Add** to start the wizard.

Figure 3-12 E-mail Setup



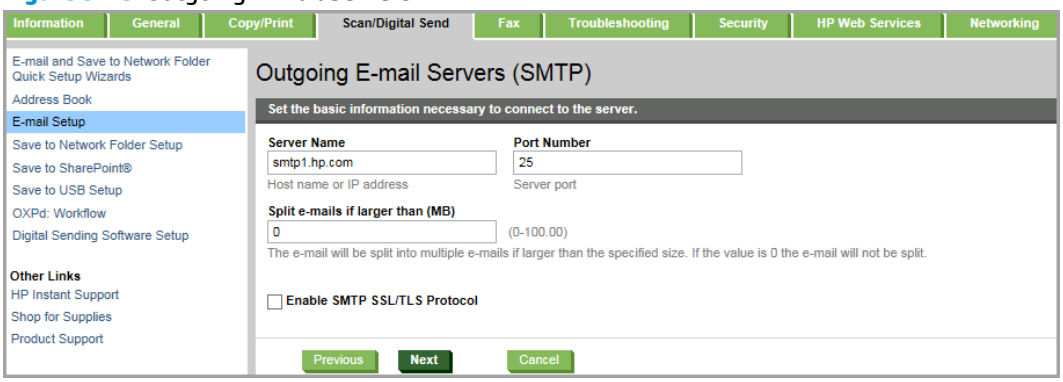
c. On the **Outgoing E-mail Servers (SMTP)** page, complete the following tasks:

i. Select **I know my SMTP server address or host name:** check box.

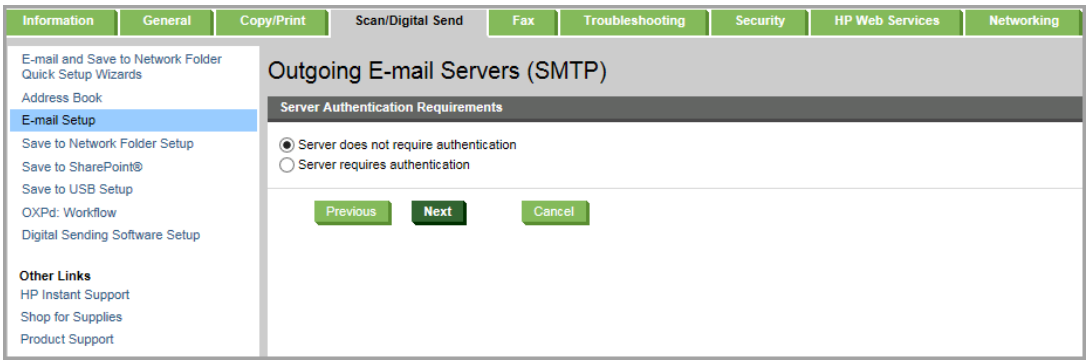
ii. Type the SMTP **Server Name** and the **Port Number**. To split large e-mails, type a value in megabytes in the **Split e-mails if larger than (MB)** field.

iii. Click **Next** to continue.

Figure 3-13 Outgoing E-mail Servers



iv. On the **Server Authentication Requirements** section, select **Server does not require authentication** radio button, and then click **Next**.



d. On the **Server Usage** section, select which functions the server is used for, and then click **Next**.

e. Review the **Summary and Test** page.To test the settings, enter an e-mail address and then click **Test**.

f. Click **Finish** to complete the configuration and return to the **E-mail Setup** page.

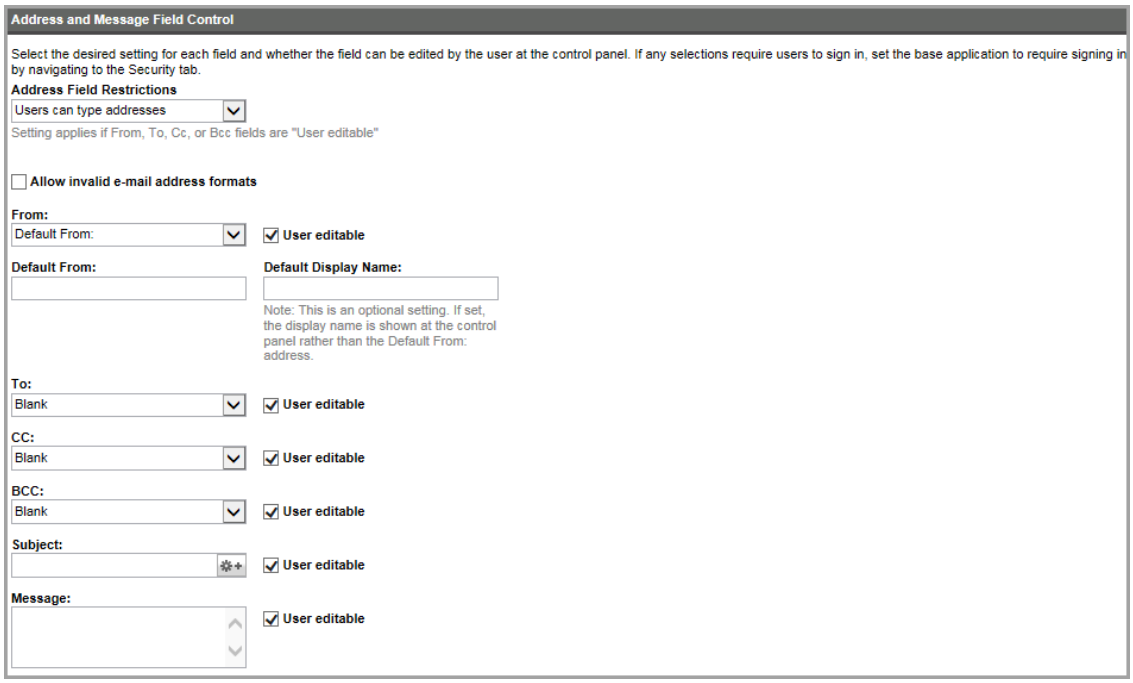
5. On the **Address and Message Field Control** section, complete the following steps to set up the address section:

a. In the **From** field, select **User's address (sign-in required)** from the drop-down list.

> **NOTE:** To prevent users from changing the **From** setting at the control panel, clear the **User editable** check box

b. Select the settings from the drop-down list for the following fields: **To**, **CC**, and **BCC**.

Figure 3-14 Address and Message Field Control



c.

6. On the **Signing and Encryption** section, complete the following steps:

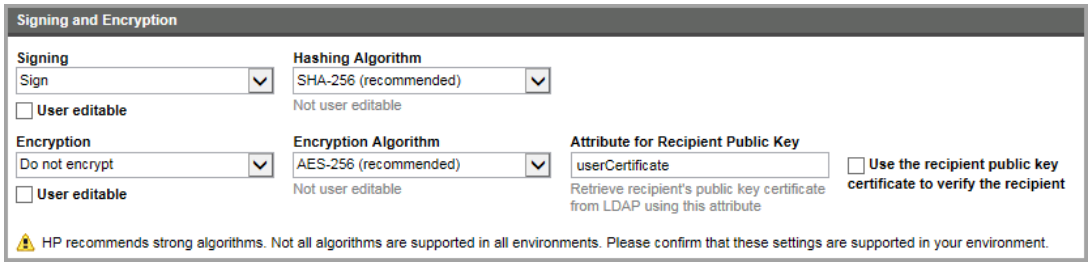
a. In the **Signing** field, select **Sign** from the drop-down list, and then clear the **User editable** check box.

b. In the **Hashing Algorithm**, select SHA-1 or SHA-256.

c. For the **Encryption** field, select **Do not encrypt** from the drop-down list, and then clear the **User editable** check box.

d. Select to clear the **Use the recipient public key certificate to verify the recipient** check box.

Figure 3-15 Signing and Encryption



7. Click the **Apply** button at the bottom of the **E-mail Setup** page to save any changes.

Save to Network Folder settings

Use the following steps to configure the **Save to Network Folder Setup**.

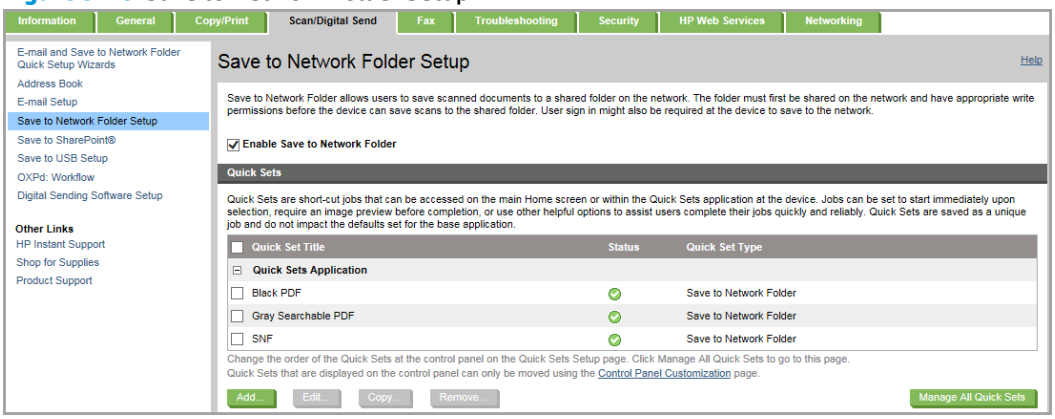
1. Open the EWS.

   For instructions, see Access the Embedded Web Server (EWS) on page 4

2. On the top navigation tabs, select the **Scan/Digital Send** tab.

3. In the left navigation pane, click **Save to Network Folder Setup**.

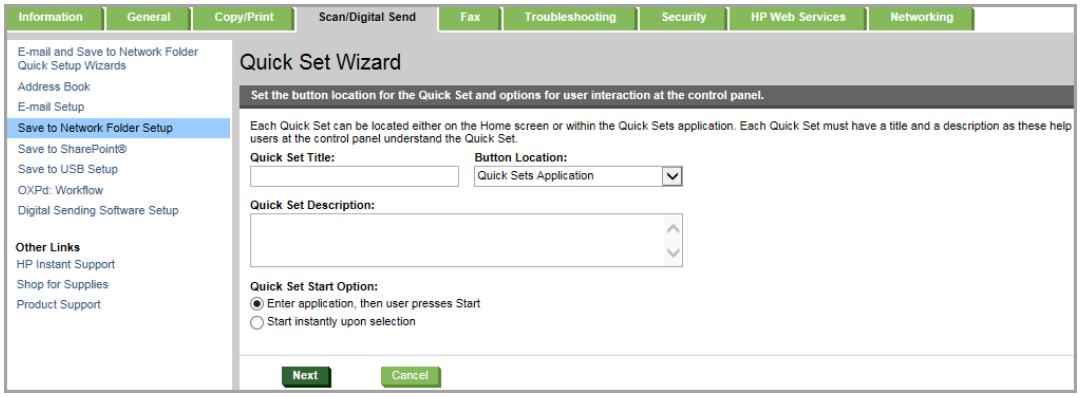
Figure 3-16 Save to Network Folder Setup



4. Select the **Enable Save to Network Folder** check box, and then click the **Add** button to start the wizard.

5. In the **Quick Sets** section, click **Add** to start the wizard.

Figure 3-17 Quick Set Wizard



6. In the **Quick Set Wizard**, complete the following tasks to define the control panel quick set options:

   a. Type a title in the **Quick Set Title** field

   b. Select the **Button Location** from the drop-down list.

   c. Type a description in the **Quick Set Description** field, if desired.

   d. Click **Next**.

   e. In the **Folder Settings** section, select one of the following options to set the folder destination:

      Option one : **Save to shared folders or FTP folders**

      i. Select the **Save to shared folders or FTP folders** radio button, and then click **Add**.

      ii. In the **UNC Folder Path:**, type the entire FQDN in the UNC folder path.

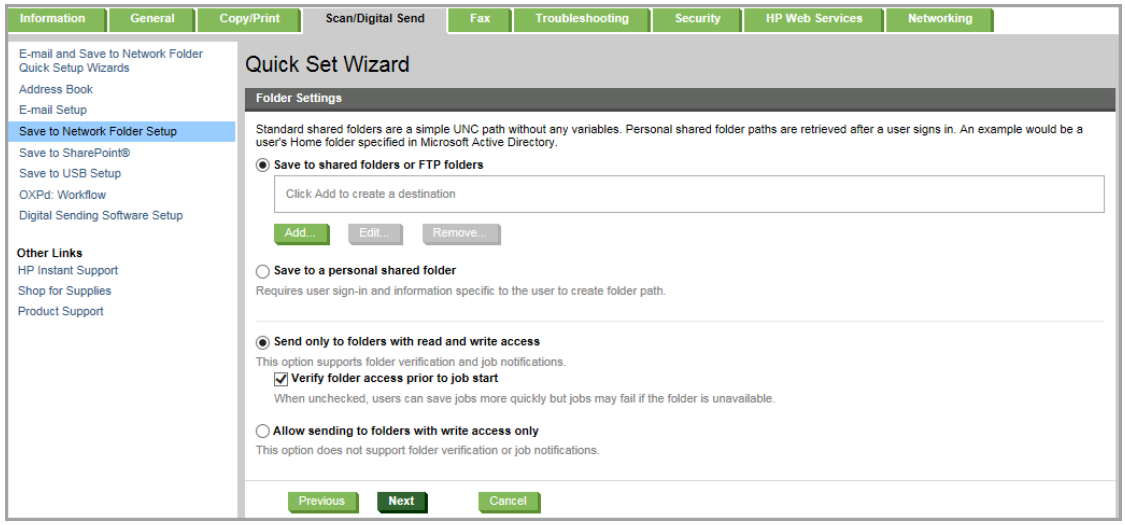
      iii. In the **Authentication Settings:**, select **Use credentials of user to connect after Sign in at the control panel**, and then select **OK**.

      Option two: **Save to a personal shared folder**

      i. Select the **Save to a personal shared folder** radio button.

ii. In the **Retrieve the device user's home folder using this attribute** field, type **homeDirectory**, and then click **Next**.

Figure 3-18 Folder settings in the Quick Set Wizard



iii. Complete the remaining settings as needed, and then click **Finish** to save the settings.

4 Device Resets

This chapter provides instructions to restore the HP printer to factory defaults.

- Restore Factory defaults
- Preboot Menu

Restore Factory defaults

NOTE: When the HP printer resets all settings to default, the **Authentication Agent** is also set to default.

Follow these steps to restore the HP printer to factory defaults:

1. On the printer's control panel, select Administration and then select the following menus:
   - General Settings
   - Restore Factory Settings

Figure 4-1 Administration menu

Figure 4-2 General Settings

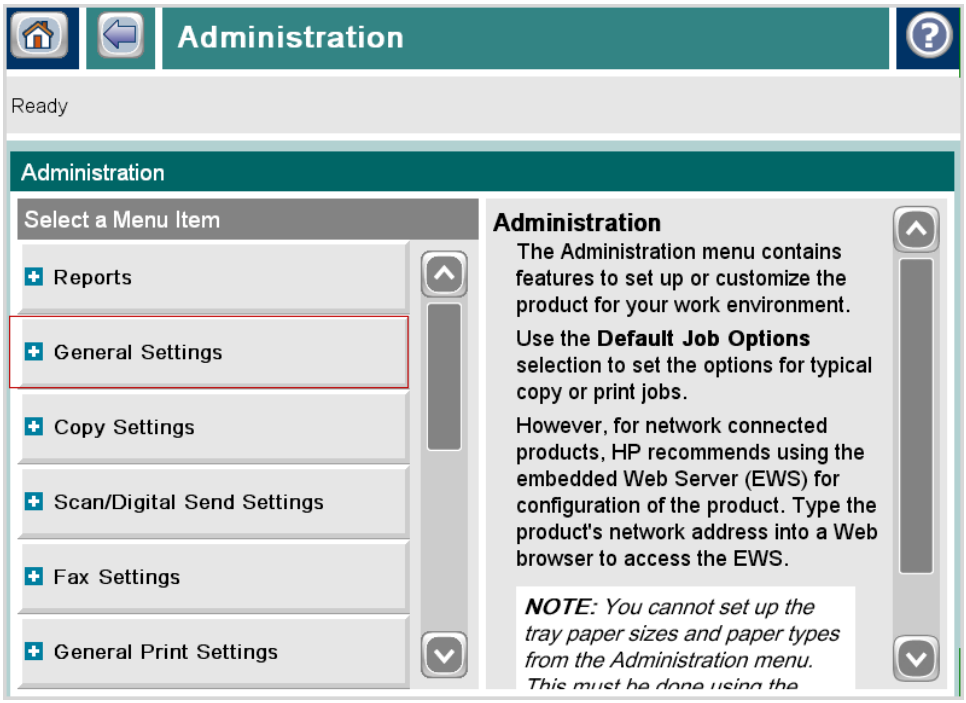
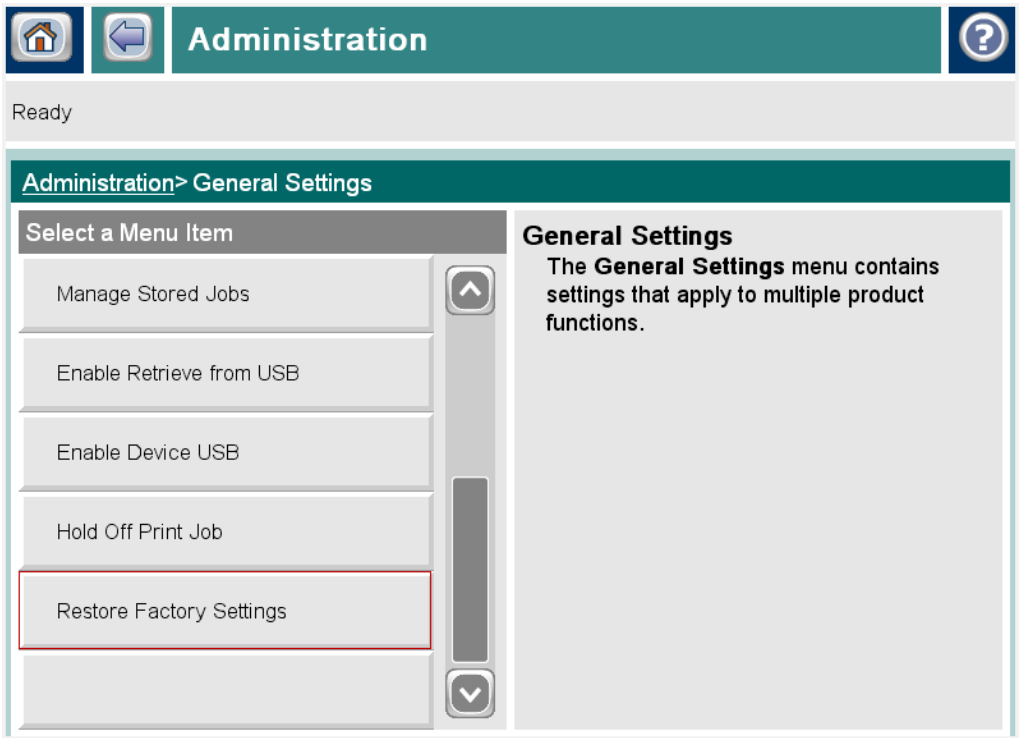


Figure 4-3 Restore Factory Settings



2. In Restore Factory Settings, select Restore or Cancel .

NOTE: Access code might be required to select this option.

3. Make sure to check and set the following settings before using the printer

- Date and Time (Time Zone)
- Network Settings (IP, DNS)
- Certificates
- Control Panel Customization

  Drag icons off the homescreen that are not used and place them in the lower section.

Preboot Menu

This section provides instructions on how to perform a Partial Clean using the printer's control panel when an error message displays on the control panel screen while rebooting.

The Partial Clean option removes all data except the firmware from the repository location where a backup copy of the master firmware bundle is downloaded and saved. When selecting this option, it allows a disk to be reformatted by removing the firmware image from the active directory without having to download new firmware code and the printer is bootable.

Partial Clean is similar Disk Initialization and Partial NVRAM in legacy firmware.

WARNING! Do not select Format Disk. This option performs a disk initialization for the entire disk, cleans all disk partitions, and removes all data. All custom settings, third-party solutions, firmware files, and the operating system are completely lost. A delete confirmation prompt is not provided. The system is not bootable after this action—a firmware download via an approved portable HDD must be performed to return the system to a bootable state

Follow these steps to perform a Partial Clean on the printer's control panel:

NOTE: Before performing a Partial Clean, make sure to back up the printer's configuration data.

To restore the customer-defined settings, select the Backup/Restore option in the Device Maintenance menu.

1. Turn the printer Off and then On.

   Wait for the Ready and Attention LEDs to illuminate and then dim out.

2. On the printer's control panel screen, touch the HP logo when 1/8 displays below the logo to open the Preboot menu.

   -or-

   Turn the printer Off and then On, and when the HP logo displays on the control panel and all three Ready, Data, and Attention LEDs illuminate solid, press ⊗

   -or-

   For M4555 and CM4540, press the Stop button ⊗ when the LED lights are illuminated.

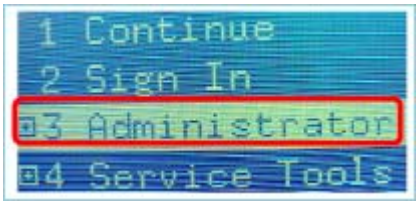
3. Depending on your printer (Touchscreen or LCD control panel), perform one of the following tasks:

   - Use the touch screen scrollbar or touch the down arrow ▼ to select Administrator, and then touch OK.

     OR

   - Press 3 (up) or 9 (down) keys to highlight the Administrator menu, and then press 6 to open the selected menu.

Figure 4-4 Preboot menu



4. Depending on your printer, perform one of the following tasks:

   Use the touch screen scrollbar or touch the down arrow ▼ to select Partial Clean, touch OK, and then touch OK again.

   OR

   Press 3 (up) or 9 (down) keys to highlight the Partial Clean menu, and then press 6 to open the selected option.

   Figure 4-5 Partial Clean option

5. Depending on your printer, perform one of the following tasks:

   Touch the Back button ⮌, touch Continue, and then touch OK.

   OR

   Press 5 or the Back button to return to the first menu and then press 6 to select Continue.

   The printer should continue to boot up.

NOTE: A reboot will automatically restore the firmware files from the repository, but does not restore any customer-defined settings.

A Licenses

This solution from HP uses and contains open source code and libraries from Heimdal Kerberos 5, OpenLDAP, OpenSC, and OpenSSL. Following are acknowledgements, copyrights, and license information associated with these open source solutions.

- Heimdal Kerberos
- OpenLDAP
- OpenSC
- OpenSSL
- SHA-2

Heimdal Kerberos

This product contains Heimdal Kerberos in binary form. Use of this software is governed by the terms of the license below:

Copyright © 1995 - 2009 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenLDAP

This product contains OpenLDAP in binary form. Use of this software is governed by the terms of the license below:

The OpenLDAP Public License

Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright © 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

This product contains engine_pkcs11 in binary form. Use of this software is governed by the terms of the license below:

Copyright © 2002 Juha Yrjola. All rights reserved.

Copyright © 2001 Markus Friedl.

Copyright © 2003 Kevin Stefanik

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSC

OpenSC Credits

OpenSC was written by (or uses code copied from):

- Alon Bar-Lev
- Andrea Frigido
- Andreas Jellinghaus
- Antonino Iacono
- Antti Partanen
- Antti Tapaninen
- Benjamin Bender
- Bert Vermeulen
- Boris Kröger
- Bud P. Bruegger
- Carlos Prados
- Chaskiel Grundman
- Danny De Cock
- David Corcoran
- Douglas E. Engert
- Eric Dorland
- Franz Brandl
- Geoff Thorpe
- Gürer Özen for TUBITAK / UEKAE
- Jamie Honan
- Jean-Pierre Szikora
- João Poupino
- Joe Phillips
- Juan Antonio Martinez
- Juha Yrjölä
- Jörn Zukowski
- Kevin Stefanik
- Ludovic Rousseau

- Marc Bevand
- Marie Fischer
- Markus Friedl
- Martin Paljak
- Mathias Brossard
- Matthias Brüstle
- Nils Larsch
- Olaf Kirch
- Peter Koch
- Priit Randla
- Robert Bihlmeyer
- Sirio Capizzi
- Stef Hoeben
- Timo Teräs
- Todd C. Miller
- Viktor Tarasov
- Villy Skyttä
- Weitao Sun
- Werner Koch
- William Wanders

and

- Zetes
- g10 Code GmbH
- [http://www.opentrust.com/ OpenTrust] (ancient Idealx)
- Dominik Fischer

License

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

OpenSC does not include the official PKCS#11 header file, because that file is under a non-free license. Instead OpenSC contains a rewritten header file from scute project under this license:

/* pkcs11.h Copyright 2006, 2007 g10 Code GmbH Copyright 2006 Andreas Jellinghaus This file is free software; as a special exception the author gives unlimited permission to copy and/or distribute it, with or without modifications, as long as this notice is preserved. This file is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, to the extent permitted by law; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. */

OpenSC (signer) also includes header file:

Java Runtime Interface Copyright (c) 1996 Netscape Communications Corporation. All rights reserved. dp Suresh <dp@netscape.com>

OpenSC also includes a copy of [http://www.geocities.com/bsittler/ my_getopt]:

my_getopt - a command-line argument parser Copyright 1997-2001, Benjamin Sittler

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSC can be compiled with OpenSSL:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

OpenSC uses autoconf m4 macros by

m4/autoconf macros by Bruno Haible

Copyright (C) 2001-2005 Free Software Foundation, Inc.

Copyright (C) 2002, 2003 Free Software Foundation, Inc.

using pkg-config and pkg.,4 autoconf macro by

Copyright (C) 2004 Scott James Remnant

OpenSC includes svn2cl by

svn2cl Arthur de Jong

Copyright (C) 2004, 2005 Arthur de Jong.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSC includes strlcpy.c (from ftp://ftp.openbsd.org/pub/OpenBSD/src/lib/libc/string/) by

Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenSC can be compiled with zlib:

This product includes general purpose compression software written by Jean-loup Gailly and Mark Adler for the 'Zlib' project (http://www.zlib.net).

Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

OpenSSL

This product contains OpenSSL in binary form. Use of this software is governed by the terms of the license below:

Copyright © 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

SHA-2

This product may include the following software in binary form: SHA-2 implementation by Olivier Gay. Use of this software is governed under terms of the following license:

FIPS 180-2 SHA-224/256/384/512 implementation

Last update: 02/02/2007

Issue date: 04/30/2005

Copyright (C) 2005, 2007 Olivier Gay (olivier.gay@a3.epfl.ch).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

B Warranty Service

HP Limited Warranty Statement

HP Product	Duration of Limited Warranty
HP SmartCard NIPRNet Solution for US Government and the HP SmartCard SIPRNet Solution for US Government for U. S. Government	1 Year

1. HP warrants to you, the original end-user customer, that HP hardware and accessories will be free from defects in materials and workmanship after the original date of purchase, for the period specified above. If HP receives notice of such defects during the warranty period, HP will, at its option, either repair or replace, products, that prove to be defective. Replacement products may be either new or equivalent in performance to new. If the original end-user customer transfers the HP hardware and accessories to another user, warranty service is available to that user only for the remainder of the original warranty period. This Limited Warranty applies only to authentic HP-branded hardware products sold by or leased from Hewlett-Packard Company, its worldwide subsidiaries, affiliates, authorized resellers, or authorized country/region distributors.

2. HP warrants to you that HP software will not fail to execute its programming instructions after the date of purchase, for a period specified above, due to defects in material and workmanship when properly installed and used. If HP receives notice of such defects during the warranty period, HP will replace software that does not execute its programming instructions due to such defects.

3. HP does not warrant that the operation of HP products will be uninterrupted or error free. If HP is unable, within a reasonable time, to repair or replace any product to a condition as warranted, you will be entitled to a refund of the purchase price upon prompt return of the product.

4. HP products may contain remanufactured parts equivalent to new in performance or may have been subject to incidental use.

5. Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts or supplies not supplied by HP, (c) unauthorized modification or misuse, (d) operation outside of the published environmental specifications for the product, or (e) improper site preparation or maintenance.

6. TO THE EXTENT ALLOWED BY LOCAL LAW, THE ABOVE WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND HP SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE. Some countries/regions, states or provinces do not allow limitations on the duration of an implied warranty, so the above limitation or exclusion might not apply to you. This warranty gives you specific legal rights and you might also have other rights that vary from country/region to country/region, state to state, or province to province.

7. HP's limited warranty is valid in any country/region or locality where HP has a support presence for this product and where HP has marketed this product. The level of warranty service you receive may vary according to local standards. HP will not alter form, fit or function of the product to make it operate in a country/region for which it was never intended to function for legal or regulatory reasons.

8. TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS WARRANTY STATEMENT ARE YOUR SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED ABOVE, IN NO EVENT WILL HP OR ITS SUPPLIERS BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL (INCLUDING LOST PROFIT OR DATA), OR OTHER DAMAGE, WHETHER BASED IN CONTRACT, TORT, OR OTHERWISE. Some countries/regions, states or provinces do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

THE WARRANTY TERMS CONTAINED IN THIS STATEMENT, EXCEPT TO THE EXTENT LAWFULLY PERMITTED, DO NOT EXCLUDE, RESTRICT OR MODIFY AND ARE IN ADDITION TO THE MANDATORY STATUTORY RIGHTS APPLICABLE TO THE SALE OF THIS PRODUCT TO YOU.

Customer self-repair warranty service

HP products are designed with many Customer Self Repair (CSR) parts to minimize repair time and allow for greater flexibility in performing defective parts replacement. If during the diagnosis period, HP identifies that the repair can be accomplished by the use of a CSR part, HP will ship that part directly to you for replacement. There are two categories of CSR parts: 1) Parts for which customer self repair is mandatory. If you request HP to replace these parts, you will be charged for the travel and labor costs of this service. 2) Parts for which customer self repair is optional. These parts are also designed for Customer Self Repair. If, however, you require that HP replace them for you, this may be done at no additional charge under the type of warranty service designated for your product.

Based on availability and where geography permits, CSR parts will be shipped for next business day delivery. Same-day or four-hour delivery may be offered at an additional charge where geography permits. If assistance is required, you can call the HP Technical Support Center and a technician will help you over the phone. HP specifies in the materials shipped with a replacement CSR part whether a defective part must be returned to HP. In cases where it is required to return the defective part to HP, you must ship the defective part back to HP within a defined period of time, normally five (5) business days. The defective part must be returned with the associated documentation in the provided shipping material. Failure to return the defective part may result in HP billing you for the replacement. With a customer self repair, HP will pay all shipping and part return costs and determine the courier/carrier to be used.