Legal notices

(c) Copyright 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HEWLETT-PACKARD required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HEWLETT-PACKARD 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. HEWLETT-PACKARD shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

Printed in the US
# Revision history

**Table 1** Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Edition</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2012</td>
<td>2</td>
<td>Version 1.2.0</td>
</tr>
<tr>
<td>September 2013</td>
<td>3</td>
<td>Version 1.3.0</td>
</tr>
<tr>
<td>December 2013</td>
<td>4</td>
<td>Version 1.3.0 Feature Pack 1</td>
</tr>
<tr>
<td>February 2014</td>
<td>5</td>
<td>Version 1.3.0 Feature Pack 1 (update)</td>
</tr>
<tr>
<td>May 2014</td>
<td>6</td>
<td>Version 1.3.0 Feature Pack 1 (update)</td>
</tr>
<tr>
<td>July 2014</td>
<td>7</td>
<td>Version 1.3.0 Feature Pack 1 (update)</td>
</tr>
<tr>
<td>September 2014</td>
<td>8</td>
<td>Version 1.4.0</td>
</tr>
<tr>
<td>October 2014</td>
<td>9</td>
<td>Version 1.4.0 (update)</td>
</tr>
<tr>
<td>October 2015</td>
<td>10</td>
<td>Version 1.4.0 (update)</td>
</tr>
</tbody>
</table>
Contents

1 Introduction
   1-1 HP CR Embedded Device Client overview ................................................................. 1
   1-1-1 Main components of the environment................................................................. 3
   1-1-2 Installation components ..................................................................................... 4
   1-1-3 Document workflow .......................................................................................... 4
   1-1-4 Deploying the HP CR Embedded Device Client ................................................ 6

1-2 Basic requirements ................................................................................................. 7
   1-2-1 Supported devices .............................................................................................. 7
   1-2-2 Server requirements ......................................................................................... 8
   1-2-3 Device authentication requirements ............................................................... 9
   1-2-4 Supporting large color documents ............................................................... 9

1-3 Planning for Device Deployment ...................................................................... 10
   1-3-1 Planning for HTTPS .......................................................................................... 10
   1-3-2 Device group planning .................................................................................... 11
   1-4 Online help and related documentation .......................................................... 11

2 Setting up a CA Certificate and SSL
   2-1 Downloading the MakeCert executable ............................................................... 13
   2-2 Creating the certificate ........................................................................................ 13
   2-3 Installing the certificate to Internet Information Services (IIS) ......................... 14
   2-4 Adding the certificate to the Client certificate directory .................................. 14
   2-5 Creating an SSL binding ..................................................................................... 15
   2-6 Requiring SSL for the virtual web sites ............................................................ 15
   2-7 Verifying the SSL binding .................................................................................. 15
   2-8 Enabling directory browsing in IIS .................................................................... 15
   2-9 Verifying HTTPS browsing ................................................................................ 16
   2-10 Editing the OmISAPIU.xml file ...................................................................... 16
   2-11 Editing the Bootstrap.xml file ........................................................................ 16

3 HP CR Embedded Device Client installation
   3-1 Installing the HP CR Embedded Device Client ................................................. 19
   3-2 Installing the HP CR Embedded Device Client on a remote system ............... 20

4 Creating Device Groups on the HP CR Server Administrator
   4-1 Creating a group of devices ................................................................................. 21
   4-2 Specifying buttons for devices ......................................................................... 27
      4-2-1 Adding new buttons ..................................................................................... 28
      4-2-2 Configuring button properties ................................................................... 29

5 Installing buttons on a new device
   5-1 Adding a new device and installing buttons ....................................................... 47
   5-2 Configuring device authentication .................................................................... 49
      5-2-1 Configuring LDAP authentication .............................................................. 49
      5-2-2 Configuring HP device authentication ....................................................... 50
   5-3 Configuring the server ...................................................................................... 51

6 Configuring HP Pro Devices
   6-1 Installing the OPS Server .................................................................................. 53
   6-2 Exporting the OPS server certificate to the Client certificate directory ......... 58
   6-3 Importing the OPS certificate into the device EWS ........................................ 58
Contents

6-4 OPS registration ......................................................................................................................................... 59
6-5 HTTPS support using the OPS-created certificate ................................................................................. 59
  6-5-1 Creating an SSL binding ................................................................................................................... 59
  6-5-2 Requiring SSL for the virtual web sites ........................................................................................... 60
  6-5-3 Enabling directory browsing in IIS .................................................................................................... 60
  6-5-4 Verifying the SSL binding ................................................................................................................. 60
  6-5-5 Verifying HTTPS browsing .............................................................................................................. 60
  6-5-6 Editing the OmISAPIU.xml file ......................................................................................................... 60
  6-5-7 Editing the Bootstrap.xml file ........................................................................................................... 61

7 Configuring HP S900 Series devices
  7-1 Enabling HTTPS for SSL on HP S900 Series devices ........................................................................... 63
  7-2 Adding buttons to HP S900 Series devices ........................................................................................... 63
    7-2-1 Creating a group with a Nested button ............................................................................................. 64
    7-2-2 Launching the Device Group XML information .................................................................................. 64
    7-2-3 Creating the URL string to use for button installation ....................................................................... 65
    7-2-4 Installing the buttons to the device ................................................................................................... 66
  7-3 Configuring device authentication ........................................................................................................... 66

8 Configuring HP FutureSmart, OZ and Pro Devices to use the OPS server certificate for HTTPS environments
  8-1 Exporting the certificate to the Embedded Device Client directory for FutureSmart and OZ devices ........ 67

9 Using HP’s Web Jetadmin application to install HP CR Embedded Device Client buttons on HP devices
  9-1 Supported devices ...................................................................................................................................... 69
  9-2 Exporting the XML files ......................................................................................................................... 70
  9-3 Manually importing a certificate .............................................................................................................. 71
  9-4 Installing HP CR Embedded Device Client buttons .................................................................................. 72

10 Testing
  10-1 Testing the Routing Sheet feature ........................................................................................................... 83
  10-2 Testing the Device Administrator user interface ..................................................................................... 84
1 Introduction

HP CR features are accessible where the users need them most—on the web, office machines, multifunction devices, and business systems that are an integral part of the communication workflow.

As an intranet-based application for multifunction devices and business systems, HP CR supports software solutions to deploy the HP CR Embedded Device Client to multifunction devices running OXPd SDK v1.6.x and Pro devices running OXPd v1.7.

NOTE: The information in this document is written for system administrators with detailed knowledge of the HP CR server and the HP device.

This section describes:

HP CR Embedded Device Client overview (1)
Basic requirements (7)
Online help and related documentation (11)

Procedures for installation, configuration, and testing are provided in the remainder of this document.

1-1 HP CR Embedded Device Client overview

The HP CR Embedded Device Client brings the versatile document routing capabilities of HP CR to supported HP devices running OXPd SDK library v1.6.x as well as a limited set of devices running OXPd SDK library v1.7. These capabilities are founded in Distribution Rule technology.

The HP CR Embedded Device Client runs on OXP, an ASP.NET layer sitting between the HP device and the HP CR server. It communicates between the OXPd SDK installed on the HP device and the HP CR server via the Embedded HP CR for Intelligent Devices application.

Figure 1-1 HP CR scanning features on the HP Device running the HP CR Embedded Device Client

In the main menu, the HP CR Embedded Device Client presents the device user with several HP CR scanning features.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Login Required</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Distributions</td>
<td>The user selects Public Distributions and then selects a Public Distribution option or Distribution Rule. The device scans and delivers the document to the HP CR server via HTTP/HTTPS protocol. The server decodes the Distribution Rules and distributes the document to the intended recipient.</td>
<td>No</td>
<td>Public Distribution options are associated with a special user account that is set up for this purpose. The user account associated with this feature must be able to create Distribution Rules. This requires access to HP CR End User Interface (where the user can create the Distribution Rules and Routing Sheets).</td>
</tr>
<tr>
<td>Personal Distributions</td>
<td>The user selects Personal Distributions, logs in to the device, and selects a Personal Distribution option, or Distribution Rule. The device scans and delivers the document to the HP CR server via HTTP/HTTPS protocol. The server decodes the Distribution Rules and distributes the document to the intended recipient.</td>
<td>Yes</td>
<td>The device user must be able to create Distribution Rules. This requires access to HP CR End User Interface (where the user can create the Distribution Rules and Routing Sheets).</td>
</tr>
<tr>
<td>Scan to Me</td>
<td>The user selects Scan to Me and logs in to the device. The device scans and delivers the document to the HP CR server (via HTTP/HTTPS protocol) where it is processed using the device user’s personal Scan to Me directive and distributed to the intended recipients. Or the scanned document is emailed to the sender (the default).</td>
<td>Yes</td>
<td>Scan to Me is an advanced feature of HP CR End User Interface. It enables the server to process all HP CR messages from the same user with the same Distribution Rule. Scan to Me requires access to HP CR End User Interface (where the user can create the Distribution Rules and Routing Sheets). In addition, Scan to Me must be configured in the HP CR End User Interface and on the server. For more information, consult the Basic requirements (7) and the HP Capture and Route (HP CR) User Guide.</td>
</tr>
<tr>
<td>Routing Sheet</td>
<td>The user selects Routing Sheet. The device scans and delivers the document to the HP CR server via HTTP/HTTPS protocol. The HP CR server then decodes the Distribution Rule and distributes the document to intended recipients.</td>
<td>No</td>
<td>The device user must be able to generate Routing Sheets. This requires access to HP CR End User Interface (where the user can create the Routing Sheets).</td>
</tr>
<tr>
<td>Scan to Folder</td>
<td>The device scans and delivers the document to a folder (HP Flow CM, Dropbox™, Microsoft® OneDrive™,(Personal), Google Drive™, box, FTP or network folder share) predetermined by your system administrator. The HP CR server picks up the scanned document from the network folder, processes it and delivers it to the intended folder.</td>
<td>Yes, except for use with FTP or network folder share</td>
<td></td>
</tr>
<tr>
<td>Fax</td>
<td>This option allows the user to do a walk-up fax. The user enters the fax number and can additionally add a cover page to fax. The device scans and delivers the document to the HP CR server via HTTP/HTTPS protocol. The HP CR server sends the fax to the intended recipients.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Login Required</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fax Release</td>
<td>This option allows the user to hold or release and print faxes as needed. The user selects the Fax Release button and logs in to the device. Once they enter the Fax number of interest, they can Enable Manual Hold to override the current print schedule, release an existing Manual Hold or Print Pending Jobs (all the faxes currently in queue for the selected fax number).</td>
<td>Yes</td>
<td>The user account associated with this feature must have access to the Administration Node on the HP CR End User Interface, where they can configure Fax Release Schedule Calendars.</td>
</tr>
<tr>
<td>Scan to My Files</td>
<td>The user selects Scan to My Files button and logs in to the device. The device scans and delivers the document to the HP CR server (via HTTP/HTTPS protocol) where it is processed and distributed to the My Files section of the user End User Interface client.</td>
<td>Yes</td>
<td>All jobs scan.</td>
</tr>
<tr>
<td>Nested Buttons</td>
<td>The Nested Buttons feature provides the ability to configure one top-level button that all other HP CR buttons will display under, minimizing the front panel home screen real estate. For example, one button can be configured and labeled “HP CR.” This button would be the only HP CR button to display on the home screen. Pressing this button would then display any other enabled buttons (such as Routing Sheets, Personal Distributions, etc.).</td>
<td>Yes</td>
<td>Login is required only if using Device Authentication and if one of the Nested Buttons needs authentication.</td>
</tr>
<tr>
<td>Mobile Reservations</td>
<td>The user selects the Mobile Reservations button and enters a Mobile Scan Reservation Code generated by the Mobile Client. The device decodes the reservation code and distributes the document to intended recipients.</td>
<td>No</td>
<td>Mobile Reservations are generated by the Mobile Client and require a Mobile Client license.</td>
</tr>
<tr>
<td>Device Information</td>
<td>This option allows users to access a screen of detailed information about the multi-function printer (MFP) with which they’re working, including the device name, hostname, IP address, serial number, fax number, Inbound/Outbound fax support, and business unit.</td>
<td>No</td>
<td>Users can print the screen information to the device.</td>
</tr>
<tr>
<td>Job Queue</td>
<td>You can use the Job Queue option to obtain a list of jobs submitted to the HP CR server from a specific MFP or by a specific user. For all users, Job Queue can provide a list of all previously scanned jobs from an MFP or all faxes sent from the device. The system administrator configures the type of items that can be reported. For authenticated users, Job Queue can list any previously faxed items associated with the logged-in user.</td>
<td>Optional</td>
<td>Users can select any job from the list and print the job details to the device.</td>
</tr>
</tbody>
</table>

1-1-1  Main components of the environment

The HP CR Embedded Device Client environment consists of the following components.

- **HP CR Server** – The HP CR server is the main back-end server for processing and routing documents.
NOTE: HP CR installs the HP CR Embedded Device Client as part of the server install. No separate installation of this component is required unless the HP CR Embedded Device Client is installed on a remote system, and then the HP CR Intelligent Device Client would be installed on the remote system as well.

- **HP CR Embedded Device Client** – See [Installing the HP CR Embedded Device Client](#) (19).
- **HP Device** – See [Supported devices](#) (7) for a list with minimum firmware requirements.

### 1-1-2 Installation components

The HP CR Embedded Device Client setup includes multiple components detailed in this table.

**Table 2** Description of installation components with locations and functions

<table>
<thead>
<tr>
<th>Component</th>
<th>Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP CR Embedded Device Client Install</td>
<td>\HP\HPCR\Clients</td>
<td>The setup contains the setup.exe file for HP OXPd Device Client. Use this file to install the HP CR Embedded Device Client.</td>
</tr>
<tr>
<td>HP CR Embedded Device Client Configuration Manager</td>
<td>Devices node in the HP CR Server Administrator</td>
<td>The Device Client Configuration node is a management tool installed with the HP CR Server Administrator, and is used to manage settings and options that will be available on the HP MFP Device.</td>
</tr>
</tbody>
</table>

### 1-1-3 Document workflow

The workflow that moves a document from the device to its final destination involves the user, the device, the HP CR Embedded Device Client, Embedded HP CR for Intelligent Devices (HP CR ISAPI web server extension), and the HP CR server. An understanding of this workflow can be helpful in troubleshooting an Embedded HP CR integration.

In its most basic workflow, when a device user scans a document, the device submits the document to HP CR Embedded Device Client via HTTP/HTTPS protocol. The HP CR Embedded Device Client then routes the document to the HP CR server via HTTP/HTTPS protocol. The Dispatch component applies rules to the message and HP CR server processes the message and routes it to the intended recipients.

The following workflow applies to the features Fax, Routing Sheet, Scan to Folder and Scan to Me.

**IMPORTANT:** For Scan to Me, the device user must authenticate himself at the device using the configured authentication type. For more information, refer to the description of configuring authentication in the [HP Capture and Route (HP CR) Installation Guide](#).

**Figure 1-2** Workflow for Fax, Routing Sheet, Scan to Folder and Scan to Me
A-The user selects an HP CR scanning feature and scans a document.

B-The device delivers the document to HP CR Embedded Device Client via HTTP/HTTPS protocol.

C-The HP CR Embedded Device Client sends the document to Embedded HP CR for Intelligent Devices (HP CR ISAPI Web Server Extension) via HTTP/HTTPS protocol which in turn routes the document to the HP CR server.

D-The Dispatch component applies rules to the message, and the server processes the message accordingly.

When a user begins a scan session with the Public Distributions, Personal Distributions, or Scan to My Files option, the device requests the HP CR Embedded Device Client retrieve Distribution Rules.

NOTE: For Personal Distributions, the device user must authenticate himself at the device using the configured authentication type. For more information, refer to the description of configuring authentication in the HP Capture and Route (HP CR) Installation Guide.

The HP CR Embedded Device Client then submits a request to Embedded HP CR for Intelligent Devices (HP CR ISAPI web server extension) which retrieves the data from the HP CR server and supplies it to the HP CR Embedded Device Client. As soon as the HP CR Embedded Device Client returns the data to the device, the basic workflow resumes.
**Figure 1-3 Workflow for Personal Distributions and Public Distributions**

A - The user selects Personal or Public Distribution feature. (If the user chooses Personal Distribution, he logs into the device.) The device requests the list of Distribution Rules from the server. The HP CR server returns the requested data. The user selects a Distribution Rule from the list and scans document.

B - The device delivers the document to the HP CR Embedded Device Client via HTTP or HTTPS protocol.

C - HP CR Embedded Device Client sends the document to Embedded HP CR for Intelligent Devices (HP CR ISAPI Web Server Extension) via HTTP/HTTPS protocol which in turn routes the document to the HP CR server.

D - The Dispatch component applies rules to the message, and the server processes the message accordingly.

### 1-1-4 Deploying the HP CR Embedded Device Client

1. Complete the installation requirements. ([Device authentication requirements](#), 9)

   **NOTE:** If you are planning to use HTTPS protocol, you must create a CA certificate before installing the HP CR Embedded Device Client. Refer to [Section 2: Setting up a CA Certificate and SSL](#) (13).

2. Install the HP CR Embedded Device Client. See [Installing the HP CR Embedded Device Client](#) (19).

3. Configure the embedded Web server of the device. Refer to the description of required configuration in the [HP Capture and Route (HP CR) Installation Guide](#).
4. Configure the HP CR server. Refer to the description of configuring the server in the HP Capture and Route (HP CR) Installation Guide.

5. Configure optional capabilities. Refer to the HP CR Server Administrator help.

6. Test the HP CR scanning features on the device. Refer to Section 10: Testing (83).

7. Troubleshoot the setup if necessary. Refer to the HP CR Server Administrator help.

1-2 Basic requirements

1-2-1 Supported devices

HP CR supports the HP CR Embedded Device Client on all devices listed in this section. Consult HP to determine compatible firmware versions for supported devices.

Table 3 List of devices supported with the HP CR Embedded Device Client

<table>
<thead>
<tr>
<th>Device</th>
<th>Group</th>
<th>Supported Firmware</th>
<th>OXPd Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>LaserJet M3035 MFP</td>
<td>20</td>
<td>48.301.7</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>LaserJet M4345 MFP</td>
<td>20</td>
<td>48.301.7</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>LaserJet M4349 MFP</td>
<td>20</td>
<td>48.301.7</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>LaserJet M5035 MFP</td>
<td>20</td>
<td>48.301.7</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>LaserJet M5039 MFP</td>
<td>20</td>
<td>48.301.7</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>LaserJet M9040 MFP</td>
<td>20</td>
<td>51.252.1</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>LaserJet M9050 MFP</td>
<td>20</td>
<td>51.252.1</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>LaserJet M9059 MFP</td>
<td>20</td>
<td>51.252.1</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>Color LaserJet CM 4730 MFP</td>
<td>20</td>
<td>50.282.0</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>Color LaserJet CM 6030 MFP</td>
<td>40</td>
<td>52.252.2</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>Color LaserJet CM 6040 MFP</td>
<td>40</td>
<td>52.252.2</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>Color LaserJet CM 6049 MFP</td>
<td>40</td>
<td>52.252.2</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>Color LaserJet CM 3530 MFP</td>
<td>50</td>
<td>53.231.6</td>
<td>1.6.3.2, 1.7</td>
</tr>
<tr>
<td>Color LaserJet CM 4540 MFP</td>
<td>XX</td>
<td>2302908_435001</td>
<td>1.6.3.2, 1.7</td>
</tr>
<tr>
<td>ScanJet 7000n</td>
<td>XX</td>
<td>2201075_229185</td>
<td>1.6.3.2</td>
</tr>
<tr>
<td>ScanJet 8500n</td>
<td>XX</td>
<td>2302829_434645</td>
<td>1.6.3.2, 1.7</td>
</tr>
<tr>
<td>LaserJet Flow M525 MXP</td>
<td>XX</td>
<td>2302908_435018</td>
<td>1.6.3.2a, 1.7</td>
</tr>
<tr>
<td>LaserJet Flow M575 MXP</td>
<td>XX</td>
<td>2302908_435018</td>
<td>1.6.3.2, 1.7</td>
</tr>
<tr>
<td>LaserJet M775 MFP</td>
<td>XX</td>
<td>2302908_435017</td>
<td>1.6.3.2, 1.7</td>
</tr>
<tr>
<td>LaserJet M4555 MFP</td>
<td>XX</td>
<td>2302908_435006</td>
<td>1.6.3.2, 1.7</td>
</tr>
<tr>
<td>HP Color LaserJet flow MFP M527</td>
<td>XX</td>
<td>2306273_536016</td>
<td>1.7.1</td>
</tr>
<tr>
<td>HP Color LaserJet flow MFP M577</td>
<td>XX</td>
<td>2306272_536017</td>
<td>1.7.1</td>
</tr>
<tr>
<td>HP Color LaserJet flow MFP M830</td>
<td>XX</td>
<td>2302908_435011</td>
<td>1.6.3.2, 1.7</td>
</tr>
</tbody>
</table>
Introduction

If you need to update the Deviceloader.xml to support new devices, refer to the HP CR administrator online help.

NOTE: All LaserJet models listed here are part of the **MFP series**. Other LaserJet models that are part of the **printer series** do not have the scanning capabilities required to support HP CR Embedded Device Client.

NOTE: OXPd:SolutionInstaller only supports network-enabled device models. OXPd:SolutionInstaller also requires that the device on which it is running has a writable, non-volatile mass storage partition.

### 1-2-2 Server requirements

Server requirements for the HP CR Embedded Device Client are automatically configured during installation. They include the following:

- HP CR Server v1.4.0
  - with an appropriate device license
  - fax-enabled to support fax-based features
- At least one fax-enabled connector to support fax-based features
- HP CR ISAPI Device Client (included with default server install)
- ASP.NET 3.5.1

NOTE: To allow the installation prerequisite process to install Microsoft .NET 3.5.1, the system must have internet access. Microsoft .NET 3.5.1 is required to install the device client application.
1-2-3 Device authentication requirements

The HP CR Embedded Device Client supports the following authentication methods. Some of these require setup prior to using the device for scanning. It is recommended that an authentication is selected and verified before installing the device client.

The types of authentication are:

- **Device** authentication uses the native HP authentication built into the device. This is configurable from the embedded web server.
- **Email** authentication occurs when a user logs into the device with a valid email address that was created in Active Directory.
- **Login** authentication occurs when a users logs into the device with a user name and password as defined in the Active Directory.
- **Pin** authentication displays on the device a text box into which a user enters a PIN login.

**NOTE:** PIN refers to an attribute of Active Directory and it can be changed to point to any other Active Directory field by modifying the LDAP Lookup Settings Filter field values on the Authentication tab of the Device Group Properties. The default attribute is set to use employeeID.

**NOTE:** HP Pro Devices do not support the Device authentication method on their own and will require a stacked solution with another authentication service installed. For example: HP AC authentication set in the Pro device when Device authentication is set in HP CR.

1-2-4 Supporting large color documents

The following configuration changes increase the success rate for large document scanning.

To support large color documents, you must adjust settings as follows:

- Increase the **Sleep Schedule** from 10 minutes to the maximum, which is 4 hours.
- Increase the **Inactivity Timeout** in the device Embedded Web Server to 300 seconds.
- Increase the **ASP > Session Properties > Time-out** value in Internet Information Service Manager (IIS).

1-2-4-1 Sleep Schedule

To increase the **Sleep Schedule**:

1. Log in to the Embedded Web Server on the HP MFP.
2. Select the **General** tab and locate the **Sleep Schedule** section in the left pane.
3. Increase the **Sleep Delay** value to the maximum allowable time – 120 minutes.
4. Click **Apply**.

1-2-4-2 Inactivity Timeout

To increase the **Inactivity Timeout** in the device Embedded Web Server:

1. Log in to the Embedded Web Server on the HP MFP.
2. Select the **General** tab and locate the **Control Panel Administration** menu.
3. Select Administration and click Display Settings.
4. Increase the Inactivity Timeout value to 300 seconds.

1-2-4-3  ASP Session Properties

To change the ASP Session setting in IIS:
1. Open Internet Information Services (IIS 7) Manager.
2. Select Sites > DeviceClient.
3. Double-click ASP.
4. Under Services, double-click Session Properties.
5. Increase the Time-out value to 1:20:00. The default is :20:00
6. Click Apply.
7. Restart IIS.

1-3  Planning for Device Deployment

Before you begin installing and configuring your device environment, it is recommended that you review and plan your device configuration. For example, you may want to consider:

- Whether you will group your devices by model, location or functionality.
- If you want to use a Local or Remote IIS server configuration.
- Whether your OPS server is local or remote to your HP CR server.

Also, keep in mind that using HP Pro devices in your environment requires an OPS server installation. See Configuring HP Pro Devices (53) for more information.

1-3-1  Planning for HTTPS

Depending on the devices in your environment, use one of the following two supported certificate types to configure HTTPS communication between the devices and the HP CR server.

- With HP Pro devices, use an OPS Server certificate.

You must create the certificate before installing the HP CR Embedded Device Client. This configuration is necessary to allow administrators to export the file and install it on the device to enable HTTPS communication.

**NOTE:** HTTP and HTTPS cannot coexist and configuration for the device communication must be either HTTP or HTTPS for all devices.

- The administrator will need to create and export the certificate for the Web server as a file named WebServer.cer and copy it to the Certificate folder created during the HP CR Embedded Device Client install.
- During the registration process for the OXPd application, the webserver.cer will be installed into the device.
NOTE: No error will be generated if the file does not exist. It will not be possible to configure the device for HTTPS until that file has been installed onto the device.

For information on how to create a self-signed certificate using makecert.exe, refer to Creating the certificate (13).

For information on using the OPS Server certificate see HTTPS support using the OPS-created certificate (59).

1-3-2 Device group planning

The HP CR Server Administrator Devices node gives the administrator the ability to manage devices and create groups of devices with customized buttons. Refer to Creating a group of devices (21).

1-4 Online help and related documentation

- HP Capture and Route (HP CR) Installation Guide
- HP CR Server Administrator help (procedures for installing, uninstalling, and troubleshooting are included)
- HP CR Embedded Device Client Quick Start Guide
- HP Capture and Route (HP CR) for HP OXPd v1.4 Device Client Quick Start Guide
- HP Capture and Route (HP CR) User Guide
2 Setting up a CA Certificate and SSL

You must meet the following requirements when setting up a CA certificate:

- Web server that meets the requirements for HP CR Intelligent Device Client.
- Windows user account that belongs to the Administrators group.

The remainder of this section provides instructions for:

- Downloading the MakeCert executable (13)
- Creating the certificate (13)
- Installing the certificate to Internet Information Services (IIS) (14)
- Adding the certificate to the Client certificate directory (14)
- Creating an SSL binding (15)
- Requiring SSL for the virtual web sites (15)
- Verifying the SSL binding (15)
- Enabling directory browsing in IIS (15)
- Verifying HTTPS browsing (16)
- Editing the OmISAPIU.xml file (16)
- Editing the Bootstrap.xml file (16)

You should complete each procedure in the order in which they are presented.

2-1 Downloading the MakeCert executable

Copy `makecert.exe` to your local computer. The MakeCert executable is available as part of the Windows SDK. For instructions on how to download the Windows SDK and the MakeCert executable, see the Microsoft documentation.

When the download is complete, copy the executable to a shared network folder from where you can access it.

2-2 Creating the certificate

1. Open a command prompt and navigate to the directory where you saved the MakeCert executable (`makecert.exe`) on your local computer (typically on the C drive).

2. Run the following command (as Administrator):

   ```
   makecert.exe -r -pe -n "CN=fully_qualified_domain_name_of_iis_server" -b 01/01/2006 -e 01/01/2015 -ss my -sr localMachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12 "fully_qualified_domain_name_of_iis_server.cer"
   ```

   `fully_qualified_domain_name_of_iis_server` should be in this format: `servername.domain.com`
NOTE: You cannot copy and paste the command text above due to formatting issues. This text is available to copy in the HP CR Embedded Device Client section of the On-line help for the administrator. If you key in the command text, note that there is a space at the end of the first three lines shown above.

When the command is run properly, the system will display a message indicating that it succeeded.

2-3 Installing the certificate to Internet Information Services (IIS)

You must now install the certificate from the root of C.

1. Select and right-click the certificate.

NOTE: In Windows 2012 environments, the Certificate Import Wizard prompts you to select either Current User or Local Machine. Select Local Machine.

3. Select NEXT.
4. Select Place all certificates in the following store and select BROWSE.
5. Select Trusted Root Certification Authorities and select OK.
6. You will be prompted with a security warning:
   
   You are about to install a certificate from a certification authority (CA) claiming to represent...
   Do you want to install this certificate?

   Select YES. A message indicating the import was successful should display.

2-4 Adding the certificate to the Client certificate directory

You will need to export the certificate from the Web server as a file named WebServer.cer and copy it to the Certificate folder created during the HP CR Embedded Device Client installation.

1. Navigate to the IIS\LOCAL_MACHINE directory and locate Server Certificates.
2. Locate the newly created certificate. Double-click to open the certificate Properties page.
3. Click on the Details tab.
5. Click Next.
6. In the Export Private Key dialog, select No, do not export the private key.
7. Click Next.
8. In the Export File Format dialog, select DER encoded binary X.509 (.CER).
9. Click Next.
10. In the File to Export dialog, select Browse. The Save As dialog opens.
11. Browse to the directory:

   C:\Program Files (x86)\HP\DeviceClient\Certificate
12. In the **File Name** field, enter `WebServer.cer` with DER Encoded Binary X.509 (*.cer) as the **Save Type**.
13. Click **Save** and then **Next**. The **Completing the Certificate Export** wizard opens.
14. Click **Finish**.
15. When a message appears stating that the export was successful, click **OK**.

### 2-5 Creating an SSL binding

1. Open the IIS Manager.
2. Click on the **Default Web Site** and locate **Bindings** under **Edit Site** (top right corner of the window).
3. Click on **Bindings**. The **Site Bindings** dialog opens.
4. Click on **HTTPS type** and select **Edit**. The **Edit Site Bindings** dialog opens.
5. In the **SSL certificate** drop-down, choose the certificate that was created earlier and click **OK**.
6. Click **Close** to close the dialog.

### 2-6 Requiring SSL for the virtual web sites

1. Open the IIS Manager.
2. Expand **Local Machine > Default Web Site** and select **Device Client**.
3. Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.
4. Expand **Local machine > Default Web Site** and select **WebAPI**.
5. Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.

### 2-7 Verifying the SSL binding

1. Open the IIS Manager.
2. Expand **Local Machine > Default Web Site** and select **WebAPI**.
3. Click on **Browse *:443 (HTTPS)** under **Manage Application/Browse Application** (located at the top right corner of the IIS dialog).
   
   You will see this message: **There is a problem with this web site’s security certificate.**

   **NOTE:** This message is expected and safe to ignore.

4. Click the **Continue to this website (not recommended)** option.
5. Verify that the **IIS 7** dialog opens.

### 2-8 Enabling directory browsing in IIS

1. Open the IIS Manager.
2. Expand **Local Machine > Default Web Site** and select **DeviceClient**.
3. Double-click on **Directory browsing**.
4. In the right **Actions** field, select **ENABLE**.
5. Expand **Local Machine > Default Web Site** and select **WebAPI**.
6. Double-click on **Directory browsing**.
7. In the right **Actions** field, select **ENABLE**.

### 2-9 Verifying HTTPS browsing

1. Open the IIS Manager.
2. Expand the **Default Web Site**.
3. Expand **OXP**.
4. Select the **Configuration** folder.
5. In the actions pane, select **Browse*:443(https)**.
6. Select **Continue to this website (not recommended)**.
7. Verify that the local page is displayed.
   - For HP OXPd:
     ```
     .../DeviceClient/Configuration/
     ```
8. In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
9. In the actions pane, select **Browse*:443(https)**.
10. Select **Continue to this website (not recommended)**.
11. Verify that the localhost page is displayed:
    ```
    .../WebAPI/
    ```
12. Select **Continue to this website (not recommended)**.

### 2-10 Editing the OmISAPIU.xml file

1. Navigate to the following path.
   ```
   C:\Program Files (x86)\HP\HPCR\WebAPI\WebAPI\Scripts
   ```
2. In OmISAPIU.xml, find the FileTransfer node. Replace the IP address with the fully qualified domain name. Also, change **http** to **https**.
   ```xml
   <FileTransfer>https://fully_qualified_domain_name/WebAPI/FileTransfer/</FileTransfer>
   ```

   **NOTE:** XML files can be edited using Microsoft Notepad.
3. Save the file.

### 2-11 Editing the Bootstrap.xml file

1. Navigate to the following path.
   - For HP OXPd:
     ```
     C:\Program Files (x86)\HP\DeviceClient\Configuration
     ```
2. In bootstrap.xml, change **http** to **https**.
<Server>https://fully_qualified_domain_name/webapi/scripts/omisapiu.dll</Server>

3. Next, replace the server name with the fully-qualified domain name.
4. Save the file.
5. Reset IIS.
3  HP CR Embedded Device Client installation

This section describes:

- Installing the HP CR Embedded Device Client (19)
- Installing the HP CR Embedded Device Client on a remote system (20)

See also Section 4: Creating Device Groups on the HP CR Server Administrator (21), Section 10: Testing (83), and the HP CR administrator on-line help (for additional information including optional configurations, testing, and troubleshooting).

3-1  Installing the HP CR Embedded Device Client

1. Log on to the system running the HP CR server using an account that belongs to the local Administrators group.

2. Navigate to the folder:
   
   C:\Program Files (x86)\HP\HPCR\Clients\DeviceClient and run setup.exe.

   The InstallShield wizard launches with the Welcome message.

3. Click Next. The Destination Folder page opens.

4. Keep the default location and click Next. The HP Capture and Route Embedded Device Client Configuration page opens.

5. In the HP Capture and Route Intelligent Device Client Server name text box, enter the server name or IP Address of the HP CR Intelligent Device Client.
6. Click **Next** and the **HP Capture and Route Server Credentials** page appears.

7. Enter the **Service Account** used by the Server and the corresponding **Password**.

8. Click **Next** and you are ready to install the program.

9. Click **Install** to begin installation. The setup installs the HP CR Embedded Device Client. The InstallShield Wizard shows a message indicating when the installation is complete.

10. Click **Finish**.

11. Continue to **Section 3: Installing the HP CR Embedded Device Client** (19).

---

### 3-2 Installing the HP CR Embedded Device Client on a remote system

Follow these steps to remotely install the HP CR Embedded Device Client onto a separate server.

**NOTE:** The system to which you are installing must be running Windows 2008 R2 x64 or 2012 64-bit and have Embedded HP CR for Intelligent Devices (HP CR ISAPI Web Server Extension) installed.

1. First, you need to change the DCOM login on the server of interest to use the Computer Account instead of the Administrator’s/Service account and log on to it using that account.

2. Follow steps 2 through 6 in **Installing the HP CR Embedded Device Client** (19) and return here.

3. On the **HP Capture and Route Server Credentials** page, enter the **Service Account** (Computer Account?) used by the Server and the corresponding **Password**.

4. Click **Next** and you are ready to install the program.

5. Click **Install** to begin installation. The setup installs the HP CR Embedded Device Client on your remote server. The InstallShield Wizard shows a message indicating when the installation is complete.

6. Click **Finish**.
Creating Device Groups on the HP CR Server Administrator

This section describes the processes for

- Creating a group of devices (21)
- Specifying buttons for devices (27)

Refer to Installing buttons on a new device for steps to install the buttons onto the devices.

See also Section 10: Testing (83) and the HP CR administrator on-line help (for additional information including optional configurations, testing, and troubleshooting).

4-1 Creating a group of devices

Create a new Group for each group of devices. While each group may have the same configuration, you can configure a group to have a configuration that is completely different from another group. For example, you might create a group named “Marketing” and configure it to use only the Routing Sheets and Fax features. You might create an additional group named “Sales” and configure it for PIN authentication and ability to use only the Routing Sheet, Personal Distributions, and Scan to Me features.

The following procedure explains how to create and configure a device group.

1. Click Start > All Programs > HP Capture and Route > HP Capture & Route Server Administrator.
2. In the console tree, expand the HP CR server.
3. Go to the Devices node.
4. Right-click and select New > HP OXPd group.
Creating Device Groups on the HP CR Server Administrator

The New Group page opens.

5. In the **Name** text box, enter a name for the device.
6. Optionally, in the **Description** text box, enter a device description.
7. Click the **Settings** tab. Change settings only if the IIS/Web server is remote or if you are configuring HTTPS.

- If you are configuring for HTTPS, change the IP Address to the fully-qualified domain name and the URL path from HTTP to HTTPS. For example:
Application URL: https://FQDN/DeviceClient/
Web API: https://FQDN/WebAPI/Scripts/omisapiu.dll

- If you are configuring a device group of HP Pro devices, confirm the IP address of the OPS Server in the **OPS Server** field.
- For remote systems – If you installed the HP CR Embedded Device Client on a remote system, you must manually enter the IP address of that system in the URL field.
- If you are using a local OPS server and an OPS-created certificate for HTTPS environments, change the Application and WebAPI’s URLs to https://IP address or FQDN name to match the OPS server. Then continue on to the following sub-sections Creating an SSL binding (15) through to Editing the OmiSAPIU.xml file (16).

8. Click the **Authentication** tab to specify the type of user authentication required for the group of devices.

9. From the **Type** drop-down, select one of the four authentication options: **Device**, **Email**, **Login**, or **PIN**.

After you select **Device**, **Email**, **Login**, or **PIN** as the authentication type, you can define the properties for the **Domain**, **User**, and **Password** in the **Fields** section.

The following pages describe:

- **Defining Domain Properties** (24)
- **Defining User Properties** (25)
- **Defining Password Properties** (26)

**NOTE:** HP Pro Devices do not support the Device authentication method on their own. They require a stacked solution with another installed authentication service. An example would be HP AC authentication set in the Pro device when Device authentication is set in HP CR.
Defining Domain Properties

To define domain properties, double-click **Domain** in the **Fields** section. The **Domain Field Properties** dialog is displayed:

![Domain Field Properties Dialog](image)

When you define a domain, you can specify a **Default value** (domain) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for Domain** - The device user will need to enter a domain for authentication during login at the device.

- **User must select a value for Domain from one of the following** - If there are multiple domains in the environment, use this option to create a list of domains from which the user can select.

- **User may not enter a value for Domain** - This option prohibits the user from entering a domain value. When you select this option, you can indicate that the device will **Display the default value to the user (read-only)**. The user will see the **Default value**, but cannot change it.

Click **OK** to return to the **Device Group Properties** page.

**NOTE:** Domain definition is optional for all authentication types.
Defining User Properties
To define user properties, double-click User in the Fields section. The User Field Properties dialog is displayed:

When you define a user, you can specify a Default value (user) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for User** - The device user will need to enter a user for authentication during login at the device.
- **User must select a value for User from one of the following** - If there are multiple users in the environment, use this option to create a list from which the user can select.
- **User may not enter a value for User** - Do not select this option if you are using Email, Login, or PIN authentication. This option prohibits the user from entering a user value.

When you select this option, you can indicate that the device will Display the default value to the user (read-only). The user will see the Default value, but cannot change it.

Click **OK** to return to the Device Group Properties page.

**NOTE:** User definition is required for Login authentication and optional for all other authentication types.
Defining Password Properties

To define password properties, double-click **User** in the **Fields** section. The **Password Field Properties** dialog appears:

When you define a password, you can specify a **Default value** (password) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for Password** - The device user will need to enter a password for authentication during login at the device.

- **User must select a value for Password from one of the following** - If there are multiple passwords available in the environment, use this option to create a list from which the user can select.

- **User may not enter a value for Password** - This option prohibits the user from entering a password. Use this option only when PIN authentication is used without a password. Do not select this option if you are using Email, Login, or PIN (with password) authentication.

When you select this option, you can indicate that the device will **Display the default value to the user (read-only)**. The user will see the **Default value**, but cannot change it.

**NOTE:** Password definition is required for **Login** authentication and optional for all other authentication types.
10. After you define **Domain**, **User**, and/or **Password** properties, click **OK** to return to the **Device Group Properties** page. For example

11. At the **LDAP Lookup Settings** section, in the **Username** text box, enter the name of a Windows user who has permissions to query the active directory.

12. In the **Password** text box, enter the Administrator password.

13. Select the **Confirm authentication** option if you want to display a prompt on the device to verify the user’s information when authenticating.

Continue with **Specifying buttons for devices** (27).

4-2 Specifying buttons for devices

Having created one or more device groups and set up authentication, you can add and configure specific buttons for your devices.

- **Adding new buttons** (28)
- **Configuring button properties** (29)
4-2-1 Adding new buttons

1. In New Group Properties, click the Buttons tab to add and/or remove buttons that appear on the device.

   ![Add Button Dialog]

   **NOTE:** It is best to add or remove buttons before installing to the device. Otherwise, if you add or remove buttons, or if button text is modified, it will be necessary to uninstall and run the installation again.

2. To add a button, click Add. The Add Button dialog is displayed.

   ![Add Button Dialog]

   **NOTE:** If the Add button is not active, click on Device Home Screen.

3. From the Type drop-down, select a button type.

4. Enter a Name for the button. Then, click OK.

   Continue with Configuring button properties.
4-2-2 Configuring button properties

You need to configure and define properties for each button that you add. **General Properties** are required for all buttons.

For some buttons, you need to define button-specific properties or make configuration changes. For more details, see:

- Personal and Public Distributions (31)
- Scan to Distribution (32)
- Fax (34)
- Routing Sheet, Scan to Destination, Scan to Distribution, Scan to Me, and Scan to My Files (36)
- Fax Release (38)
- Job Queue (40)
- Device Information (41)

If you are not adding one of the button types listed above, after defining **General** properties, continue with

- Defining Prompts (43)
- Defining Device Settings (44)
- Defining Advanced Device Settings (45)

4-2-2-1 General Properties

1. From the **Buttons** tab of **Group** properties, highlight a button on the list and click **Properties**.

You can edit the default **Name**, **Display Text**, and **Description** for any button.

**NOTE:** Do not change **Image** from the default value.
NOTE: For buttons using Require Authentication, select Capture user password for the credential pass-through feature and Always prompt user for password for use with HPAC authentication.

2. Specify a location for the button. Select either of these options:

- **Auto assign based on configured ordering** - The button is positioned based on a predefined order.
- **Use specific ordering priority** - You can enter a value to indicate the button placement. Position 1 is in the upper left location and position 2 is in the upper right location, in a Z-order layout. The pattern is as follows:
  
  1 2
  3 4
  5 6
  etc.

3. Select additional options for the button:

- **Enable this button for use on the device** - Self-explanatory.
- **Enable job build** - This option enables the Scan More feature.
- **Enable One-Touch scanning** - This allows the user to select a button with the documents already loaded in the Automatic Document Feeder for one-touch scanning. Typically, this is used with a Distribution that has all scan settings saved.
- **Enable scan preview by default (only on supported devices)** - This allows the user to visually preview the documents being scanned from the device. This only applies to Futuresmart devices.
- **Require authentication** - If you select this option, you can then indicate that the button should capture the user’s password. Note that although the Routing Sheet feature typically does not require authentication, you can configure this requirement here.
4-2-2-2 Personal and Public Distributions

1. If you are adding a Personal Distributions or Public Distributions button, click the Options tab.

2. Enter a Public Email address (if applicable) and set the Enumeration Limit for distributions (the maximum number of distributions allowable).
4-2-2-3 Scan to Distribution

1. If you are adding a **Scan to Distribution** button, click the **Options** tab to route using an existing (already created) distribution.
2. Click **Select** and the **Select Embedded Directive** dialog appears.

3. Click the **Find** button to display all distributions.

4. Select a distribution and then click the **Select** button to choose the distribution that will be used when this button is selected from the device.
4-2-2-4 Fax

1. If you are adding a Fax button, click the Options tab to configure fax cover pages.

2. Select options to allow a cover page to be specified and include the cover page by default. In addition, you can indicate the information (subject, etc.) that will appear on the cover page.

3. Next, click the Confirmations tab to:
   - Allow authenticated and non-authenticated users to select the button.
   - Define the type of fax confirmations (select a field and click Properties).
   - Add recipients for confirmations (click the Add button).
For example, you can edit the fields for the Originator for faxed faxes:
4-2-2-5 Routing Sheet, Scan to Destination, Scan to Distribution, Scan to Me, and Scan to My Files

1. If you are adding a Routing Sheet, Scan to Destination, Scan to Distribution, Scan to Me, or Scan to My Files button, click the Job Properties tab.

You can add, remove, or change a property. This example shows the property of a Destination.

You can change an Originator, Destination, or Recipient. You also can add a Transformation (replacing a data value (a message property, recipient property, Embedded Directive property, or template variable) with another value.).
Note that the **Scan to Destination** button allows for message routing based on routing rules.

- The default setting is to send to a destination of scantodestination, which can have an outbound rule associated with that destination to route to any location to which the HP CR server can route messages. You can edit this destination value.

- You can also add Transformations here.
4-2-2-6 Fax Release

If you are adding a Fax Release button, once you define its General Properties, you need to configure User Group access settings for those who will be using the Fax Release option. You also need to set up a Fax Release Calendar schedule, Routing information and/or other details for incoming faxes.

1. In the Server Administrator, go to Configuration > Groups node. Double-click the group of interest to open its Group properties.

2. Select Web in the Clients section. Check the Enable members of this group to use the following web view check box.

3. From the Web View drop-down menu, select the Web View for which you will enable Web Client Administration access. Click OK.


5. On the Folders tab, double-click Administration and select the Display this folder check box. Click OK and OK again.
6. Open the HP CR End User Interface and select Administration > Calendars. Click New to create a new Fax Release Scheduling Calendar.

7. In the Calendar, define the time periods within which you want to allow authorized users to manually release faxes. Click OK.

8. Also under Administration, select Routing and click New.

9. In New Routing Destination, enter the Fax number for which you want to set up receiving details.

10. On this screen you can
    - Associate a Device Serial Number or Business Unit.
    - Enable Manual Hold for all faxes from this number.
    - Enable Fax Release and assign a specific Calendar (such as the one created in step 7) to guide its use.
    - Assign a Manual Override Pin.
• Assign a **Destination** for these faxes, with options such as a specific device, a regulated printer, or another destination, such as email or a Folder.

• Identify whether the fax should be printed on a specific **Media Size** or have a **Document Stamp** applied.

• Assign a **Delivery Format** and/or **Document Name** for all faxes from this number.

11. Click **OK**.

### 4-2-2-7 Job Queue

If you are adding a **Job Queue** button, once you define its **General Properties**, you need to enable the Destination Translation Table (DTT) in the End User Interface for Administrative users of the **Job Queue** button. After that, you need to add a device of interest as a destination in the DTT.

To enable the DTT in the End User Interface for Administrative users:

1. In the Server Administrator, go to **Configuration > Web Client Views** node. Double-click **View.admin.xml** to open **Web Client View Properties**.

2. In the **Folders** tab, select **Administration > Routing** and click the **Properties** button.

3. In **Folder Properties**, verify that **Display this folder** is selected.

4. Click **OK** and click **OK** again.

5. In the Server Administrator, go to **Configuration > Groups** node. Double-click the group of which the Administrative user is a member to open **Group Properties**.

**NOTE:** If Administrator(s) do not already have a separate group, create one for them before proceeding.

6. Select **Clients > Web** and click the **Properties** button. Verify that **Enable members of this group to use the following web view** is selected.

7. Select **View.admin.xml** from the **Web View** drop-down menu.

8. Click **OK**.

To add a device as a destination in the DTT:

1. Log in to a Windows client system as an Administrative user (same as in Step 5 above) and open Internet Explorer.

2. In the address bar, enter the URL for the End User Interface. The default value for this is `http://<ServerName>/WebClient`.

3. In the End User Interface, select **Administration** on the left. The **Routing** screen is the default display. Click the **New** button.

4. Enter the following information on the **New Routing Destination** page:
   a. **Fax Number**: Enter the fully normalized fax number. For example: +10005551234
   b. **Device Serial Number**: Enter the serial number for the HP device.
   c. For the **Manual Hold** option, check the **Hold all jobs** option if all jobs to this device number are to be held indefinitely.
   d. If you selected the **Manual Hold** option, go to the **Manual Override Pin** text box and enter the PIN value to be used for enabling or disabling Manual Hold.
   e. **Fax Release Calendar**:
      - Check the **Enabled** option.
      - Select the **Calendar** from the drop-down menu.
Creating Device Groups on the HP CR Server Administrator

- Select the **Time Zone** from the drop-down menu.

**NOTE:** To be an option, the **Fax Release Calendar** must be created first.

For more information about the **Administration** features of the End User Interface, see the ‘Customizing the HP CR End User Interface’ section of the **HP CR Server Administrator Help**.

**f** **Destination:** Choose **Print on Device Printer**, **Route via RightFax**, or the **Email/UNC** option:

- For the **Print on Device Printer** option, provide the device IP Address or the UNC path to the device.
  - If using a Regulated Printer, select the **Regulated Destination** check box and enter the IP Address or the UNC path to the regulated printer.
  - You can select the **Print on specific Media** check box and identify from the drop-down menu the paper size on which incoming faxes will be printed.
  - You can also select the **Apply Document Stamp** check box and choose the stamp type of interest from the drop-down menu.

- For the **Route via RightFax** option, select **HP CR FSP Connector for RightFax** from the first drop-down menu and then select the server address of the RightFax Server from the second drop-down menu.

- For the **Email/UNC** option, select either **E-mail** or **UNC** and enter the email address or UNC path in the **Destination** text box.
  - You can define a specific document format from the **Delivery Format** drop-down menu.
  - You can also specify a document name in the **Delivered Document Name** text box.

5. Click **OK**.

### 4-2-2-8 Device Information

If you are adding a **Device Information** button, once you define its **General Properties**, you need to enable the Destination Translation Table (DTT) in the End User Interface for Administrative users of the **Device Information** button. After that, you need to add a device of interest as a destination in the DTT.

To enable the DTT in the End User Interface for Administrative users:

1. In the Server Administrator, go to **Configuration > Web Client Views** node. Double-click **View.admin.xml** to open **Web Client View Properties**.
2. In the **Folders** tab, select **Administration > Routing** and click the **Properties** button.
3. In **Folder Properties**, verify that **Display this folder** is selected.
4. Click **OK** and click **OK** again.
5. In the Server Administrator, go to **Configuration > Groups** node. Double-click the group of which the Administrative user is a member to open **Group Properties**.

**NOTE:** If Administrator(s) do not already have a separate group, create one for them before proceeding.

6. Select **Clients > Web** and click the **Properties** button. Verify that **Enable members of this group to use the following web view** is selected.
7. Select **View.admin.xml** from the **Web View** drop-down menu.
8. Click **OK**.
To add a device as a destination in the DTT:

1. Log in to a Windows client system as an Administrative user (same as in Step 5 above) and open Internet Explorer.

2. In the address bar, enter the URL for the End User Interface. The default value for this is http://<ServerName>/WebClient

3. In the End User Interface, select **Administration** on the left. The **Routing** screen is the default display. Click the **New** button.

4. Enter the following information on the **New Routing Destination** page:
   
a. **Fax Number**: Enter the fully normalized fax number. For example: +10005551234  
b. **Device Serial Number**: Enter the serial number for the HP device.  
c. For the **Manual Hold** option, check the **Hold all jobs** option if all jobs to this device number are to be held indefinitely.  
d. If you selected the **Manual Hold** option, go to the **Manual Override Pin** text box and enter the PIN value to be used for enabling or disabling Manual Hold.  
e. **Fax Release Calendar**:  
   - Check the **Enabled** option.  
   - Select the **Calendar** from the drop-down menu.  
   - Select the **Time Zone** from the drop-down menu.  

   **NOTE**: To be an option, the **Fax Release Calendar** must be created first.

   For more information about the **Administration** features of the End User Interface, see the ‘Customizing the HP CR End User Interface’ section of the **HP CR Server Administrator Help**.

   f. **Destination**: Choose **Print on Device Printer**, **Route via RightFax**, or the **Email/UNC** option:
      
      - For the **Print on Device Printer** option, provide the device IP Address or the UNC path to the device.  
        - If using a Regulated Printer, select the **Regulated Destination** check box and enter the IP Address or the UNC path to the regulated printer.  
        - You can select the **Print on specific Media** check box and identify from the drop-down menu the paper size on which incoming faxes will be printed.  
        - You can also select the **Apply Document Stamp** check box and choose the stamp type of interest from the drop-down menu.  
      
      - For the **Route via RightFax** option, select **HP CR FSP Connector for RightFax** from the first drop-down menu and then select the server address of the RightFax Server from the second drop-down menu.  
      
      - For the **Email/UNC** option, select either **E-mail** or **UNC** and enter the email address or UNC path in the **Destination** text box.  
        - You can define a specific document format from the **Delivery Format** drop-down menu.  
        - You can also specify a document name in the **Delivered Document Name** text box.  

5. Click **OK**.
6. Click the Prompts tab. Click Add to select a prompt configured on the HP CR server. The Select Property Dictionary Field is displayed.

Select a prompt and click OK.
4-2-2-10 Defining Device Settings

7. Click the **Device Setting** tab to configure native device scan settings. This is used for configuring a fleet of monochrome or color machines to use the same scanning settings. For example, the Fax button should only use Monochrome scan settings for better output quality.

![Device Settings Configuration](image)
Select a setting and click **Properties** to change the setting value. For example:

![Device Properties](image)

**NOTE:** The HP Officejet Pro 276dw does not support 600 x 600 scanning with the HP CR Embedded Device Client.

8. Click **OK** to return to the **Device Group Properties**.

**NOTE:** All features/settings within each button can be configured after the button has been installed to a device and are updated instantaneously after selecting **OK**. Uninstallation and re-installation are required only if a button is added or removed, or if the button text is modified.

**4-2-2-11 Defining Advanced Device Settings**

9. Click the **Advanced** tab to modify settings that control the device’s native settings for connectivity timeouts and job refresh settings.
10. Click **OK** to complete the **Device Group Properties**.

11. Once a button configuration is complete, you can install devices using the configured Device Group settings, and the xml files can be exported for importing into HP's WebJet Admin server for button deployment.

   Go to the **Devices** node and right-click on the group name. Then, select the **Export to Web Jet Admin** option. See Installing **HP CR Embedded Device Client buttons** (72).
5 Installing buttons on a new device

Having created on the server one or more device groups and associated buttons, you can continue with the following steps:

- Adding a new device and installing buttons (47)
- Configuring device authentication (49)
- Configuring the server (51)

5-1 Adding a new device and installing buttons

1. In the console tree, expand the HP CR server and go to the Devices node.
2. Select the group to which you want to add a device. Then, right-click and select New > Device. The Properties for device page opens.

3. In the Name text box, enter a name for the device.
4. Optionally, in the Description text box, enter a device description.
5. In the Network Address text box, enter the HP device IP address.
6. Click the **Connection** tab. The following example is for HP OXPd v1.6 or OXPd 1.7 devices:

   ![Connection Tab Example](image)

   When installing to an HP OXPd v1.4 device using either HTTP or HTTPS, you must enter the device Administrator name in the **Username** text box and select the **Use SSL for secure communication** option.

   ![Connection Tab Example](image)

7. In the **Password** text box, enter the Administrator password.

8. If you are using HP OXPd v1.6 or OXPd 1.7, configure the **SNMP Community Strings** section (this section will not appear for HP OXPd v1.4).
Installing buttons on a new device

- In the **Public** text box, enter the v1.6 device public community string.
- In the **Private** text box, enter the v1.6 device private community string.
  The default value is public in both the **Public** and **Private** fields.

9. Click **OK** to add the device.
10. Test by selecting the newly added device. Right-click on the device name and select **Query** from the drop-down options. Verify that the device is successfully queried from the server.
11. After a successful query, right-click and select **Install** to install buttons on your device.
12. Verify that the buttons appear on the device.

5-2 Configuring device authentication

When you select **Device Authentication** from the Device Group properties, you need to complete the following configuration at the device in order to properly identify the logged-in user.

**NOTE:** HP Pro devices do not support LDAP authentication.

5-2-1 Configuring LDAP authentication

When you choose LDAP Authentication, the user is prompted to enter an email username and password. The HP Authentication Manager uses the login credentials to initiate a lookup. The lookup validates the user and returns the user’s email address. Then the HP CR Embedded Device Client uses the email address to request information from the HP CR server, such as a list of the user’s Personal Distributions. When the scan is submitted to the HP CR server as a message, the email address is used to set the property prOriginator.

Both the email username and password are required to identify the device user, and the credentials are validated via LDAP authentication. This method provides increased security.

The following figure is an example of an LDAP Authentication configuration for Active Directory. (For information on configuring LDAP Authentication, consult HP documentation.)
Figure 5-1 Example of an LDAP authentication configuration for Active Directory (2 screens)
LDAP Authentication binds to the LDAP server with the device user’s common name (CN). The search is conducted within the root ou=engineering, cn=users, dc=hp, dc=com using the device user’s common name (CN). The return value is the user’s email address (mail) and name (displayName).

5-2-2 Configuring HP device authentication

1. Open a Web browser and enter the device IP address.
2. Log in to the Embedded Web Server. All options become available.
3. Go the Settings tab and click Authentication Manager.
4. Locate the following HP CR functions:
   - Scan to My Files
   - Personal Distributions
   - Scan to Me

   The list shows the options that are installed with HP CR Embedded Device Client, so it can contain all, some, or none of these functions.
5. For each of the features listed above, click on the drop-down menu.

6. Select LDAP as the authentication method for each scanning feature that requires user login.

7. Click Apply.

5-3 Configuring the server

When a message arrives on the HP CR server, the Dispatch component applies rules to the message. The rules determine how the server processes the message. Every message on the server must match a rule associated with an action in order to be processed and distributed to its final destination. The additional configuration in this section ensures that rules exist for HP CR scanning features.

Several HP CR scanning features require special rules on the HP CR server. Most of these rules are created by default when you install HP CR. You can, if needed, create rules based on the HP CR scanning features available on devices in your environment. For more information on rules and how to create them, refer to the HP CR administrator on-line help.

When rules have been created for all HP CR scanning features available on devices in your environment, the HP CR server is fully configured for the HP CR Embedded Device Client. Now you are ready to test the HP CR scanning features. Continue with the information in Section 10: Testing (83).
Installing buttons on a new device
This section describes the installation and configuration process for HP Pro devices. HP Pro devices require an OPS server for registration prior to installing feature buttons on the devices. The OPS server creates a certificate used for a secure registration of each Pro device. You can also use this certificate in your IIS server for HTTPS support.

**NOTE:** The CA Certificate steps, described in Setting up a CA Certificate and SSL (13), are not supported for HP Pro devices.

The OPS Server installation process includes the following steps:

1. **Installing the OPS Server** (53)
2. **Exporting the OPS server certificate to the Client certificate directory** (58)
3. **Importing the OPS certificate into the device EWS** (58)
4. **OPS registration** (59)
5. **HTTPS support using the OPS-created certificate** (59)

**NOTE:** Scanning in landscape orientation is currently unavailable for HP Pro Devices.

### 6-1 Installing the OPS Server

1. On the server, navigate to `C:\Program Files (x86)\HP\HPCR\Tools`.
2. Right-click and select Run as Administrator.
3. Run `setup.exe` for OPS.
4. The OPS InstallShield wizard appears and requests that you install the following two items:

   - GnuWin32_OpenSSL-0.9.8h-1
   - setup-couchdb-1.2.0_otp_R15B
5. Click **Install**.

6. After installing the items in Step 3, the following message may appear:

   To complete the installation of Apache CouchDB, setup must restart your computer. Would you like to restart now?

   If this message appears, click **Yes** to restart. The OPS InstallShield wizard reappears upon restarting the system.
Otherwise, the OPS InstallShield wizard **Welcome** screen immediately appears.

7. Click **Next**. The **License Agreement** screen appears.

8. Select **I accept the terms in the license agreement** and click **Next**. The **Destination Folder** screen appears.
9. Click **Next**. The **OPS Instance Details** screen appears.

![OPS Instance Details](image1)

10. In the **Hostname** field enter either the IP or FQDN of the server on which OPS is installed. This value is the OPS server name. Make note of this value, as you will need to reference it later during device registration and HTTPS configuration.

11. Enter the **Passwords** in both the **OPS Details** and **DB Details** sections. Also make note of these for later use.

12. Click **Next**. The **Ready to Install the Program** screen appears.

![Ready to Install the Program](image2)

13. Click **Install**.
14. The **OPS InstallShield Wizard Completed** screen appears.

![OPS InstallShield Wizard Completed](image)

Select both the **Launch OPS** and **Show the readme file** check boxes (**Show the readme file** is optional) and then click **Finish**.

15. A pop-up message appears to inform you that the OPS server is listening at the IP address and port listed in step 9.

![OPS server listening](image)

**NOTE:** Make a note of the address that appears in the OPS server listening url. You will need this when registering the OPS server.
Click OK. OPS now appears as a Windows service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Status</th>
<th>Start Type</th>
<th>Log On As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Source Engine</td>
<td>Series inst...</td>
<td>Manual</td>
<td>Local System</td>
<td></td>
</tr>
<tr>
<td>Office Software Pr...</td>
<td>Office Soft...</td>
<td>Manual</td>
<td>Network S...</td>
<td></td>
</tr>
<tr>
<td>Ondemand Address 64...</td>
<td>Manages t...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Component ...</td>
<td>Manages ...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Connector ...</td>
<td>Manages ...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Device Man...</td>
<td>This service...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Message Ser...</td>
<td>Manages ...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Mobile Push...</td>
<td>This service...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Modem Ser...</td>
<td>Manages ...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Interface ...</td>
<td>Manages ...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Object Archive</td>
<td>Manages ...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand ObjectArchive</td>
<td>Manages ...</td>
<td>Started</td>
<td>Automatic</td>
<td>TESTDCy...</td>
</tr>
<tr>
<td>Ondemand Print Spooler</td>
<td>Loads Res ...</td>
<td>Started</td>
<td>Automatic</td>
<td>Automatic</td>
</tr>
</tbody>
</table>

Click the service to stop it, and then click the service to start it.

**NOTE:** If your environment requires you to install the OPS kit on a remote server, first navigate from the local server to the remote one and perform the steps there.

### 6-2 Exporting the OPS server certificate to the Client certificate directory

1. Open a Windows console and select File > Add /Remove snap in...
2. Select Certificates and click the Add button. The Certificates snap-in wizard appears.
3. Select the Computer account radio button and click Next, Finish and OK.
   
   The console loads with the new Certificate snap-in.
4. Expand Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates.
5. Right-click the OPS certificate and select All tasks > Export.
7. Choose Base-64 encoded x.509(.CER) and select Next.
8. Name the file and select Browse.
9. Place the certificate in C:\Program Files (x86)\Hewlett-Packard\OPS.

**NOTE:** When using the OPS-created certificate as the certificate in an HTTPS environment for HP Pro, Futuresmart and Oz devices, you must browse to place the certificate in C:\Program Files (x86)\HP\DeviceClient\OPS.

10. Select Next and then click Finish.

### 6-3 Importing the OPS certificate into the device EWS

1. Open and log into the Embedded Web Server (EWS) of the Pro Device.
2. On the Network tab select Advanced settings > Certificates.
4. Browse to the location where the OPS certificate was saved and select Open and then Finish.

6-4 OPS registration

1. At a command prompt enter
   
   C:\Program Files (x86)\Hewlett-Packard\OPS\bin>OPSSetup

2. You will be prompted to choose from a selection of options.
   Select Option 3: Register a device to the OPS server.
3. Enter the IP address for the device. For example, 123.456.78.9.
4. Enter the device username and password you want to use, noted from Installing the OPS Server (53).
5. Enter the OPS server URL you want to register. Use the url that was noted in step 15 above. For example, https://<hostname or IP>:port.
6. Enter the username and password for the OPS server.

**NOTE:** The OPS server URL and username can be obtained from Steps 8 and 9 above in Installing the OPS Server (53).

7. The following message appears:

   OPS Registered successfully
   Your OPS server is now installed.

For more information on creating device groups and installing buttons on the devices, see:

Section 4: Creating Device Groups on the HP CR Server Administrator (21)
Section 5: Installing buttons on a new device (47)

6-5 HTTPS support using the OPS-created certificate

**NOTE:** If you are working with a remote installation and you want HTTPS support for it, you must install the OPS server on the system where the IIS server is installed. To use the HTTPS certificate, the OPS server must be installed on the IIS server.

6-5-1 Creating an SSL binding

1. Open the IIS Manager.
2. Click on the Default Web Site and locate Bindings under Edit Site (top right corner of the window).
3. Click on Bindings. The Site Bindings dialog opens.
4. Click on HTTPS type and select Edit. The Edit Site Bindings dialog opens.
5. In the SSL certificate drop-down, choose the certificate that was created earlier and click OK.
6. Click Close to close the dialog.
6-5-2 Requiring SSL for the virtual web sites
1. Open the IIS Manager.
2. Expand Local Machine > Default Web Site and select Device Client.
3. Open SSL Settings and check Require SLL. Under client certificates, select Ignore.
4. Expand Local machine > Default Web Site and select WebAPI.
5. Open SSL Settings and check Require SLL. Under client certificates, select Ignore.

6-5-3 Enabling directory browsing in IIS
1. Open the IIS Manager.
2. Expand Local Machine > Default Web Site and select DeviceClient.
3. Double-click on Directory browsing.
4. In the right Actions field, select ENABLE.
5. Expand Local Machine > Default Web Site and select WebAPI.
7. In the right Actions field, select ENABLE.

6-5-4 Verifying the SSL binding
1. Open the IIS Manager.
2. Expand Local Machine > Default Web Site and select WebAPI.
3. Click on Browse *:443 (HTTPS) under Manage Application/Browse Application (located at the top right corner of the IIS dialog).
   You will see this message: There is a problem with this web site’s security certificate.

   **NOTE:** This message is expected and safe to ignore.

4. Click the Continue to this website (not recommended) option.
5. Verify that the IIS 7 dialog opens.

6-5-5 Verifying HTTPS browsing
1. Open the IIS Manager.
2. Expand the Default Web Site.
3. Expand OXP.
4. Select the Configuration folder.
5. In the actions pane, select Browse*:443(https).
6. Select Continue to this website (not recommended).
7. Verify that the local page is displayed.
   For HP OXPd:
   .../DeviceClient/Configuration/
8. In the IIS Manager with Default Web Site expanded, expand WebAPI.
9. In the actions pane, select **Browse*:443(https).**
10. Select **Continue to this website (not recommended).**
11. Verify that the localhost page is displayed:

   .../WebAPI/

### 6-5-6 Editing the OmISAPIU.xml file

1. Navigate to the following path.
   
   C:\Program Files (x86)\HP\HPCR\WebAPI\WebAPI\Scripts

2. In OmISAPIU.xml, find the FileTransfer node. Replace the IP address with the OPS Servername or IP. Also, change http to https.
   
   `<FileTransfer>https://OPS Servername or IP/WebAPI/FileTransfer/</FileTransfer>`

   This OPS Servername is based on the value from Step 10 of **Installing the OPS Server**.

   **NOTE:** XML files can be edited using Microsoft Notepad.

3. Save the file.

### 6-5-7 Editing the Bootstrap.xml file

1. Navigate to the following path.
   
   For HP OXPd:
   
   C:\Program Files (x86)\HP\DeviceClient\Configuration

2. In bootstrap.xml, change http to https.
   
   `<Server>https://OPS Servername or IP/webapi/scripts/omisapiu.dll </Server>`

   This OPS Servername is based on the value from Step 10 of **Installing the OPS Server**.

3. Save the file and reset IIS.
7 Configuring HP S900 Series devices

The HP S900 Series devices support all of the features in the Device Client, with some modifications to the standard process. See the sections below for the modified configuration settings.

This section describes the processes for

- Enabling HTTPS for SSL on HP S900 Series devices (63)
- Adding buttons to HP S900 Series devices (63)
- Configuring device authentication (66)

NOTE: Verify that Section 3: HP CR Embedded Device Client installation has been completed and that the Device Client is installed.

7-1 Enabling HTTPS for SSL on HP S900 Series devices

Apply the following steps to the HP S900 Series device after completing the HTTPS configuration outlined in Section 2: Setting up a CA Certificate and SSL.

1. In a browser, open the Embedded Web Server for the HP S900 Series device by entering the IP address of the device and log in.
2. Select Security Settings > SSL settings.
3. In the Setting of SSL section, select Enable for Client Port: HTTPS.
4. Save the configuration.

7-2 Adding buttons to HP S900 Series devices

The HP S900 series devices require information from the HP CR Server device group in order to install the HP CR buttons to the device.

This section describes

- Creating a group with a Nested button (64)
- Launching the Device Group XML information (64)
- Creating the URL string to use for button installation (65)
- Installing the buttons to the device (66)

It is recommended that you use Nested buttons, because

- The HP S900 Series MFP devices have a display limit of 8 buttons in the main window.
- By using nested buttons, one avoids the need to register each individual button and only the top-level button needs to be registered.
7-2-1 Creating a group with a Nested button

1. Launch the HP CR MMC Administrator and select the Devices node.
2. Right-click and select the HP OXPd group.
3. Create a group as described in Section 4: Creating Device Groups on the HP CR Server Administrator.
4. Select the Buttons tab in the Device Group screen.
5. Click Add and select Nested Button from the Type drop-down menu.
6. Add a name for this top level button and click OK.
7. Select the Routing Sheet button and click Move.
8. Select the Nested Button name and click the Move button again.
9. Verify that the Routing Sheet button appears under the new Nested Button.
10. Move the remaining buttons under the Nested button.
11. Click OK.

7-2-2 Launching the Device Group XML information

1. In the HP CR MMC Administrator, acquire an XML Group Dump from the Device Group.
2. Highlight the Devices node, right-click it while holding the CTRL key and select Dump XML. By default, this .xml opens in Internet Explorer.
Configuring HP S900 Series devices

3. The following XML Group dump example shows a Nested button Feature id within the HP S900 Series Device Group:

```xml
<Device>
  <DeviceName>hp</DeviceName>
  <Group>
    <GroupName>hp</GroupName>
  </Group>
  <Feature>
    <FeatureName>Button0</FeatureName>
    <FeatureId>Button0</FeatureId>
    <FeatureDescription>Scan to HP Capture and Route</FeatureDescription>
    <FeatureOptions/>
    <FeatureState/>
    <FeatureContext>
      <FeatureContextName></FeatureContextName>
      <FeatureContextValue></FeatureContextValue>
    </FeatureContext>
    <FeaturePriority>1</FeaturePriority>
    <FeatureIcon>button.png</FeatureIcon>
  </Feature>
</Device>
```

4. Within the <FeatureSets> section of the XML file, locate the section associated with the device group you created at step 3 of Creating a group with a Nested button (64).

Make note of the Feature id value.

7-2-3 Creating the URL string to use for button installation

You need to customize and add the following URL to the Embedded Web Server of the device:

```
```

1. Copy and paste the above link in Notepad.

2. Replace the following fields with their appropriate values:

   - `DeviceClientServerIP` – the IP address of the system where the Device client is installed.
   - `<GroupName>` – the name of the device group as it appears in the HP CR MMC Administrator.
   - `<FeatureID>` – the value in the .xml file of the Feature id property.

   For example, using the sample .xml, the URL would appear as:

   ```
   http://10.0.0.1/DeviceClient/device.aspx?Group=hp&FeatureID=Button0&ClearHistory=1
   ```

   where the `DeviceClientServerIP` is 10.0.0.1, the `<GroupName>` is `hp` and the `<FeatureID>` is `Button0`.

**NOTE:** If there are multiple Device Groups, verify the Group Node before searching for the feature button.

Continue to Installing the buttons to the device (66), where you can apply this URL.
7-2-4 Installing the buttons to the device

1. In a browser, open the Embedded Web Server for the HP S900 Series device by entering the IP address of the device, and log in.
2. From the left-hand menu, select Application Settings/External Application Settings.
3. Select Add(Y).
4. In the Standard Application Registration page, add an Application Name for the feature button.
5. In Address for Application UI, paste the URL that you created in the prior section.

7-3 Configuring device authentication

Device Groups specify the authentication that must be used to identify the users. In a case in which Device authentication is selected, follow these steps for configuring the HP S900 series devices to support device authentication.

1. In a browser, open the Embedded Web Server for the device and log in.
2. Select Network Settings > LDAP settings.
3. Enter the Name, Search root, and LDAP server IP information.
4. Set Server Type to Custom (the Search attribute has a default value of CN.)
5. Optionally, you can set other Custom Attributes, which allow for additional return results.
6. Enter the Domain\Username and Password for LDAP queries.
7. Change the Bind Prefix to CN. This will search based on the user’s Common name and can be changed to any Active Directory Attribute.

**NOTE:** Other login options are available based on Email address or User number.

8. Select Execute to verify LDAP search permissions and then select Submit.
9. From the left menu, select User Control > Default Settings.
10. Select User Authentication > Enable.
11. Select Authentication Method Setting > Authenticate a User by Login name and Password.
12. Select Submit and then Update.
8 Configuring HP FutureSmart, OZ and Pro Devices to use the OPS server certificate for HTTPS environments

This section describes how to configure FutureSmart and OZ devices to use the certificate created during the OPS Server installation for HTTPS support. This is a quick and convenient way to set up HTTPS without the need to use the MakeCert process.

Before continuing, verify that the OPS Server is installed and working as described in Chapter 5: Configuring HP Pro Devices (53)

8-1 Exporting the certificate to the Embedded Device Client directory for FutureSmart and OZ devices

When an environment includes HP Pro devices and FutureSmart or OZ devices, the certificate used for HTTPS communication must be an OPS server certificate, not a MakeCert-generated certificate.

IMPORTANT: As a requirement, the OPS Server must be correctly installed and configured before obtaining the OPS Server certificate.

1. Navigate to C:\Program Files (x86)\Hewlett-Packard\OPS and copy the certificate saved from previous steps.
2. Navigate to and then paste the certificate into C:\Program Files (x86)\HP\DeviceClient\Certificate\OPS.

All FutureSmart and OZ devices will use this certificate for HTTPS communication.
Configuring HP FutureSmart, OZ and Pro Devices to use the OPS server certificate for HTTPS environments
9 Using HP’s Web Jetadmin application to install HP CR Embedded Device Client buttons on HP devices

The information in this section will allow you to administrate and install HP CR Embedded Device Client buttons onto HP devices using the Web Jetadmin application. This section includes:

- Supported devices (69)
- Exporting the XML files (70)
- Manually importing a certificate (71)
- Installing HP CR Embedded Device Client buttons (72)

9-1 Supported devices

The following devices support installation with Web Jetadmin:

<table>
<thead>
<tr>
<th>Device</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color LaserJet CM 4730 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>Digital Sender 9250c</td>
<td>Oz</td>
</tr>
<tr>
<td>LaserJet M3035 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>LaserJet M4345 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>LaserJet M4349 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>LaserJet M5035 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>LaserJet M5039 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>LaserJet M9040 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>LaserJet M9050 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>LaserJet M9059 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>Color LaserJet CM 6030 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>Color LaserJet CM 6040 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>Color LaserJet CM 6049 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>Color LaserJet CM 3530 MFP</td>
<td>Oz</td>
</tr>
<tr>
<td>Color LaserJet CM 4540 MFP</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>ScanJet 7000n</td>
<td>FutureSmart</td>
</tr>
</tbody>
</table>
Using HP’s Web Jetadmin application to install HP CR Embedded Device Client buttons on HP devices

**9-2 Exporting the XML files**

Complete the following procedure for HP CR to configure the HP CR Embedded Device Client with the appropriate settings for your environment.

1. Once the configuration is complete (as described in Section 3: HP CR Embedded Device Client installation and Section 4: Creating Device Groups on the HP CR Server Administrator), right-click the Devices group to which you intend to deploy buttons. Select Export to Web Jet Admin.

2. You can now store the XML files by browsing to a network folder or creating a new folder destination.

Browse:

<table>
<thead>
<tr>
<th>Device</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScanJet 8500</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>LaserJet Flow M525 MXP</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>LaserJet Flow M575 MXP</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>LaserJet M775 MFP</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>LaserJet M4555 MFP</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>HP Color Laserjet Flow MFP M880</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>HP Color Laserjet Flow MFP M830</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>HP Laserjet MFP M725</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>HP X585 MFP group</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>HP M680 MFP group</td>
<td>FutureSmart</td>
</tr>
<tr>
<td>HP M630 MFP group</td>
<td>FutureSmart</td>
</tr>
</tbody>
</table>
Using HP’s Web Jetadmin application to install HP CR Embedded Device Client buttons on HP devices

Make New Folder:

3. Click OK and verify that the correct buttons are represented in XML format.

9-3 Manually importing a certificate

For HTTPS support, you need to import the client certificate into the device Embedded Web Server (EWS) before installation, as follows:

1. Save the certificate to be used for HTTPS communication to a network-accessible location.
2. Open and log into the EWS of the device.
4. Under Certificates, select Choose File > Browse.
5. Browse to the location where you saved the certificate and select Open > Import.
6. Verify that the certificate appears under the Certificates section within the device Embedded Web Server.
9-4 Installing HP CR Embedded Device Client buttons

Once you can discover devices using the Web Jetadmin application, you can install the buttons using the Web Jetadmin application.

**NOTE:** If Omtool AccuRoute buttons exist on the device, HP CR buttons will overwrite them during installation.

1. Right-click the **Group** node and select **New group**.
   
   The **Specify group options** page appears.

2. Enter the name of the new group that you will use to group similar devices for button installation. (Preferably, this is a device group name that will allow the administrator to easily configure similar firmware or button functionality installations such as Jedi, Oz, etc.)
3. Click **Next** and verify that the group name is correct. The **Confirm** page appears, showing the settings for the group.

4. Click **Create Group** and then **Done**.

5. Right-click the newly created group and select **Add devices to group**.

**NOTE:** For more options to use the Web Jetadmin device filters to find or add devices, consult HP’s Web Jetadmin team for a complete Web Jetadmin installation guide.
Using HP’s Web Jetadmin application to install HP CR Embedded Device Client buttons on HP devices

The Select Devices page appears.

6. In the Available devices list (on the left), highlight the device(s) to be added to the group. Then click the > (add) button. The selected device(s) are added to the Devices to add list (on the right).
7. Click **Next**. The **Confirm** page appears.

8. Click the **Add Devices** button. You should see the devices added to your new group in the **Group** page.

9. Highlight the device(s) on which you want to install buttons.
10. Click the **Config** tab and scroll to the **OXPd Device Functions** subset (as shown below). Check the box in the upper left corner of the center screen. The title bar of that area will read: *OXPd Device Functions (Changes Pending - Click ‘Apply’ to continue)*.

11. Click the **Add** button. The **Add OXPd Device Functions** page appears.
12. Click the Edit button. The OXPd Device Function Repository page appears and enables you to import the edited HP OXPd solutions XML files (from Exporting the XML files on 70).

13. Click Import. In the Open page, search for your XML files.
14. Select and highlight the file and then click Open to add the file. (You can import only one file at a time in the Open page.)

15. Verify that the selected feature XML file is reflected in the OXPd Device Function Repository page.

16. Click OK. The Add OXPd Device Functions page appears.

17. You should see the file referring to the feature(s) or button(s) you are about to install onto the device. Click OK to close the Add OXPd Device Functions page and return to the OXPd Device Functions page.

At this point, you can continue to add another feature or button (repeating Steps 11 through 16).
18. After you have added and confirmed all of the features/buttons of interest, click **Apply**. The **Confirm** page appears.
19. Click the **Configure Devices** button. The **In Progress** page appears.

The **Results** page indicates whether the installation was successful or an error was received.

**NOTE:** You can click the **Details** button to show additional notes if an error has occurred.
20. Click Done to return to the main Group page, which defaults to the Device subset node.

21. Scroll down to the OXPd Device Functions subset and you should see the feature buttons that were successfully added to the HP device.

22. Test the buttons on the device panel to verify all functionality.
The following section provides a procedure for testing the Routing Sheet feature and the Device Administrator user interface. This will ensure that your installation is operational. For additional button testing procedures, refer to the HP CR administrator on-line help.

10-1 Testing the Routing Sheet feature

1. Create at least one Distribution Rule with your user account.
2. Generate and print a Routing Sheet using the HP CR End User Interface application.
3. Assemble a test document. Add the Routing Sheet to the front of the document and go to the device.

   The main screen looks like this:

   ![Main screen screenshot]

4. Load the document into the document feeder.
5. Press Routing Sheet. (If this feature is not visible, use the scroll bar to find it.)

   **NOTE:** If you have configured prompts, you will see them now. Enter the appropriate prompt values and click Next. For information on configuring prompts, refer to the HP CR administrator on-line help.

   The device indicates it is ready to scan. When scanning from the Routing Sheet button, always keep the Routing Sheet first, followed by other documents.

6. To begin scanning, press Start on the display screen or on the hard keypad.

   Alternately, to change the scan attributes, click More Options.

   For example, you can specify the page size for the scanned document. The default page size is Letter. After you have made your modifications, click Start to begin scanning.

   The scan job starts. A progress indicator shows the scan job status.

   To stop the scan job, press Cancel Job. Otherwise wait for the job to finish. When scanning is complete, the device shows the scan completed message.

   The message is transferred to the HP CR server via HTTP/HTTPS where it is processed and routed to the intended recipient. If the document does not arrive at the destination, troubleshoot the setup. Refer to “Troubleshooting” in the HP CR administrator on-line help.
7. To scan another document using the Routing Sheet option, click Back. To end the session and go back to the main HP CR menu, click [Back] or the OK button.

**IMPORTANT:** If you see that the HP CR server cannot decipher or interpret the Distribution Rule instructions in the Routing Sheet, you must change the device setting from **mixed** to **text**. For instructions, refer to “Troubleshooting Issues When the HP CR Server Cannot Decipher the Distribution Rule Instructions in a Routing Sheet” in the HP CR administrator on-line help.

## 10-2 Testing the Device Administrator user interface

To test the Device Administrator user interface, complete the procedure for **Creating a group of devices** (21).

You can set up tests to test all authentication types at once by configuring groups on the HP CR server, with each group having a different authentication type:

- Email
- PIN
- Device
- Login

Then, test one device by uninstalling and reinstalling from each authentication type group to verify that all authentication types will work at once.