HP Capture and Route (HP CR) Embedded Device Client for HP OXPd Installation Guide HP Capture and Route (HP CR) Embedded Device Client for HP OXPd Installation Guide

Legal notices

(c) Copyright 2012 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

Date	Edition	Revision
September 2012	1	Version 1.2.0

Contents

1	Introduction	
	1-1 Embedded Device Client for HP OXPd overview	1
	1-1-1 Main components of the environment	3
	1-1-2 Installation components	3
	1-1-3 Document workflow	3
	1-1-4 Deploying Embedded Device Client for HP OXPd	5
	1-2 Basic requirements	6
	1-2-1 Supported devices	6
	1-2-2 Server requirements	7
	1-2-3 Device authentication requirements	7
	1-2-4 Configuring to use HTTPS	8
	1-2-5 Custom configuration	8
	1-3 On-line help and related documentation	8
2	Embedded Device Client for HP OXPd installation	
	2-1 Installing Embedded Device Client for HP OXPd v1.6	9
	2-2 Installing Embedded Device Client for HP OXPd v1.4	
	2-3 Installing Embedded Device Client for HP OXPd (v1 4 or v1 6) on a remote system	11
3	Configuration for HTTPS support	10
	3-1 Setting up a CA certificate and enabling SSL with Windows 2008	
	3-1-1 Requirements for setting up a CA certificate	
	3-1-2 Downloading the MakeCert executable	
	3-1-3 Creating the certificate	
	3-1-4 Installing the certificate to Internet Information Services (IIS)	
	3-1-5 Exporting the certificate to the OXPd v1.6 Device Client directory	
	3-1-6 Creating an SSL binding	
	3-1-7 Requiring SSL for the Virtual Web Sites	
	3-1-8 Verifying the SSL binding	
	3-1-9 Enabling directory browsing in IIS	
	3-1-10 Verifying HTTPS browsing	
	3-1-11 Editing the OmISAPIU.xml file	
	3-1-12 Editing the Bootstrap.xml file	
	3-2 Setting up a CA certificate and enabling SSL with Windows 2003 64-bit	
	3-2-1 Requirements for setting up a CA certificate	
	3-2-2 Downloading the MakeCert executable	
	3-2-3 Running the MakeCert executable and creating the certificate	18
	3-2-4 Exporting the certificate	19
	3-2-5 Requiring SSL for Web Sites	
	3-2-6 Editing the OmISAPIU.xml file	
	3-2-7 Editing the Bootstrap.xml file	27
4	Required configuration	
	4-1 Adding devices using the HP CR Server Administrator	29
	4-1-1 Creating a group of devices	
	4-1-2 Updating the Deviceloader.xml to support new devices	49
	4-1-3 Adding a new device	50
	4-2 Choosing an authentication method	52
	4-2-1 Configuring LDAP authentication	52
	4-2-2 Configuring HP authentication on the device	53

	4-2-3 Configuring authentication when Embedded Device Client for HP OXPd and HP CR Intelligent Dev Client are remote	ice . 54
	4-3 Configuring the server	. 55
5	Using HP's Web Jetadmin application to install OXPd v1.6 buttons on HP devices	
	5-1 Supported devices	. 57
	5-2 Exporting the XML files	. 58
	5-3 Installing OXPd v1.6 buttons	. 60
6	Testing	
	6-1 Testing the Routing Sheet feature	. 71
	6-2 Testing the Device Administrator user interface	. 72

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 Embedded Device Client for HP OXPd to multifunction devices running OXPd SDK v1.4.x and OXPd SDK v1.6.x.

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:

Embedded Device Client for HP OXPd overview (1)

Basic requirements (6)

On-line help and related documentation (8)

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

1-1 Embedded Device Client for HP OXPd overview

Embedded Device Client for HP OXPd 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 v1.4.x. These capabilities are founded in Distribution Rule technology.

Embedded Device Client for HP OXPd 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 Embedded Device Client for HP OXPd



In the main menu, Embedded Device Client for HP OXPd presents the device user with several HP CR scanning features.

Feature	Description	Login Required	Notes
Public Distributions	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.	No	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).
Personal Distributions	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.	Yes	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).
Scan to Me	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).	Yes	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 <u>Basic</u> requirements (6) and the <u>HP Capture and</u> <u>Route (HP CR) User Guide</u> .
Routing Sheet	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.	No	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).
Scan to Folder	The device scans and delivers the document to the HP CR folder via HTTP/HTTPS protocol. The HP CR server picks up the scanned document from the network folder, processes it and delivers it to the intended folder.	No	
Fax	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.	No	
Scan to My Files	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.	Yes	All jobs scan.

Table 1 HP CR scanning features in Embedded Device Client for HP OXPd

Feature	Description	Login Required	Notes
Nested Buttons	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.).	No	

1-1-1 Main components of the environment

The Embedded Device Client for HP OXPd 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 Intelligent Device Client as part of the server install. No separate installation of this component is required unless the Embedded Device Client for HP OXPd is installed on a remote system, and then the HP CR Intelligent Device Client would be installed on the remote system as well.

- Embedded Device Client for HP OXPd 1.6 (see page 9) and/or OXPd 1.4 (see page 10).
- **HP Device** See <u>Supported devices</u> (6) or a list with minimum firmware requirements.

1-1-2 Installation components

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

Component	Location	Function
Embedded Device Client for HP OXPd Install	\HP\HPCR\Clients	The setup contains the setup.exe file for both HP OXPd v1.4 and HP OXPd v1.6. Use this file to install the Embedded Device Client for HP OXPd.
Embedded Device Client for HP OXPd Configuration Manager	Devices node in the HP CR Server Administrator	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.

Table 2 Description of installation components with locations and functions

1-1-3 Document workflow

The workflow that moves a document from the device to its final destination involves the user, the device, the Embedded Device Client for HP OXPd, 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 Embedded Device Client for HP OXPd via HTTP/HTTPS protocol. The Embedded Device Client for HP OXPd then routes the document to the HP CR server via HTTP/HTTPS protocol. The Dispatch components applies rules to the message and HP CR server processes the message and routes them to the intended recipients.

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

IMPORTANT: For Scan to Me and Scan to Me with More features, 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 <u>HP Capture and Route (HP CR) Installation Guide</u>.

Figure 1-2 Workflow for Fax, Routing Sheet, Routing Sheet with More, Scan to Folder, Scan to Folder with More, Scan to Me and Scan to Me with More



When a user begins a scan session with the Public Distributions, Personal Distributions, or Scan to My Files option, the device requests the Embedded Device Client for HP OXPd to 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 <u>HP Capture and Route (HP CR) Installation Guide</u>.

The Embedded Device Client for HP OXPd 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 Embedded Device Client for HP OXPd. As soon as the Embedded Device Client for HP OXPd returns the data to the device, the basic workflow resumes.





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. User selects a Distribution Rule from the list and scans document.

B-Device delivers the document to the Embedded Device Client for HP OXPd via HTTP or HTTPS protocol.

C-Embedded Device Client for HP OXPd 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 Embedded Device Client for HP OXPd

1. Complete the installation requirements. (Device authentication requirements, 7)

NOTE: If you are planning to use HTTPS protocol, you must create a CA certificate before installing the Embedded Device Client for HP OXPd. For instructions, refer to the description of setting up a CA certificate using Microsoft Certificate Services and enabling SSL in <u>Section 4: Required configuration</u> (29).

- Install the Embedded Device Client for HP OXPd. See <u>Installing Embedded Device Client for HP</u> <u>OXPd v1.6</u> (9) or <u>Installing Embedded Device Client for HP OXPd v1.4</u> (10).
- **3.** Configure the embedded Web server of the device. Refer to the description of required configuration in the <u>HP Capture and Route (HP CR) Installation Guide</u>.
- 4. Configure the HP CR server. Refer to the description of configuring the server in the <u>HP Capture and</u> <u>Route (HP CR) Installation Guide</u>.

- 5. Configure optional capabilities. Refer to the <u>HP CR administrator on-line help</u>.
- 6. Test the HP CR scanning features on the device. Refer to Section 6: Testing (71).
- 7. Troubleshoot the setup if necessary. Refer to the <u>HP CR administrator on-line help</u>.

1-2 Basic requirements

1-2-1 Supported devices

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

Device	Group	Supported Firmware	Minimum Installed RAM	OXPd Version
Color LaserJet 4730 MFP	10	46.350.1	256 MB	1.4.9.0
Digital Sender 9200c	10	09.270.2	256 MB	1.4.9.0
LaserJet 4345 MFP	10	09.270.1	256 MB	1.4.9.0
LaserJet 9040 MFP	10	08.250.9	256 MB	1.4.9.0
LaserJet 9050 MFP	10	08.250.9	256 MB	1.4.9.0
LaserJet 9500 MFP	10	08.250.9	512 MB	1.4.9.0
Color LaserJet CM 4730 MFP	20	50.221.3	N/A	1.6.3.2
Digital Sender 9250c	20	48.171.2	N/A	1.6.3.2
LaserJet M3035 MFP	20	48.250.8	N/A	1.6.3.2
LaserJet M4345 MFP	20	48.250.8	N/A	1.6.3.2
LaserJet M4349 MFP	20	48.241.2	N/A	1.6.3.2
LaserJet M5035 MFP	20	48.241.2	N/A	1.6.3.2
LaserJet M5039 MFP	20	48.241.2	N/A	1.6.3.2
LaserJet M9040 MFP	20	51.191.3	N/A	1.6.3.2
LaserJet M9050 MFP	20	51.191.3	N/A	1.6.3.2
LaserJet M9059 MFP	20	51.191.3	N/A	1.6.3.2
Color LaserJet CM 6030 MFP	40	52.191.2	N/A	1.6.3.2
Color LaserJet CM 6040 MFP	40	52.200.4	N/A	1.6.3.2
Color LaserJet CM 6049 MFP	40	52.180.5	N/A	1.6.3.2
Color LaserJet CM 3530 MFP	50	53.180.3	N/A	1.6.3.2
Color LaserJet CM 4540 MFP	XX	2200887_229562	N/A	1.6.3.2
ScanJet 7000n	XX	2131311_192131	N/A	1.6.3.2
ScanJet 8500	XX	2200643_228340	N/A	1.6.3.2
LaserJet Flow M525 MXP	XX	2200893_229650	N/A	1.6.3.2a

Table 3 List of devices supported with Embedded Device Client for HP OXPd

Device	Group	Supported Firmware	Minimum Installed RAM	OXPd Version
LaserJet Flow M575 MXP	XX	2200893_229649	N/A	1.6.3.2
LaserJet M775 MFP	XX	2200890_229591		1.6.3.2
LaserJet M4555 MFP	XX	2200887_229566		1.6.3.2

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 Embedded Device Client for HP OXPd.

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.

NOTE: Only the OXPd 1.4 for Group 10 device model is supported. Other devices will fail to install.

1-2-2 Server requirements

Embedded Device Client for HP OXPd requires:

- HP CR Server
- At least one fax-enabled connector to support fax-based features
- HP CR ISAPI Device Client (included with default server install)

1-2-3 Device authentication requirements

The Embedded Device Client for HP OXPd 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**.

1-2-4 Configuring to use HTTPS

In order to use HTTPS protocol communication when sending documents from the device to the HP CR server, you must create a CA Certificate using Microsoft Certificate Services and enable Secure Socket Layer (SSL). You must create this certificate before installing the Embedded Device Client for HP OXPd. 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 Embedded Device Client for HP OXPd install.
- During the registration process for the OXPd application onto the device, 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 into the device.

For information on how to create a self-signed certificate using makecert.exe, refer to the description of <u>Adding devices using the HP CR Server Administrator</u> (29).

1-2-5 Custom configuration

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 <u>Creating a group of devices</u> (29).

1-3 On-line help and related documentation

- HP Capture and Route (HP CR) Installation Guide
- <u>On-line help for the administrator</u> (procedures for installing, uninstalling, and troubleshooting are included)
- On-line Quick Start Guides for HP OXPd v1.6 Device Client Quick Start Guides
- On-line Quick Start Guides for HP OXPd v1.4 Device Client Quick Start Guides
- On-line HP CR User Guide

2 Embedded Device Client for HP OXPd installation

This section describes:

Installing Embedded Device Client for HP OXPd v1.6 (9)

Installing Embedded Device Client for HP OXPd v1.4 (10)

Installing Embedded Device Client for HP OXPd (v1.4 or v1.6) on a remote system (11)

See also <u>Section 4: Required configuration</u> (29), <u>Section 6: Testing</u> (71), and the <u>HP CR administrator on-</u> <u>line help</u> (for additional information including optional configurations, testing, and troubleshooting).

2-1 Installing Embedded Device Client for HP OXPd v1.6

- 1. Logon 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\HPOXP1.6 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 for OXP 1.6 InstallShield Wizard opens.

🔂 HP Capture and Route for OXP 1.6 -	InstallShield Wizar	rd	×
HP Capture and Route for OXP 1.6 C	onfiguration		
Enter HP Capture and Route for OXP	9 1.6 Server name:		
InstallShield	< <u>B</u> ack	<u>N</u> ext >	Cancel

5. In the HP Capture and Route for OXP 1.6 Server name text box, enter the HP CR server name or IP Address.

- 6. Click Next and you are ready to install the program.
- 7. Click **Install** to begin installation. The setup installs Embedded Device Client for HP OXPd. The InstallShield Wizard shows a message indicating when the installation is complete.
- 8. Click Finish.
- 9. Continue to Section 4: Required configuration (29).

2-2

Installing Embedded Device Client for HP OXPd v1.4

- **1.** Logon to the system running the HP CR server using an account that belongs to the local Administrators group.
- 2. If you are installing on a default drive:

Navigate to the folder:

\\HP\HPCR\Clients\HPOXP1.4 and run setup.exe.

If you are installing on a non-default drive:

- a Open a command prompt window (run as Administrator).
- **b** Navigate to the HP CR Clients directory:

\\HP\HPCR\Clients\HPOXP1.4

c Enter the following command, where D:\Progam Files (x86)\HP\HPOXP1.4 is the location to which you want to install the client.

setup.exe /s /v"INSTALLDIR="D:\Program Files (x86)\HP\HPOXP1.4""

The Device Client will be installed on the D drive.

3. The InstallShield wizard launches with the Welcome page. Click Next.

The HP Capture and Route for OXP 1.4 InstallShield Wizard opens.

HP Capture and Route for OXP	1.4 - InstallShield Wizard	
HP Capture and Route for OXP	1.4 Configuration	
Specify the configuration informa	tion to use for this installation.	
Enter the HP Capture and Rou	ite for OXP 1.4 Intelligent Device Client Serv	er name:
	-	
VMWIN2008R2		
stallShield		
	< Back Next >	Cancel

- 4. In the HP Capture and Route for OXP 1.4 Server name text box, enter the HP CR server name or IP Address.
- 5. Click Next. The Ready to Install the Program page opens.
- 6. Click **Install** to begin installation. The setup installs Embedded Device Client for HP OXPd. The InstallShield Wizard shows a message indicating when the installation is complete.
- 7. Click Finish.
- 8. Continue to Section 4: Required configuration (29).

2-3 Installing Embedded Device Client for HP OXPd (v1.4 or v1.6) on a remote system

1. Logon to the system where you want to install Embedded Device Client for HP OXPd using an account that belongs to the local Administrators group.

NOTE: The system must be running Windows 2008 or 2003 64 bit and must have Embedded HP CR for Intelligent Devices (HP CR ISAPI Web Server Extension) installed.

2. For HP OXPd v1.6: Navigate to the \\HP\HPCR\Clients\HPOXP1.6 directory and run setup.exe.

For HP OXPd v1.4: Navigate to the \\HP\HPCR\Clients\HPOXP1.4 directory and run setup.exe.

The InstallShield wizard configures your system for installation and shows the Welcome message.

3 Configuration for HTTPS support

This section describes setting up a CA certificate using Microsoft Certificate Services and enabling SSL.

NOTE: If you are using HTTP, skip this section and go to Section 4: Required configuration (29).

If you require HTTPS support, you can follow the instructions in this section to set up a CA certificate with the Microsoft Certificate Services and enable SSL.

Setting up a CA certificate and enabling SSL with Windows 2008 (13)

Setting up a CA certificate and enabling SSL with Windows 2003 64-bit (18)

Otherwise, use a certificate from a trusted certificate authority. The certificate must be installed on the IIS system.

3-1 Setting up a CA certificate and enabling SSL with Windows 2008

The instructions in this section detail how to set up a CA certificate and enable Secure Socket Layer (SSL). The certificate must be created and installed in the IIS.

NOTE: If you are using Windows 2003 64-bit, refer to <u>Setting up a CA certificate and enabling SSL with</u> <u>Windows 2003 64-bit</u> (18).

3-1-1 Requirements for setting up a CA certificate

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 procedures for:

Downloading the MakeCert executable (14) Creating the certificate (14) Installing the certificate to Internet Information Services (IIS) (14) Exporting the certificate to the OXPd v1.6 Device Client directory (15) Creating an SSL binding (15) Requiring SSL for the Virtual Web Sites (15) Verifying the SSL binding (16) Enabling directory browsing in IIS (16) Verifying HTTPS browsing (16) Editing the OmISAPIU.xml file (17) Editing the Bootstrap.xml file (17) You should complete each procedure in the order in which they are presented.

3-1-2 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 <u>Microsoft documentation</u>.

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

3-1-3 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 01/01/2013 -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 Embedded Device Client for HP OXPd section of the <u>On-line help for the administrator</u>. 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.

3-1-4 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.
- 2. Select Install Certificate. The Certificate Import wizard is displayed.
- 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.

3-1-5 Exporting the certificate to the OXPd v1.6 Device Client directory

NOTE: Skip this procedure if you are using only the HP OXPd v1.4 Device Client.

- 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.
- 4. Choose the Copy to File option. The Certificate Export wizard opens.
- 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 (86) \HP\OXP1.6\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.

3-1-6 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.

3-1-7 Requiring SSL for the Virtual Web Sites

- 1. Open the IIS Manager.
- 2. Expand Local Machine > Default Web Site and select OXP1.6 (or OXP1.4).
- 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.

3-1-8 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.

3-1-9 Enabling directory browsing in IIS

- **1.** Open the IIS Manager.
- 2. Expand Local Machine > Default Web Site and select OXP1.6 (or OXP1.4).
- 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.

3-1-10 Verifying HTTPS browsing

- **1.** Open the IIS Manager.
- 2. Expand the Default Web Site.
- 3. Expand OXP v1.6 (or OXP v1.4).
- 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 v1.6:

.../OXP1.6/Configuration/

For HP OXPd v1.4:

.../OXP1.4/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).

3-1-11 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.

```
<FileTransfer>https://fully_qualified_domain_name/WebAPI/FileTransfer/</FileTransfer>
```

NOTE: XML files can be edited using Microsoft Notepad.

3. Save the file.

3-1-12 Editing the Bootstrap.xml file

1. Navigate to the following path.

```
For HP OXPd v1.6:
C:\Program Files (x86)\HP\OXP1.6\Configuration
For HP OXPd v1.4:
C:\Program Files (x86)\HP\OXP1.4\Configuration
```

2. In bootstrap.xml, change http to https.

```
<Server>https://fully_qualified_domain_name/webapi/scripts/omisapiu.dll
</Server>
```

- 3. Save the file.
- 4. Reset IIS.

3-2 Setting up a CA certificate and enabling SSL with Windows 2003 64-bit

The instructions in this section detail how to set up a CA certificate and enable Secure Socket Layer (SSL). The certificate must be created and installed in the IIS.

NOTE: If you are using Windows 2008, refer to <u>Setting up a CA certificate and enabling SSL with Windows</u> <u>2008</u> (13).

3-2-1 Requirements for setting up a CA certificate

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.

This section provides procedures for:

Downloading the MakeCert executable (14) Running the MakeCert executable and creating the certificate (18) Exporting the certificate to the OXPd v1.6 Device Client directory (15) Requiring SSL for Web Sites (25) Editing the OmISAPIU.xml file (27) Editing the Bootstrap.xml file (27)

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

3-2-2 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 <u>Microsoft documentation</u>.

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

3-2-3 Running the MakeCert executable and 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:

```
makecert.exe -r -pe -n "CN=fully_qualified_domain_name_of_iis_server" -b
01/01/2006 -e 01/01/2013 -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 Embedded Device Client for HP OXPd section of the <u>On-line help for the administrator</u>. If you key in the command text, note that there is a space at the end of the first three lines shown above.

3-2-4 Exporting the certificate

NOTE: This procedure applies to HP OXPd v1.6 Device Clients only.

Using the Web Server Certification wizard:

1. Open IIS and select Default Website properties. The Directory Security page is displayed.

Web Site	Performa	ance ISAPI Filters	Home Directory	Documents
Directory :	5ecurity	HTTP Headers	Custom Errors	ASP.NET
Authentica	ation and acc Enable an authentic	ess control onymous access and edit ation methods for this res	the purce. Edit	
IP address	and domain Grant or o IP addres	name restrictions deny access to this resour ses or Internet domain na	ce using mes. Edit	
Secure cor	nmunications			
*	Require si enable dia resource i	ecure communications and ent certificates when this is accessed.	Server Certi View Certif	ficate
			Edit	

 Click the Server Certificate button. The Welcome to the Web Server Certification Wizard page is displayed. 3. Click Next. The IIS Certification Wizard is displayed.



4. Select Assign an existing certificate. Click Next. The certificate created using MakeCert.exe is displayed.

ielect a certificate	1	In the pro-	1
OI DBU221	VB Dau221	Expliation U ate	Inlended Purp
		1100	

5. Click Next. A window is displayed prompting for the SSL port..

IIS Certificate Wizard	2
SSL Port Specify the SSL port for this web site.	
SSL port this rveb site should use:	
	< Back Next > Cancel

6. The port selected should be 443. Click Next. The Certificate Summary is displayed.

IIS Certificate Wizard		×
Certificate Summary You have chasen to inst	al an existing certificate.	
The following certilicale i certificate, cick Next Certificate details:	s evailable for installation on your Web server. To install this	
Issued To Issued By Expiration Date Friendly Name	sr14Dsps1.quality.net sr14Dsps1.quality.net 1./1/2013 <none></none>	
	< Black Next> Cance	:1

- 7. Click Next. A message indicates that the Web Server Certificate wizard is completed.
- 8. Click Finish. You are returned to the Directory Security page.
- 9. Export the certificate:
 - a Open IIS\local machine and navigate to the **Default Web Site** node.
 - **b** Select web site **OXP1.6**.

c Right-click and select Properties.

Thternet Information Services	(IIS) Manayer <u>H</u> elp		×
⇔ → 🗈 🖬 🗙 🗗 🖸		II	
Internet Information Services I SR1405YS2 (local computer) Application Pools Web Sites Default Web Site OXP1.6 OXP1.6 Web Service Extensions Oxefault SMTP Virtual Service	XP1.6 Properties Virtual Directory Docume The content for this re (*) (*	ants Directory Security HTTP Header source should come from: A girectory located on this computer A ghare located on another computer A redirection to a URL C:)Program Files (x86))(HP\OXP1.6) s I cog visits I index this resource	? × s Custam Errors Brgwse
	Application settings Application name: Starting point: Execute germissions: Application pool:	CXP1.6 <default site="" web="">\CXP Scripts only OXP1.6</default>	Remove Configuration
	[OK Cancel Ap	ply Həlp

d Click the Directory Security tab.

ull Web Sil	e Properties		22.1		-
Web Site	Performance	15APt Filters		Home Dired	tory
Documents	Directory Security	HTTP Hea	ders	Custom E	mors
Authenticati	an and access control				
₩¢	Enable anonymous access a authentication methods for	and edit the this resource.]	Edit	
(P address a	and domain name restrictions	-			
8	Grant or deny access to this IP addresses or Internet do	s resource using main nantes.	2		
				Edļt	
Secure cam	nunications				
	Require secure communicati enable client certificates wh resource is accessed.	ians and ien this	Server	Certificate	
				Edit	
			1	1	

e In the Secure communications section, click the View Certificate button.

f Click the **Details** tab. Select the newly created certificate name.

ield	Value
Valid from Valid to Subject Public key Authority Key Identifier Thumbprint algorithm	Sunday, January 01, 2006 12: Tuesday, January 01, 2013 1 sr140sys2.quaity.net RSA (1024 Bbs) KeyID=60 28 6d ac 39 c6 af f sha1
S Fierdy rang	art/Osys2 quality.ho:
140sys2.quaity.net	

- g Click the Copy to File button. The Welcome to the Certificate Export Wizard screen is displayed.
- h Click Next. The Export Private Key page is displayed.

Certificate Export Wizard	X
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key w certificate, you must type a password on a later page.	ith the
O Yes, export the private key	
No. do not export the private key	
< <u>Back</u> <u>N</u> ext >	Cancel

i Select No, do not export the private key and click Next. The Export File Format page is displayed.

Certificat	ernal as can be exported in a variety of file forma	ıts.
Select th	s farmat you want to use:	
Οĝ	IR encoded binary X, 509 (.CER)	
€в	128-64 encoded X.509 (.CER)	
0 0 1	yptographic Message Syntax Standard - PK _ Include all cartificaties in the cartification p	:C5 #7 Certificates (.P7B) path if possible
С в Г	rsond Information Exchange - PKC5 #12 (, Include all certificates in the certification p	PFK) path if possible
Г	Enable strong protection (requires IE 5.0,	NT 4.0 SP4 or above)
Г	Delete the private <u>k</u> ey if the export is suc	ceeeful

- j Select Base-64 encoded x.509 (CER). Click Next.
- **k** Browse to this location.

C:\Program Files (x86)\HP\OXP1.6\Certificate\

I Enter the file name as:

Webserver.cer

- m Click Save. A message indicates the export was successful. Click OK.
- n Click Finish to exit the Certificate Export wizard.

3-2-5 Requiring SSL for Web Sites

- 1. Open IIS\local machine and navigate to the **Default Web Site** node.
- 2. Select web site OXP1.6 (or OXP1.4).
- 3. Right-click and select Properties.

Internet Information Services (IIS) Manayer		
	1eb	II 11	
Internet Information Services ISR 1405Y52 (local computer) Application Pools Web Site Default Web Site Default Web Site OXP1.6 Default Service Extensions Default SMIP Wrtual Service	KP1.6 Properties Wrbual Directory Docume The content for this re (*) (*) (*)	ants Directory Security HTTP Her source should come from; A directory located on this computer A ghara located on another computer A redirection to a URL :\Program Files (x86)\HP\OXP1.6) s	? × aders Custam Errors ar Brgwse source
	Application settings Application name: Starting point: Execute germissions: Application pool:	CXP1.6 <default site="" web="">\OXP Scripts anly OXP1.6</default>	Configuration
	[OK Cancel	Арріу Неф

4. Click the Directory Security tab.



5. In the Secure communications section, click the Edit button. The Secure Communications page is displayed.

Require secure channel (SSL);	
Require 128-bit encryption	
Client certificates	
Ignore client certificates	
C Accept dient certificates	
Require client certificates	
Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using direct certificates.	Edt.
]

- 6. Select Require secure channel (SSL) and Require 128-bit encryption.
- 7. Click OK twice.

3-2-6 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 fully qualified domain name. Also, change http to https.

```
<FileTransfer>https://fully_qualified_domain_name/WebAPI/FileTransfer/</FileTransfer>
```

NOTE: XML files can be edited using Microsoft Notepad.

3. Save the file.

3-2-7 Editing the Bootstrap.xml file

1. Navigate to the following path.

```
For HP OXPd v1.6:
C:\Program Files (x86)\HP\OXP1.6\Configuration
For HP OXPd v1.4:
C:\Program Files (x86)\HP\OXP1.4\Configuration
```

2. In bootstrap.xml, change http to https.

```
<Server>https://fully_qualified_domain_name/webapi/scripts/omisapiu.dll
</Server>
```

- 3. Save the file.
- 4. Reset IIS.

4 Required configuration

This section describes:

Adding devices using the HP CR Server Administrator (29)

Choosing an authentication method (52)

Configuring the server (55)

See also <u>Section 6: Testing</u> (71) and the <u>HP CR administrator on-line help</u> (for additional information including optional configurations, testing, and troubleshooting).

4-1 Adding devices using the HP CR Server Administrator

This section describes the procedures for:

Creating a group of devices (29)

Updating the Deviceloader.xml to support new devices (49)

Adding a new device (50)

4-1-1 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.



IMPORTANT: For HP OXPd v1.6 (Windjammer-based) OZ devices, the name of the group must not contain any spaces. For example:

Correct: Group Name = EastCoastSales Incorrect: Group Name = East Coast Sales

The following procedure explains how to create and configure a 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 1.6 group (or HP OXPd 1.4 group).



The New Group page opens.

New Group	×
General S	Settings Authentication Buttons Advanced
Туре:	HP 0XPd 1.6
<u>N</u> ame:	
<u>D</u> escription	
	OK Cancel

- 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 <u>only</u> if the IIS/Web server is remote or if you are configuring HTTPS.

General Se	tings Authentication Buttons Advanced
Application U	RL: http://SERVER_IP/OXP1.6/
Web API	http://SERVER_IP/WebAPI/Scripts/omisapiu.dll
Timeout:	C Automatically exit UI after 60 🚖 seconds of inactivity. © Do not exit UI Automatically
	OK Cancel

NOTE: If you installed HP CR for Embedded Device Client for HP OXPd on a remote system, you must manually enter the IP address of that system.

NOTE: If you are installing as HTTPS, change the URL path from HTTP to HTTPS. For example: Application URL: https://FQDN/OXP1.6/ Web API: https://FQDN/WebAPI/Scripts/omisapiu.dll 8. Click the **Authentication** tab to specify the type of user authentication required for the group of devices.

Device Group Properties	×
General Settings Authentication Buttons Advanced	
Iype: Device]
Fields: Domain User Entered User User Entered Password User Entered	Properties
LDAP Lookup Settings	
Server: VMAD70.vmad700.com	
Port: 389	
Search Base: DC=vmad700,DC=com	
Eilter: [&(objectClass=user)(sAMAccountName=[USER_NAME]))	
<u>U</u> sername:	
Pass <u>w</u> ord:	
Attribute Map: Exchange.default.xml	•
Test LDAP Loc	okup
Confirm authe <u>n</u> tication	
Message: @msgConfirmation	_
	Cancel

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

Device is the default and requires no configuration. In this case, the **Fields** section and **Properties** button are not active. The HP CR server is only verifying the native DEVICES LDAP query information.

If you select **Email**, **Login**, or **PIN** as the authentication type, you can define the properties for the **Domain**, **User**, and **Password**. For example, if you select **Email**, notice that the **Fields** section is active:

Device Group Properties	×
General Settings Authentication Buttons Advanced	
Iype: Email	
Fields: Domain User Entered User User Entered Password User Entered	Properties
LDAP Lookup Settings	
Server: VMAD70.vmad700.com	_
Port: 389	
Search Base: DC=vmad700,DC=com	
Eilter: [&(objectClass=user)(proxyAddresses=SMTP:[USER_NAME]))	
Username:	
Password:	
Attribute Map: Exchange.default.xml	•
Test LDAP Lookup	
Confirm authentication	
Message: @msgConfirmation	
OK	Cancel

Domain, User, and Password properties are described on the following pages.

Defining Domain Properties

To define domain properties, double-click Domain. The Domain Field Properties dialog is displayed:

Domain Field Pr	operties	×
Label:	@authDomainLabel	
Defaul <u>t</u> value:		
User must ent	er a value for Domain	
🔲 Enable inp	put <u>v</u> alidation	
Regular E	zpression:	
Error mes	sage: @authDomainErrorText	
O User <u>m</u> ust sele	ect a value for Domain from one of the following:	
		<u>A</u> dd
		<u>R</u> emove
		Set Default
		∧ v
O User may not	enter a value for Domain	
🗌 Displa <u>y</u> the	e default value to the user (read-only)	
	ОК	Cancel

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.

NOTE: Domain definition is optional for all authentication types.

Defining User Properties

To define user properties, double-click User. The User Field Properties dialog is displayed:

User Field Prop	perties	×
Label:	PIN	
Default value:		
C Liser must er	pter a value for liser	
Enable in	nor a value for eser	
Regular	Expression	
Front De	Copy Copy the Loss Encor To ye	
Litter me	waddioserErrorText	
O User must set	elect a value for User from one of the following:	
1234		Add
4567		Remove
		Set Default
		^ v
C User may no	t enter a value for User	
🗖 Display ti	he default value to the user (read-only)	
	ОК	Cancel

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.

NOTE: User definition is required for Login authentication and optional for all other authentication types.

Defining Password Properties

To define user properties, double-click User. The User Field Properties dialog is displayed:

Password Field	Properties	×
Label:	PW	
Default value:		
 User must er 	nter a value for Password	
📃 Enable ir	nput validation	
Regular	Expression:	
Error me	essage; @authPasswordErrorText	
C User must se	elect a value for Password from one of the following:	
		Add
		Remove
		Set Default
		^ V
O User may no	t enter a value for Password	
🔲 Display ti	he default value to the user (read-only)	
	ОК	Cancel

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:

Device Group Pi	roperties				×
General Settir	as Authentication Butt	ons Advanced	1		
Tune:	in International				1
Fi <u>e</u> lds: Dor Use	nain er	User Entered User Entered	1	Properties	
Pas	sword	User Entered	t		
LDAP Lookup	Settings				
Server: VM/	AD 70. vmad700. com				
P <u>o</u> rt: 389	•				
Search <u>B</u> ase	DC=vmad700,DC=com				
<u>F</u> ilter:	(&(objectClass=user)(sA	MAccountName	=[USER_NAME]))		
<u>U</u> sername:					
Pass <u>w</u> ord:					
<u>A</u> ttribute Map	Exchange.default.xml			•	
			Test LDAP Look	up	
🗖 Confirm auti	he <u>n</u> tication				
<u>M</u> essage:	@msgConfirmation			_	
				Cancel	

- **11.** 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.

14. Click the **Buttons** tab where you can add or remove buttons that appear on the device.

Device Group Properties		×
General Settings Authentication Buttons Advanced		
Device Home Screen 		Properties Add Remove Move ^ v
	OK	Cancel

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

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

Add But	ton		×
Type:			
Name:			
		OK	Cancel

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

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

Add Bul	tton
<u>T</u> ype:	Routing Sheet
<u>N</u> ame:	Fax Nested Button Personal Distributions Public Distributions Routing Sheet
	Scan to Destination Scan to Distribution Scan to me

- **17.** Enter a **Name** for the button. Then, click **OK**.
- **18.** You will need to define properties for the button. With the button highlighted on the list, click **Properties**.

Button Prope	rties 🗙
General Jot	p Properties Prompts Device Settings
Туре:	Routing Sheet
Name:	Routing Sheet
Display Text:	@buttonroutingsheetText
Description:	@buttonroutingsheetDesc
Image:	routingsheet
Location:	Auto assign based on configured ordering Use specific ordering priority:
Options:	 Enable this button for use on the device Enable job build Enable One-Touch scanning Enable scan preview by default (only on supported devices) Require authentication Capture user password
	OK Cancel

Each button has a default Name, Display Text, and Description that you can edit.

NOTE: Do not change Image from the default value.

- **19.** 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.
- 20. Select addition 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 applies to Futuresmart devices only.
- **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.

21. If you are adding a Personal Distributions of Public Distributions button, c	CIICK THE UP	Dtions tab.
---	--------------	--------------------

Button Properties	×
General Options Job Properties Prompts Device Settings	
Public Email: administrator@vmad1.com	
Enumeration Limit: 24 🛖	
	OK Cancel

Enter a **Public Email** address (if applicable) and set the **Enumeration Limit** for distributions (the maximum number of distributions allowable).

22. If you are adding a **Scan to Distribution** button, click the **Options** tab to route using an existing (already created) distribution.



Click Select and the Select Embedded Directive dialog is displayed.

🔯 Select Embedded Directive		×
Title		
🔲 Owner e-mail:		
Date created: 8/15/2012	to 8/15/2012 +	
Date last used: 8/15/2012	to 8/15/2012	
Expired		
🔲 Single use		
🗖 Public		
		Find
Tala t Quarte	Constant Landland Circletter Environ	T Calast
Title 🔺 Owner	Created Last Used Single Use Expires	Select
Title 🔺 Owner	Created Last Used Single Use Expires	Select Cancel
Title 🔺 Owner	Created Last Used Single Use Expires	Select Cancel
Title 🔺 Owner	Created Last Used Single Use Expires	Select Cancel Properties
Title 🔺 Owner	Created Last Used Single Use Expires	Select Cancel Properties
Title 🔺 Owner	Created Last Used Single Use Expires	Select Cancel Properties
Title 🔺 Owner	Created Last Used Single Use Expires	Select Cancel Properties
Title Owner	Created Last Used Single Use Expires	Select Cancel Properties

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

Select the distribution and then click the **Select** button to choose the distribution that will be used when that button is selected from the device.

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

Button Properties X
General Options Confirmations Job Properties Prompts Device Settings
Allow Coverpage to be specified
Include Coverpage by default
Defaults:
Subject:
Comment:
Recipient Name:
Sender Name:
OK Cancel

- 24. If you are adding a Fax button, 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).

Button Properties × General Options Confirmations Job Properties Prompts Device Settings Allow user to specify confirmations: ⊡ Authenticated Users Properties --- Email on Failure --- Print on Failure -- Email and Print on Failure Remove None . Unauthenticated Users --- Print on Failure --- None **Confirmation Properties** × Email on Failure Name: Display Text: @labelEmailDelivery Recipients: %\\prOriginator% Properties Add... Remove OK Cancel

For example, you can edit the fields for the Originator for faxed faxes:

25. 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.

Button Properties	×
General Job Properties Prompts Device Settings	
<pre>Message prOriginator = HPCapture&Route prOriginatorType = 0 prBecipientType = 0 Transformations</pre>	Properties Add Remove
OK	Cancel

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

Recipient				×
Property:	prDestination			
Value:	routingsheet			
			ОК	Cancel

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 is set to send to a destination of MyFiles, which can have an outbound rule associated with that destination to route to any location to which the HP CR server can route messages. This destination value can be edited.
- Transformations can also be added here.

eneral Job Properties Prompts Device Settings	
⊡- Message	Properties
	Add
Recipient prDestination = myfiles prRecipientType = 0 Transformations	Remove

26. 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**.

27. 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.

Button Properties		×
General Options Jo	h Properties Promots Device Settings	
		· · · · · · · · · · · · · · · · · · ·
Setting	Value	Properties
Resolution	300 DPI	
Duplex Calas Mada	Halse	
Compression	Monochrome	
Drientation	Portrait	
Media Size	Letter	
	ОК	Cancel

a a stanting		Value	Properties
Resolution		300 DPI	
Duplex		False	
Color Mode		Monochrome	
Compression		Redium	
Media Size		l etter	
	Description		
Device Setting	Properties		^
Resolution:	300 DPI		•
	150 DPI		
	200 DPI		
	300 DPI		
	000 DP1		

Select a setting and click **Properties** to change the setting value. For example:

28. 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.

29. Click the **Advanced** tab to modify settings that control the device's native settings for connectivity timeouts and job refresh settings.

Name	Value	Properties
ConfigurationRefreshInterval DelayCount JobRefreshTimer ConnectionTimeout ResponseTimeout RetryInterval MaxConsecutiveRetries UIInactivityTimer	1800 100 3 60 300 60 3 60	Add Remove
IOTE: These settings are advanc longer work and should or	ed and changing them could c ly be done when requested by !	ause the button to no Support.

NOTE: Take note of all defaults before changing any of these settings.

- 30. Click OK to end your work with the Device Group Properties.
- **31.** Once a button configuration is complete, 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 <u>Installing OXPd v1.6 buttons</u> (60).

4-1-2 Updating the Deviceloader.xml to support new devices

If you need to update the Deviceloader.xml to include new devices, refer to <u>HP CR administrator on-line</u> <u>help</u>.

4-1-3 Adding a new device

- 1. In the console tree, expand the HP CR server and go to the **Devices** node.
- 2. Right-click and select the group name. Then, select New > Device.

The **Properties for device** page opens.

Properties for device	×
General Device Configuration Journal	
(Device Details Not Known)	
Name:	
Description:	
Network Address:	
Group: 2nd floor HP	•
OK Ca	ncel <u>H</u> elp

- 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 **Device Configuration** tab. The following example is for HP OXPd v1.6 devices:

Properties for	device	×
General Devi	ce Configuration Journal	
Device Authen	tication	
Username:	[
Password:		
SNMP Commu	nity Strings	·
Public:	public	
Private:	HXXXXX	
	OK Cancel Help	

When installing to an HP OXPd v1.4 device using HTTPS, you must select the **Use SSL for secure communication** option.

	HP OXPd 1.4 device		2
General Dev	ice Configuration	al	
Device Auther	ntication		
Usemame:	admin		
Password:			
Use SS	L for secure communicati	ion	

- 7. In the Username text box, enter the device Administrator name.
- 8. In the **Password** text box, enter the Administrator password.

- **9.** If you are using HP OXPd v1.6, configure the **SNMP Community Strings** section (this section will not appear for HP OXPd v1.4).
 - 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.

- **10.** Click **OK** to add the device.
- **11.** 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.
- **12.** After a successful query, right-click and select **Install**.
- **13.** Verify that the buttons appear on the device.

4-2 Choosing an authentication method

The Embedded Device Client for HP OXPd must be able to authenticate the device user when the **Personal Distributions** or **Scan to My Files** option is used.

You can configure:

- LDAP authentication
- HP authentication at the device

4-2-1 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 Embedded Device Client for HP OXPd 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 <u>HP documentation</u>.)

Figure 4-1 Example of an LDAP authentication configuration for Active Directory

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).

Information Setti	i ngs (Digital Sending) (Networking)	
Configure Device	LDAD Authenticotion	
E-mail Server	LDAP Authentication	
Alerts		
AutoSend	Accessing the LDAP Server	
Security	I DAP Server Bind Method:	Dimute
Authentication Manager	LDAP Server	Simple
LDAP Authentication	LDAF Server.	1711100.005
Kerberos Authentication	Port:	389
PIN Authentication		
Edit Other Links	Credentials	
Device Information	O Use Device User's Credentials	
Language	Bind Prefix:	cn
Date & Time	C	
Wake Time	O Use LDAP Administrator's Credentials	
	LDAP Administrator's DN	
	Password:	
Other Links		
hp instant support Order Supplies	Searching the Database	
Product Support	Bind and search Root:	ou=engineering,cn=users,dc=hp,dc=com
	Match the name entered	
	with the LDAP attribute of	cn
	Retrieve the device user's	
	email address using attribute of	mail
	and name using the attribute of	displayName

4-2-2 Configuring HP authentication on the device

- 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
 - Scan to Me with More

The list shows the options that are installed with Embedded Device Client for HP OXPd, 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.

Device	Authentication Managor		
es/Types	Authentication Manager		
Server			
	Set the Device Functions that require users to succe	ssfully sign in before us	e. Each function can require a different Sign In Method.
end			
rity	Home Screen Access	Sign In Method	
entication Manager			
Authentication	Sign In At Walk Up	None	•
eros Authentication	Device Functions	Sign In Method	
e PIN			
PIN	Сору	None	•
)ther Links	Color Copy	None	•
e Information	Send to E-mail	None	v
uage	Send Fax	None	
& Time	Send to Folder	None	
Schedule	Job Storage	None	•
ict Color	Create Stored Job	None	 ▼
icate Management	Digital Sending Service (DSS) Secondary E-mail	None	•
Screen Setup	Digital Sending Service (DSS) Workflow	None	•
C-Agent	Simplex Copy	None	•
r Links	Public Distributions	None	
stant support	Personal Distributions	None	
for Supplies	Fax	None	
uct Support	Routing Sheet	None	
	Scan To Me		
	Scan To Folder	Nana	
	Scan to rober	None	
	HP AC Express	HPAC - PIC Server	
	Scan To My Files	LDAP	•

- 7. Click Apply.
- 4-2-3 Configuring authentication when Embedded Device Client for HP OXPd and HP CR Intelligent Device Client are remote

IMPORTANT: This section is applicable only if you have chosen to configure HP CR authentication. It is not applicable if you have chosen to configure HP native authentication.

For situations when the HP CR Intelligent Device Client is remote, configure the UseABService node in the Configuration.xml file so that HP CR for HP OXPd talks directly to Active Directory.

It is necessary for both HTTP and HTTPS and for all types of authentication - that is PIN, PIN with password, non-authentication email and Login with password.

To configure authentication for when HP CR Intelligent Device Client is remote:

- 1. Navigate to: C:\Program Files\HP\HPCR\HPOXP\Configuration
- 2. Open configuration.xml for editing.
- 3. Search for the <Search UseABService node.
- 5. Save your changes to the configuration file.

- 6. Open a command prompt and click Start > Run.
- 7. Enter cmd and then perform an iisreset.
- **8.** Load the HP CR buttons using the force update option. For instructions, see the <u>HP CR</u> <u>administrator on-line help</u>.

NOTE: It is necessary to stop all the web site and application pools and restart them. Without this reset, the changes to configuration.xml are not reflected. Then, during authentication, Embedded Device Client for HP OXPd talks directly to the Active Directory.

4-3 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 Embedded Device Client for HP OXPd. Now you are ready to test the HP CR scanning features. Continue with the information in <u>Section 6: Testing</u> (71).

Required configuration

5 Using HP's Web Jetadmin application to install OXPd v1.6 buttons on HP devices

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

Supported devices (57) Exporting the XML files (58) Installing OXPd v1.6 buttons (60)

5-1 Supported devices

The following devices are supported:

Table 1 HP Device Series Matrix

Device	Operating System
Color LaserJet 4730 MFP	
Digital Sender 9200c	
LaserJet 4345 MFP	
LaserJet 9040 MFP	
LaserJet 9050 MFP	
LaserJet 9500 MFP	
Color LaserJet CM 4730 MFP	Oz
Digital Sender 9250c	Oz
LaserJet M3035 MFP	Oz
LaserJet M4345 MFP	Oz
LaserJet M4349 MFP	Oz
LaserJet M5035 MFP	Oz
LaserJet M5039 MFP	Oz
LaserJet M9040 MFP	Oz
LaserJet M9050 MFP	Oz
LaserJet M9059 MFP	Oz
Color LaserJet CM 6030 MFP	Oz
Color LaserJet CM 6040 MFP	Oz
Color LaserJet CM 6049 MFP	Oz

Device	Operating System
Color LaserJet CM 3530 MFP	Oz
Color LaserJet CM 4540 MFP	FutureSmart
ScanJet 7000n	FutureSmart
ScanJet 8500	FutureSmart
LaserJet Flow M525 MXP	FutureSmart
LaserJet Flow M575 MXP	FutureSmart
LaserJet M775 MFP	FutureSmart
LaserJet M4555 MFP	FutureSmart

5-2 Exporting the XML files

Complete the following procedure for HP CR to configure the HP OXPs device client with the desired settings.

- Once the configuration is complete (as described in <u>Section 2: Embedded Device Client for HP</u> <u>OXPd installation</u> and <u>Section 4: Required configuration</u>), right-lick 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**:

Browse For Folder Select folder to store Web Jet Admin export	×
 Desktop Libraries Administrator I = Computer Computer Network Fax_output 	
Folder: Administrator	
Make New Folder OK Can	

Make New Folder:

🧾 Desktop		
⊞ ☐ Libraries ∴ Administrator		
E 🙀 Network		
Fax_output New folder		
-		

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

퉬 New folder				
New folder	r			👻 🔯 Search New folder
Organize 🔻 Include in libra	ary 🔻 Share with 🔻 New folder			
🚖 Favorites	Name *	Date modified	Туре	Size
🧮 Desktop	FutureSmart-Fax	9/13/2012 7:12 PM	XML Document	6 KB
Downloads	FutureSmart-HP Capture and Route	9/13/2012 7:12 PM	XML Document	4 KB
🕍 Recent Places	FutureSmart-Personal Distributions	9/13/2012 7:12 PM	XML Document	7 KB
🚝 Libraries	FutureSmart-Public Distributions	9/13/2012 7:12 PM	XML Document	7 KB
	FutureSmart-Routing Sheet	9/13/2012 7:12 PM	XML Document	6 KB
🌙 Music	🕋 FutureSmart-Scan To Me	9/13/2012 7:12 PM	XML Document	6 KB
📔 Pictures	📄 FutureSmart-Scan To My Files	9/13/2012 7:12 PM	XML Document	7 KB
📑 Videos				
👰 Computer				

5-3 Installing OXPd v1.6 buttons

Once the XML files have been edited and you are able to discover devices using the Web Jetadmin application, you can install HP OXPd 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 is displayed.

A Create Group					? ×
Specify gro	up options				
Group identific Group name: Parent group: Group member (C Manual gro (Devices a	ation 02 Groups ship type sup are added or removed by	y the user)			
C Automatic (Devices a	group are automatically added	or removed based on	filter criteria)		
Configure gr	oup properties now				
				Next >	Cancel

2. Enter the name of the new group that you will use to group similar devices for HP OXPd 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 the group name is correct. The **Confirm** page is displayed, showing the settings for the group.

Freate Group		
onfirm		
Settings		
Group name:	Oz	
Parent group:	<no parent=""></no>	
Description:	<not specified=""></not>	
Contact:	<not specified=""></not>	
Membership type:	Manual (0 devices)	
Policies:	0	

- 4. Click Create Group and then Done.
- 5. Right-click the newly created group and select Add devices to group.



NOTE: For more options in using the Web Jetadmin device filters to find or add devices, consult HP's Web Jetadmin team for a complete Web Jetadmin installation guide.

The Select Devices page is displayed.

IP Hostname IP / FP NPID1240D 0.13 CAN0N4F5598 172 /2320bii M NPID64D7F 172 // S40 MFP NPI48C028 172 // S40 MFP NPI48C028 172 // SF0 MFP NPI48C028 172 // SFP NPI84A104 172	ce Model IP Hostname IP / asesJet M3035 MFP NPID1240D nn R-ADV 6065 40.13 CANON4F5598 Toolc LasesJet CM2320bi M. NPI82A248 asesJet 435 MFP NPI48C028 172 >> Color LasesJet CM4540 MFP NPI48C028 172 >> asesJet M4555 MFP NPIB4A104 172
PP NPID1240D 0.13 CANON4F5598 172 /42320bii M NPI82A248 172 > NPID6AD7F 172 /4540 MFP NPI48C028 172 /h Series HPF2A85C 172 FP NPI84A104 172	aseulet M3035 MFP NPID1240D nn R-ADV 6065 40.13 CAN0N4F5598 172 Color Laseulet CM2320bii M. NPI82A248 172 aseulet 4345 MFP NPID6AD7F 172 Color Laseulet CM4540 MFP NPI49C028 172 Jifficejet Pro X451dn Series HPF2A85C 172 aseulet M4555 MFP NPIB4A104 172
113 CANON4F5598 172 42320bii M NPI82A248 172 NPID6AD7F 172 4540 MFP NPI48C028 172 An Series HPF2A85C 172 FP NPI84A104 172	nn IR-ADV 6065 40.13 CANDN4F5598 172 Color LasexJet CM2320bii M. NPI82A248 172 asexJet 4345 MFP NPI06AD7F 172 Color LasexJet CM4540 MFP NPI48C028 172 Ulficejet Pro X451dn Series HPF2A85C 172 asexJet M4555 MFP NPI84A104 172
42320hi M. NPI82A248 172 NPID6AD7F 172 4540 MFP NPI48C028 172 An Series HPF2A85C 172 FP NPI84104 172	Color LasesJet CM2320bii M. NPI82A248 172 assesJet 4345 MFP NPID6AD7F 172 Color LasesJet CM4540 MFP NPI48C028 172 Jifficejet Pro X451dn Series HPF2A85C 172 assesJet M4555 MFP NPI84A104 172
NPID6AD7F 172 4540 MFP NPI48C028 172 An Series HPF2A85C 172 FP NPIB4A104 172	asesJet 4345 MFP NPID6AD7F 172 Color LasesJet CM4540 MFP NPI48C028 172 Ulficejet Pro X451dh Series HPF2A85C 172 asesJet M4555 MFP NPIB4A104 172
1540 MFP NPI48C028 172 In Series HPF2A85C 172 FP NPI84A104 172	Color Lases/Jet CM4540 MFP NPI48C028 172 Ufficejet Pro X451dn Series HPF2A85C 172 abes/Jet M4555 MFP NPIB4A104 172
In Series HPF2A85C 172 >> FP NPIB4A104 172	Utficejet Pro X451dn Series HPF2A85C 172 abel Jet M4555 MFP NPIB4A104 172
FP NPIB4A104 172	abel/et M4555 MFP NPIB4A104 172
	i i i i i i i i i i i i i i i i i i i
14	14

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) will be added to the **Devices to add** list (on the right).

IP Hostname NPID1240D	IP /	Device Model	IP Hostname
NPID1240D			
	<td>HP LaserJet 4345 MFP</td> <td>NPID6AD7F</td>	HP LaserJet 4345 MFP	NPID6AD7F
CANON4F5598	172		
M NPI82A248	172		
NPI48C028	172		
HPF2A85C	172 >		
NPIB4A104	172 >>		
	<		
	M NPI824248 NPI492028 HFF2A88C NPI84A104	M NPI82A248 172 NPI48C028 172 HFF2A88C 172 NPI84A104 172 >>>	M. NPI82A248 172 NPI48C028 172 HFF2A85C 172 NPIB4A104 172 →> <<<

7. Click Next. The Confirm page is displayed.

Add Devices			?
onfirm			
Settings iroup name: OZ Devices:			
Device Model	IP Hostname	IP Address	
HP LaserJet 4345 MFP	NPID6AD7F	172.16.5.131	

- 8. Click the **Add Devices** button. You should see the devices added to your new group in the **Group** window.
- **9.** Highlight the device(s) to which you want to install buttons.

OZ (1 of 3 Selected)						
Layouts 👻	🍸 Filters 🔹 🚺	🤣 📾 🖬 👼				
Device Model	IP Address	IP Hostname	Port (Any)	Severity	Hardware Address	
HP LaserJet M4345 MFP	172.16.5.208	NPI822592	1	0	001708822592	
HP Color LaserJet 4730 MFP	172.16.5.130	NPI5BDA67	1	Â	0014385BDA67	
HP Color LaserJet CM6040 MFP	172.16.5.117	NPI1CB481	1	<u> </u>	001B781CB481	
	i - 1 -	1	f f .			
Contig Alerts Troubleshoot	Groups Reports	s Supplies Storage	e Solutions Ca	apabilities Firm	re	
oply Template 💯 View History	Customize	. SRefresh				
ly Settings 🔄	Alternative L	etterhead Mode				
Alternative Letterhead Mo	C On					
- Asset Number	● Off					
Auto Cleaning Page	Accel Number					
Auto Continue	Asset Nullide	-iCD				
Browser Clearable Warnings	I I I I I I I I I I I I I I I I I I I	cified)				
- Company Name	Auto Cleaning	n Page				
Contact Person			000	-		
Control Panel Display	Auto de	aning nequency. 12	000			
- Date and Time	Cleaning	g page size: L	etter (8.5x11 in)	-		
- Date/Time Format	Auto Continu					
- Daylight Savings Time				_		
Default Media Size	i o un					
- Default Print Density	C Off					
- Default Printer Copies	Browser					
- Device Certificates	Г					
Device Location	Con	nection timeout:	60 💌 se	conds		
- Device Name - Duplex Binding	Res	nonse timeout:	300 🔻 💏	conds		
- Duplex Blank Pages	nes	porise amedia.	1000 56	conda		
Dunley Impressions	Trus	ted sites:				

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 window. The title bar of that area will display: *OXPd Device Functions (Changes Pending - Click 'Apply' to continue)*.

Status Config Alerts Troubleshoot Grou	ups Reports Supplies Storage	e Solutions Capabilities Firmware				
D Apply Template D View History 👷 Customize D Refresh						
Apply Template More screen Language I/O Timeout to End Print J Input Auto Continue Input Auto Continue Input Auto Continue Input Auto Continue Job Hold Timeout Job Hold Timeout Job Storage Limit Key Press Sound Keyboard Layout Manually Feed Prompt Media Administration Order Supplies % Level Original Orientation Override A4/Letter OXPd Enabled PJL Configuration Print PDF Errors Print PDF Errors Print PDF Errors Print Wakeup Replace Supplies	Customize OXPd Device Functions (Ch ID	anges Pending - Click 'Apply' to co	ntinue)	Add Remove		
Resolution Resolution Enhancement Restore Modes						
Show Date and Time Show Network Address Size / Type Prompt						
				Save as Template	Schedule Apply	

11. Click the Add button. The Add OXPd Device Functions windows is displayed.

Status Config Alerts Troubleshoot Group	s Reports Supplies Sto	rage Solutions Capabilities Firmw	are		
Di Apply Template Di View History	Justomize 😥 Refresh				
Home Screen Language 🔺 🕵 🛛	DXPdDeviceFunctions ((Changes Pending - Click 'Apply' to	o continue)		
I/U Timeout to End Print J					
Input Auto Continue					
Input Auto Continue Time	ID	Title	Description	Add	
Jam Recovery				Bomouro	
Job Hold Timeout					
Job Retention	Add OXPd Device Fun	ctions		? ×	
- Job Storage Limit					
Key Press Sound					
Manually Ecod Promot	ID	Title	Description	Edit	
Madia Administration		1102			
Order Supplies % Level					
Original Orientation					
- Override A4/Letter					
- OXPd Accessory Records					
- 😥 OXPd Device Functio					
- 0XPd Enabled					
PJL Configuration					
Print PDF Errors					
- Print PS Errors					
- Printer Wakeup					
Replace Supplies			40	Cancel	
Resolution					
Resolution Enhancement					
- Restore Modes					
- Show Date and Time					
Show Network Address					
Sleep () (slee Time					
				Courses Trend 1	Colored Land
				bave as i emplate	Schedule Apply

 Click the Edit button. The OXPd Device Function Repository window is displayed and will enable you to import the edited HP OXPd solutions XML files (from <u>Exporting the XML files</u> on 58).



13. Click Import. In the Open window, search for your XML files.



- **14.** Select to highlight the file and then click **Open** to add the file. (You can import only one file at a time in the **Open** window.)
- **15.** Verify that the selected feature XML file is reflected in the **OXPd Device Function Repository** window.

4	Dptions				? ×
	Templates	► OXPd Devic	e Function Repositor	y	
Status Config Ale Status Config Ale Status Template. - Home Scre - I/O Timeou - Input Auto (- Input Auto (- Job Hold Ti - Job Retenti - Job Storage	Templates User Defined PJL Repository Certificate Repository OXPd Device Functio OXPd Accessory Rec Alerts Firmware Reports Supplies	OXPd Devic Name Fax Button	≥ Function Repositor	y Description Send a Fax	Edit
Keyboard L Manually Fe Media Admi Order Supp Order Supp Orginal Orie Override A4	Reset Page	<u></u>		ОК	Cancel Apply

16. Click OK. The Add OXPd Device Functions window is displayed.

Status Config Alerts Troubleshoot	Groups 📌 Cust	Reports Supplies Storage Soluti	ions Capabilities Firmwa	re		
Home Screen Language I/O Timeout to End Print J Input Auto Continue Input Auto Continue Time Jam Recovery Job Hold Timeout Lob Petertion	i i konstantin na senara	Pd Device Functions (Changes P	'ending - Click 'Apply' to	continue)	Add Remove	
	- A A	dd OXPd Device Functions			?×	
Override A4/Letter OXPd Accessory Records OXPd Device Functio OXPd Enabled PJL Configuration Print PDF Errors Print PS Errors Printer Wakeup Replace Supplies Resolution Resolution Enhancement		ID 23920c5c-f3dd-442f-a56f-0935deb	Title 09e Fax	Description Send a Fax	Edit	
Restore Modes Show Date and Time Show Network Address Size / Type Prompt Show (Micke Time				<u> </u>	Cancel Save as Template	Schedule Apply

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 window and return to the OXPd Device Functions window.

At this point, you can continue to add another feature or button (repeating Steps 11 through 16).
Status Config Alerts Troubleshoot Gro	roups Reports Supplies Storage Solutio	ons Capabilities Firmv	are			
🕼 Apply Template 🅼 View History 🖇	🕅 Customize 🔁 Refresh					
Apply Template Wiew History	Customize Refresh	ending - Click 'Apply'i	D continue)	Add Remove		
Size / Type Prompt						
				Save as Template	Schedule	Apply

18. After you have added and confirmed all of the desired features/buttons, click **Apply**. The **Confirm** page is displayed.

Configure Devices		1
onfirm		S
C-Wine-		
Settings Devices: 1		
Device settings:		
Item	Value	
🔌 OXPd Device Functions	0	
	< Back Configure Devices C	ancel
	Configure Devices	ancer

19. Click the Configure Devices button. The In Progress window is displayed.

rogress		Ş
A		
M Progress		
Summary		
Success:	0	
🔒 Warning:	0	
🖸 Error:	0	
i Information needed:	0	
Pending:	1	

The **Results** screen will then indicate if the installation was successful or if an error was received.

esults		
~		
Success		
Summary		
Success:	1	
🚹 Warning:	0	
3 Error:	0	
Information needed:	0	
Pending:	0	

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 window, which defaults to the Device subset node.

OZ (1 of 3 Selected)							
Layouts -	🍸 Filters 🔹 👔						
Device Model	IP Address	IP Hostname	Port (Any)	Severity	Hardware Address	 	
HP LaserJet M4345 MFP	172.16.5.208	NPI822592	1		001708822592		
HP Color Laser let 4730 MEP	172165130	NPI5BDA67	1	Â	0014385BDA67		
HP Color Lasor lat CMC040 MEP	172 16 5 117	NDI1CD 401	1		001070100401		
	172.10.3.117	In Incoron		1	001070100401		
C		la slav	face fa		1		
s Conrig Alerts I roubleshoot	Groups Heports	Supplies Storage	e Solutions Ca	apabilities Firm	ware		
pply Template 🕼 View History	Customize	. 🤁 Refresh					
My Settings 📃	Alternative Le	etterhead Mode					
Device							
-Alternative Letterhead Mo							
- Asset Number	• Off						
- Auto Cleaning Page	Assethlember						
- Auto Continue	AssetNumber						
Browser	Not spe	cified)					
Clearable Warnings							
- Company Name -	Auto Cleaning	Page					
Contact Person	L Avan ala		000				
- Control Panel Display	Auto cie	aning rrequency: 12	000	<u> </u>			
Control Panel Language	Cleaning	page size:	etter (8.5x11 in)	-			
- Date and Time	5000000			_			
- Date/Time Format	Auto Continue						
- Default Media Size	🗆 🔍 On						
- Default Media Type	C 04						
- Default Print Density	v un						
- Default Printer Copies	Browser						
- Device Certificates	F						
- Device Location	Cont	nection timeout:	60 × se	conds			
- Device Name	- Corn	in the second second					
Duplex Binding	Resp	oonse timeout:	300 💌 se	conds			
- Duplex Blank Pages			and the second				
- Duplex Impressions	Trus	ted sites:					
- Economode							
Fuser Modes							
- Home Screen Applications							
- Home Screen Language 🖕	1						
·		Use semio	colons(;) to separ	ate addresses			
	-						1 1
							Save as Template Schedule

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

Apply Template W View His OXPd Device Functions OXPd Enabled	tory 👷	Customize 🧭 Refresh		_			
 PIL Configuration Print PDF Errors Print PS Errors Print PS Errors Print PS Errors Replace Supplies Resolution Enhancement Resolution Enhancement Show Date and Time Show Network Address Size / Type Prompt Sleep / Wake Time Stored Job Sort Order Supplies Status Message. Supplies Status Message. Supplies Status Message. Supplies Status Message. Time Zone Tray Administration Use Another Tray Use Requested Tray Copier Network Security Fax Embedded Web Server File System Digital Sending 		ID 23920c5c+73dd-442f+a56f-0935deb09e 4cbfa532-6be8-4877-89f7-2tbfa836df2a	Title Fax Personal Distributions	Description Send a Fax Distribute document using	Add Remove		
					Save as Template	Schedule	Apply

22. Test the buttons on the device panel to insure all functionality.

Using HP's Web Jetadmin application to install OXPd v1.6 buttons on HP devices

6 Testing

The following section provides a procedure for testing the Routing Sheet feature. This will ensure that your installation is operational. For additional button testing procedures, refer to the <u>HP CR administrator on-line help</u>.

6-1 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:

OXPd Ren	note Control Panel	
	Sign In Ready	Copies: 1
	Routing Sheet	Personal Distributions
2	Distribute a document using a routing sheet	Distribute document using a personal distribution
	Public Distributions	Scan To Me
the second secon	Distribute document using a public distribution	Scan document to my desktop

- 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 the them now. Enter the appropriate prompt values and click **Next**. For information on configuring prompts, refer to the <u>HP CR administrator on-line help</u>.

The device indicates it is ready to scan.

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 <u>HP CR administrator on-line help</u>.

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 [6] 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 <u>HP CR administrator on-line help</u>.

6-2 Testing the Device Administrator user interface

To test the Device Administrator user interface, complete the procedure for <u>Creating a group of devices</u> (29). This applies to both Embedded Device Client for HP OXPd v1.4 and v1.6.

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

- Email
- PIN
- PIN with Password
- Login

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