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

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

Edition: September 2013

Legal notices

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.

Printed in the US

Revision history

Table 1 Revisions

Date	Edition	Revision
December 2012	2	Version 1.2.0
September 2013	3	Version 1.3.0

Contents

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:

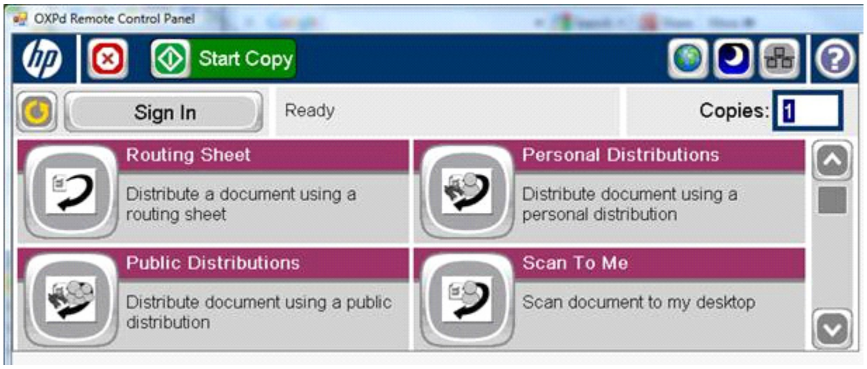
Procedures for installation, configuration, and testing are provided in the remainder of this document.

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



Ready

Copies: 1

Routing Sheet
Distribute a document using a routing sheet

Personal Distributions
Distribute document using a personal distribution

Public Distributions
Distribute document using a public distribution

Scan To Me
Scan document to my desktop

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

Table 1 HP CR scanning features in the HP CR Embedded Device Client

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 Basic requirements (7) and the HP Capture and Route (HP CR) User Guide.
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 a folder (Dropbox, 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.	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	

Feature	Description	Login Required	Notes
Fax Release	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).	Yes	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.
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.
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.).	Yes	Login is required only if using Device Authentication and If one of the Nested Buttons needs authentication.
Mobile Reservations	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.	No	Mobile Reservations are generated by the Mobile Client and require a Mobile Client license.

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 (11).
- **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

Component	Location	Function
HP CR Embedded Device Client Install	`\HP\HPCR\Clients`	The setup contains the `setup.exe` file for HP OXPd Device Client. Use this file to install the HP CR Embedded Device Client.
HP CR Embedded Device Client 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.

1-1-3 Document workflow

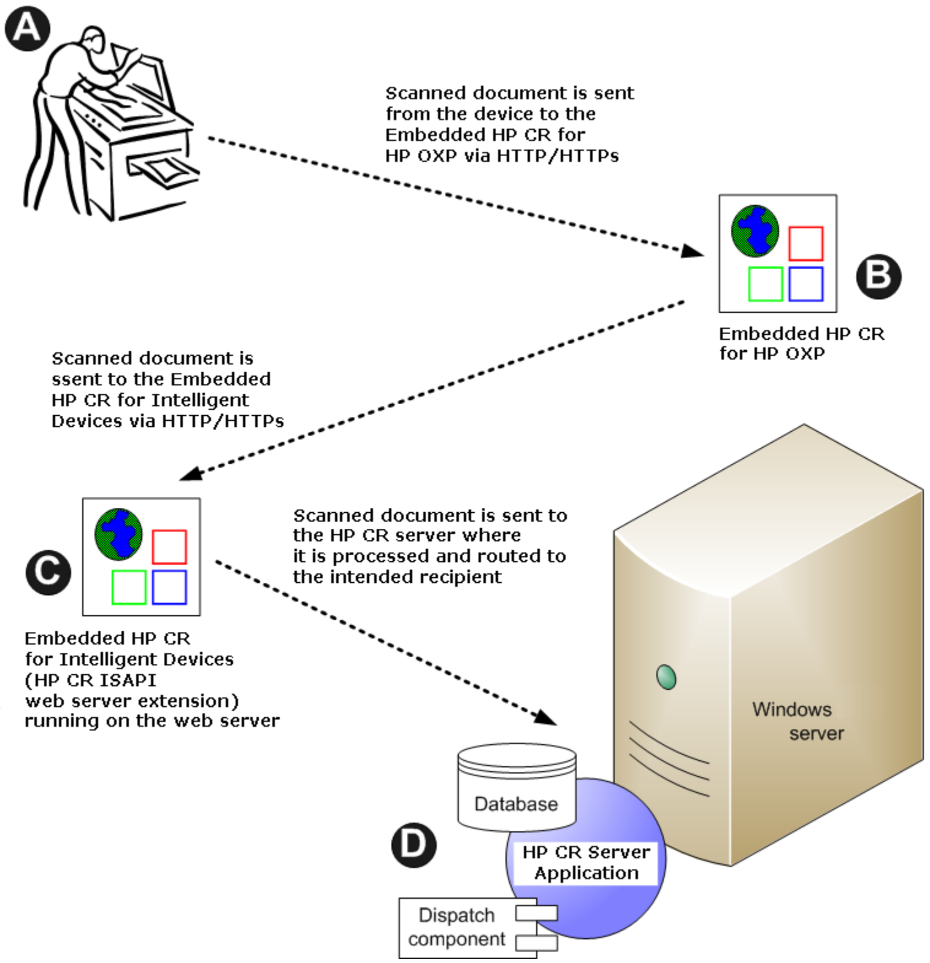
The workflow that moves a document from the device to its final destination involves the user, the device, the HP CR Embedded Device Client, Embedded HP CR for Intelligent Devices (HP CR ISAPI web server extension), and the HP CR server. An understanding of this workflow can be helpful in troubleshooting 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
Scanned document is sent from the device to the Embedded HP CR for HP OXP via HTTP/HTTPs
B
Embedded HP CR for HP OXP
Scanned document is ssent to the Embedded HP CR for Intelligent Devices via HTTP/HTTPs
C
Embedded HP CR for Intelligent Devices (HP CR ISAPI web server extension) running on the web server
Scanned document is sent to the HP CR server where it is processed and routed to the intended recipient
Windows server
Database
D
HP CR Server Application
Dispatch component

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.

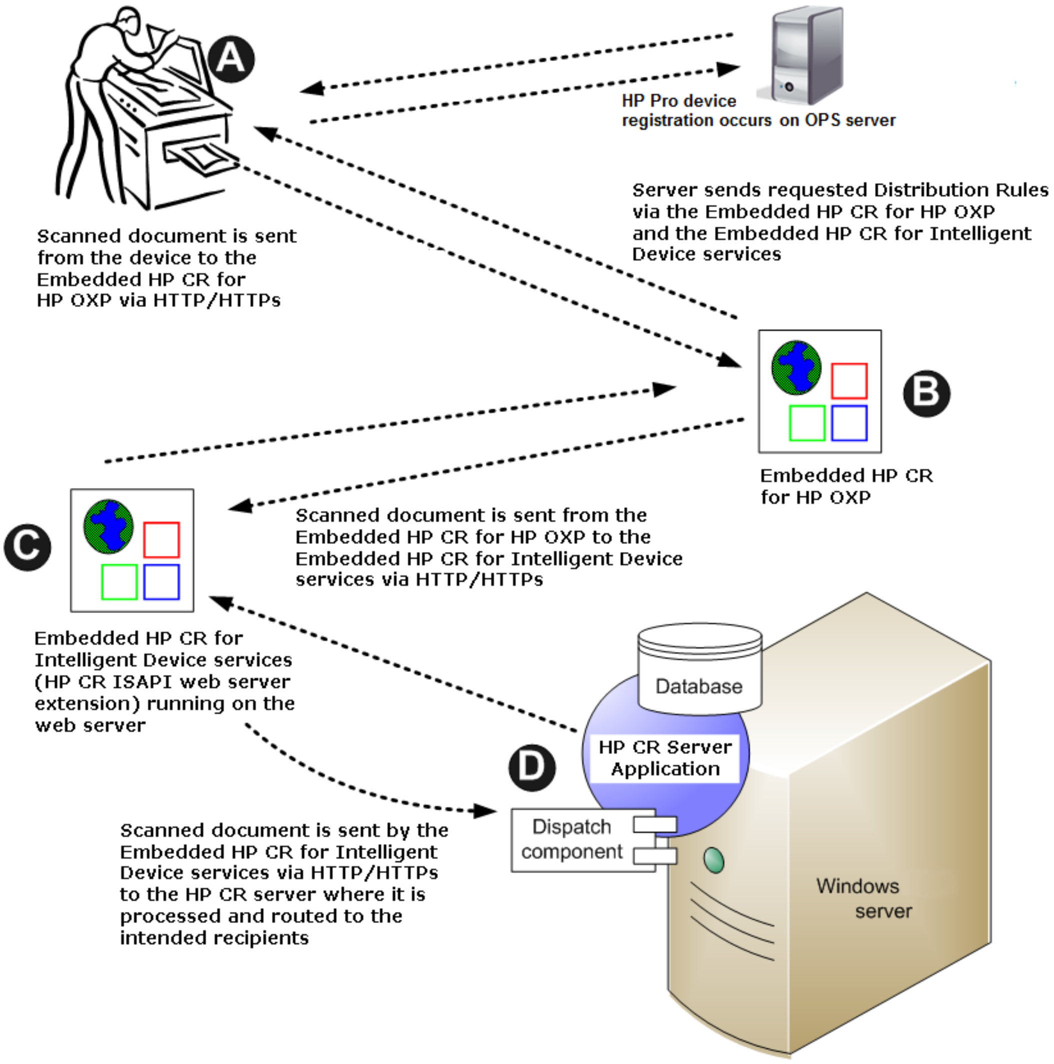
D-The Dispatch component applies rules to the message, and the server processes the message accordingly.

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
HP Pro device registration occurs on OPS server
Server sends requested Distribution Rules via the Embedded HP CR for HP OXP and the Embedded HP CR for Intelligent Device services
Scanned document is sent from the device to the Embedded HP CR for HP OXP via HTTP/HTTPs
B
Embedded HP CR for HP OXP
C
Scanned document is sent from the Embedded HP CR for HP OXP to the Embedded HP CR for Intelligent Device services via HTTP/HTTPs
Embedded HP CR for Intelligent Device services (HP CR ISAPI web server extension) running on the web server
Database
HP CR Server Application
D
Dispatch component
Windows server
Scanned document is sent by the Embedded HP CR for Intelligent Device services via HTTP/HTTPs to the HP CR server where it is processed and routed to the intended recipients

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, 8)

NOTE: If you are planning to use HTTPS protocol, you must create a CA certificate before installing the HP CR Embedded Device Client. For instructions, refer to the description of setting up a CA certificate using Microsoft Certificate Services and enabling SSL in Section 6: Required Configuration (39).

2. Install the HP CR Embedded Device Client. See Installing the HP CR Embedded Device Client (11).

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 8: Testing (79).
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

Device	Group	Supported Firmware	Minimum Installed RAM	OXPd Version
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	48.283.4	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 4730 MFP	20	50.221.3	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	2201057_231923	N/A	1.6.3.2
ScanJet 7000n	XX	2131311_192131	N/A	1.6.3.2
ScanJet 8500	XX	2300293_377163	N/A	1.6.3.2
LaserJet Flow M525 MXP	XX	2201074_229181	N/A	1.6.3.2a
LaserJet Flow M575 MXP	XX	2200893_229649	N/A	1.6.3.2
LaserJet M775 MFP	XX	2201057_231933	N/A	1.6.3.2
LaserJet M4555 MFP	XX	2200887_229566	N/A	1.6.3.2

Device	Group	Supported Firmware	Minimum Installed RAM	OXPd Version
HP Color LaserJet flow MFP M830	XX	2301122_395323	N/A	1.6.3.2
HP Color LaserJet flow MFP M880	XX	2301122_395321	N/A	1.6.3.2
HP LaserJet MFP M725	XX	2300312_393688	N/A	1.6.3.2
HP Officejet Pro 276dw MFP	XX	FRP1CN1336BR	N/A	1.6.3.2
HP Officejet Pro x476dn MFP	XX	LNP1CA1336CR	N/A	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 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

The HP CR Embedded Device Client requires:

- HP CR Server with appropriate device license
- 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 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

To support large color documents, an IIS setting (**Request Filtering**) must be set to the maximum 4294967295. The content length must be modified on the WebAPI site. To increase content length in IIS:

1. Open Internet Information Services (IIS 7) Manager.
2. Select **WebAPI** under **Sites**.
3. Double-click on **Request Filtering**.
4. Select **Edit Feature Settings** under the **Actions** menu.
5. Increase the value in **Maximum allowed content length**. The default is 30000000 and it must be increased to **4294967295**.
6. Reset 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 (only) (19) for more information.

1-3-1 Configuring to use HTTPS (not supported for HP Pro devices)

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 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 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 onto the device.
Also note, if you are using HP Pro devices, the makecert certificates are not supported.

For information on how to create a self-signed certificate using makecert.exe, refer to the description of Creating the certificate (14).

1-3-2 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 Creating a group of devices (part 1) (39).

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 HP CR Embedded Device Client Installation

This section describes:

Installing the HP CR Embedded Device Client (11)

Installing the HP CR Embedded Device Client on a remote system (12)

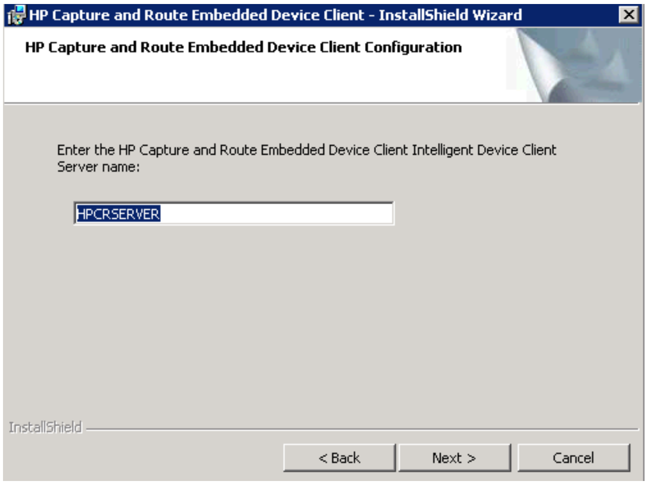
See also Section 6: Required Configuration (39), Section 8: Testing (79), and the HP CR administrator on-line help (for additional information including optional configurations, testing, and troubleshooting).

2-1 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 for OXP Configuration** page opens.



HP Capture and Route Embedded Device Client - InstallShield Wizard

HP Capture and Route Embedded Device Client Configuration

Enter the HP Capture and Route Embedded Device Client Intelligent Device Client Server name:

HPCRSERVER

5. In the **HP Capture and Route for OXP 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 6: Required Configuration (39).

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

1. Log on to the system where you want to install the HP CR Embedded Device Client using an account that belongs to the local Administrators group.

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

2. Navigate to the `\\HP\HPCR\Clients\DeviceClient` directory and run `setup.exe`.

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

3 Configuring FutureSmart and Oz Devices (only)

This section describes the configuration process for FutureSmart and OZ devices only. The configuration consists of 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 6: Required Configuration (39).

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.

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

NOTE: The CA Certificate steps in this section are not supported for HP Pro devices.

3-1 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)

Adding the OPS server certificate to the Client certificate 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.

3-2 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 Microsoft documentation.

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

3-3 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 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.

3-4 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 appears.

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.

3-5 Adding the OPS server certificate to the Client certificate directory

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\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**.

3-6 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.

3-7 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**.

3-8 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.

3-9 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**.

3-10 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)**.

3-11 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.

3-12 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. Save the file.
4. Reset IIS.

4 Configuring HP Pro Devices (only)

This section describes the installation and configuration process for local HP Pro devices only.

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.

The OPS Server installation process includes the following steps:

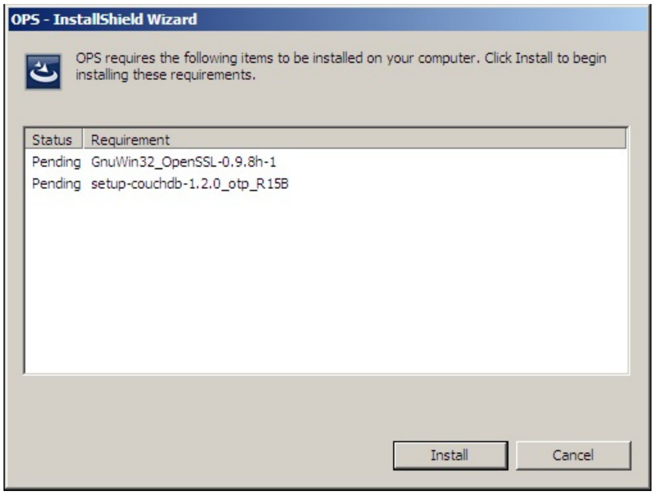
4-1 Installing the HP CR Embedded Device Client on the server

On the system running the HP CR server, install the HP CR Embedded Device Client. See HP CR Embedded Device Client Installation (11) for more information.

4-2 Installing the OPS kit on the 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`



OPS - InstallShield Wizard

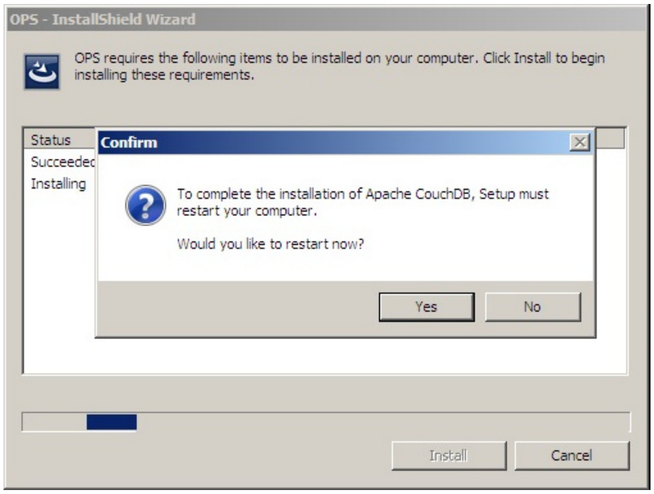
OPS requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	GnuWin32_OpenSSL-0.9.8h-1
Pending	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?



OPS - InstallShield Wizard

OPS requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status
Succeeded
Installing

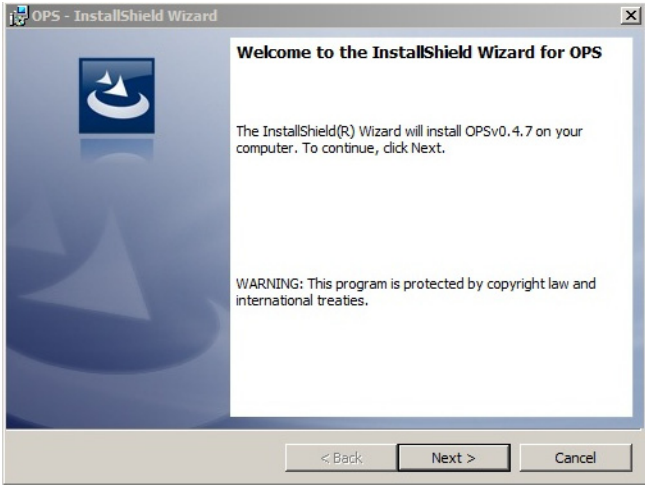
Confirm

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.

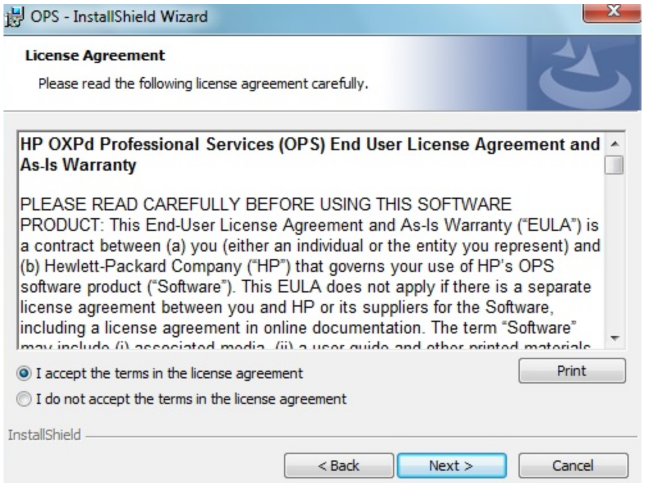


Welcome to the InstallShield Wizard for OPS

The InstallShield(R) Wizard will install OPSv0.4.7 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



License Agreement

Please read the following license agreement carefully.

HP OXPd Professional Services (OPS) End User License Agreement and As-Is Warranty

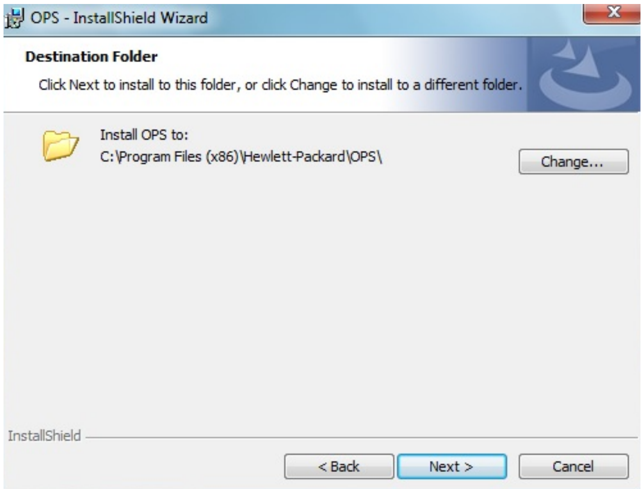
PLEASE READ CAREFULLY BEFORE USING THIS SOFTWARE PRODUCT: This End-User License Agreement and As-Is Warranty ("EULA") is a contract between (a) you (either an individual or the entity you represent) and (b) Hewlett-Packard Company ("HP") that governs your use of HP's OPS software product ("Software"). This EULA does not apply if there is a separate license agreement between you and HP or its suppliers for the Software, including a license agreement in online documentation. The term "Software" may include (i) associated media, (ii) a user guide and other printed materials

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

8. Select **I accept the terms in the license agreement** and click **Next**.

   The **Destination Folder** screen appears.

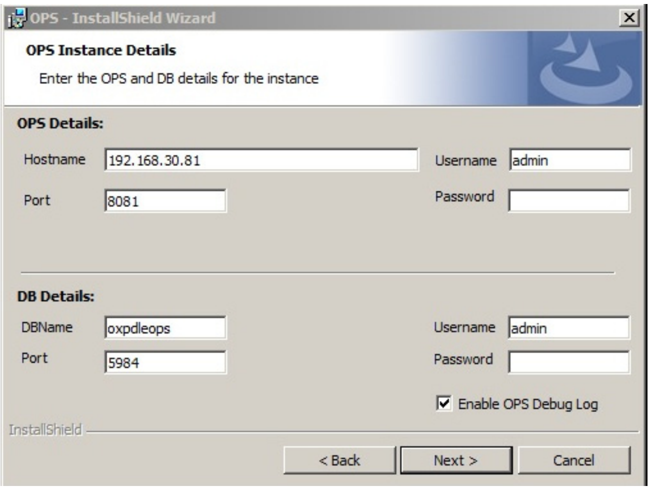


Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install OPS to:
C:\Program Files (x86)\Hewlett-Packard\OPS\

9. Click **Next**. The **OPS Instance Details** screen appears.



OPS - InstallShield Wizard

OPS Instance Details

Enter the OPS and DB details for the instance

OPS Details:

Hostname: 192.168.30.81

Username: admin

Port: 8081

Password:

DB Details:

DBName: oxpdleops

Username: admin

Port: 5984

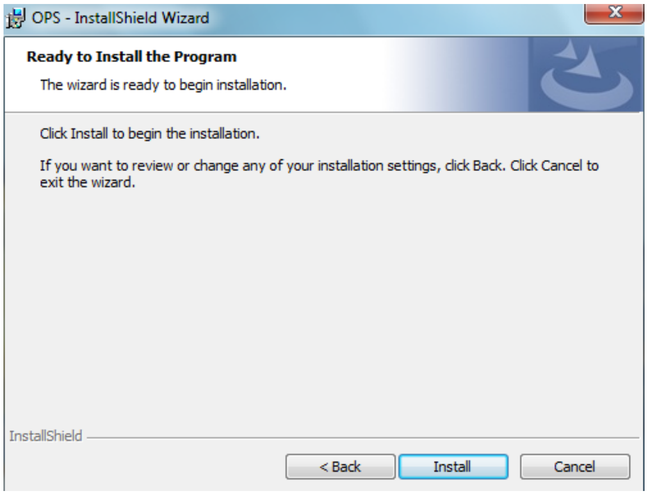
Password:

☑ Enable OPS Debug Log

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.



OPS - InstallShield Wizard

Ready to Install the Program

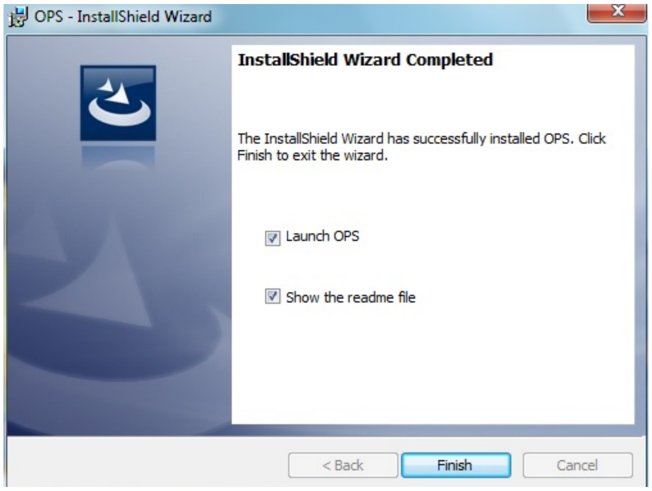
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

13. Click **Install**.

14. The **OPS InstallShield Wizard Completed** screen appears.



OPS - InstallShield Wizard

InstallShield Wizard Completed

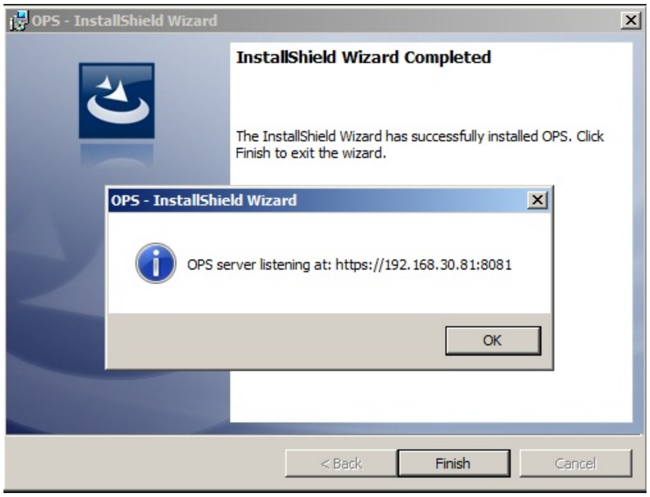
The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.

☑ Launch OPS

☑ Show the readme file

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 - InstallShield Wizard

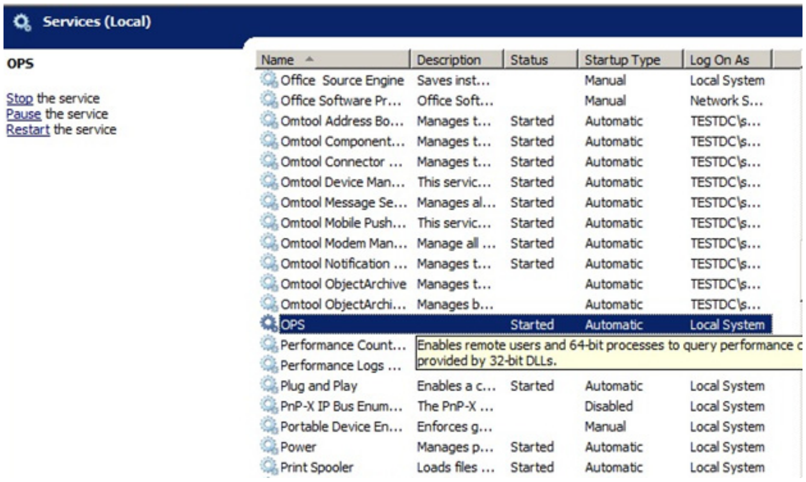
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.

OPS - InstallShield Wizard

OPS server listening at: https://192.168.30.81:8081

Click **OK**. OPS now appears as a Windows service.



Services (Local)

OPS

Stop the service
Pause the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Office Source Engine	Saves inst...		Manual	Local System
Office Software Pr...	Office Soft...		Manual	Network S...
Omtool Address Bo...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Component...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Connector ...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Device Man...	This servic...	Started	Automatic	TESTDC\s...
Omtool Message Se...	Manages al...	Started	Automatic	TESTDC\s...
Omtool Mobile Push...	This servic...	Started	Automatic	TESTDC\s...
Omtool Modem Man...	Manage all ...	Started	Automatic	TESTDC\s...
Omtool Notification ...	Manages t...	Started	Automatic	TESTDC\s...
Omtool ObjectArchive	Manages t...		Automatic	TESTDC\s...
Omtool ObjectArchi...	Manages b...		Automatic	TESTDC\s...
OPS		Started	Automatic	Local System
Performance Count...				
Performance Logs ...				
Plug and Play	Enables a c...	Started	Automatic	Local System
PnP-X IP Bus Enum...	The PnP-X ...		Disabled	Local System
Portable Device En...	Enforces g...		Manual	Local System
Power	Manages p...	Started	Automatic	Local System
Print Spooler	Loads files ...	Started	Automatic	Local System

Enables remote users and 64-bit processes to query performance c
provided by 32-bit DLLs.

4-3 Adding 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**.
6. The **Certificate Export** wizard appears. Select **Next**.
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`.
10. Select **Next** and then click **Finish**.

4-4 Importing the OPS certificate into the device EWS

1. Open and log into the EWS of the Pro Device.
2. On the **Network** tab select **Advanced settings > Certificates**.
3. Select **Import > Choose File**.
4. Browse to the location where the OPS certificate was saved and select **Open** and then **Finish**.

4-5 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 kit on the server (19).
5. Enter the **OPS server URL** you want to register. 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 kit on the server (19).

7. The following message appears:

```
OPS Registered successfully
```

Your local OPS server is now installed. See Creating a group of devices (part 1) (39) for more information on creating device groups.

4-6 HTTPS support using the OPS-created certificate

4-6-1 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.

4-6-2 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**.

4-6-3 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.

4-6-4 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**.

4-6-5 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/`
12. Select **Continue to this website (not recommended)**.

4-6-6 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 kit on the server.

NOTE: XML files can be edited using Microsoft Notepad.

3. Save the file.

4-6-7 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 kit on the server.

3. Save the file and reset IIS.

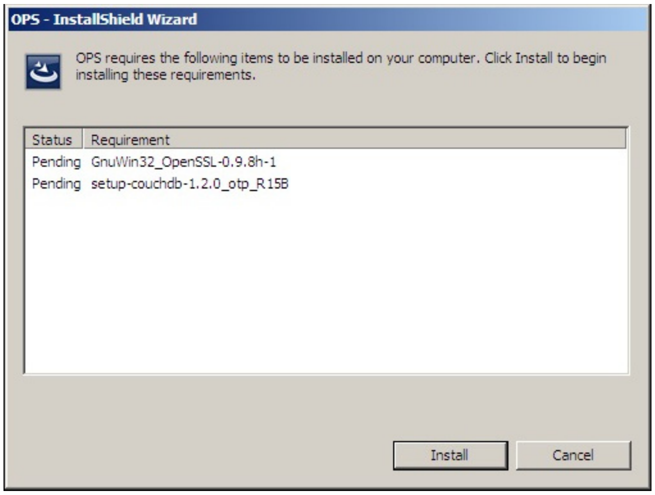
5 Configuring Mixed Devices in the Same Environment (HP Pro, FutureSmart and OZ)

This section describes the installation and configuration process for a mixed environment of HP Pro, FutureSmart and OZ devices with HTTPS support. This scenario uses the OPS-created certificate for HTTPS communication between all three types of devices and the server.

5-1 Installing the OPS kit on the 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`



OPS - InstallShield Wizard

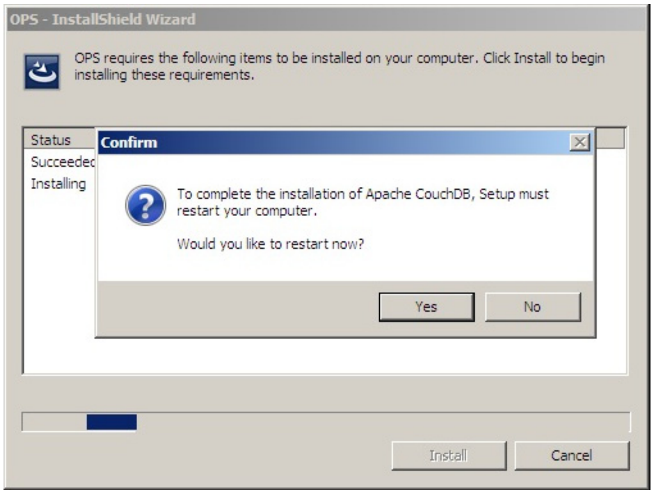
OPS requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	GnuWin32_OpenSSL-0.9.8h-1
Pending	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?



OPS - InstallShield Wizard

OPS requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status
Succeedec
Installing

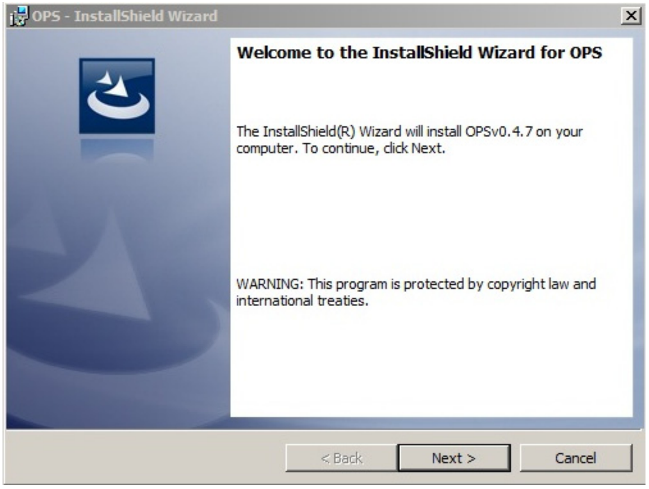
Confirm

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.



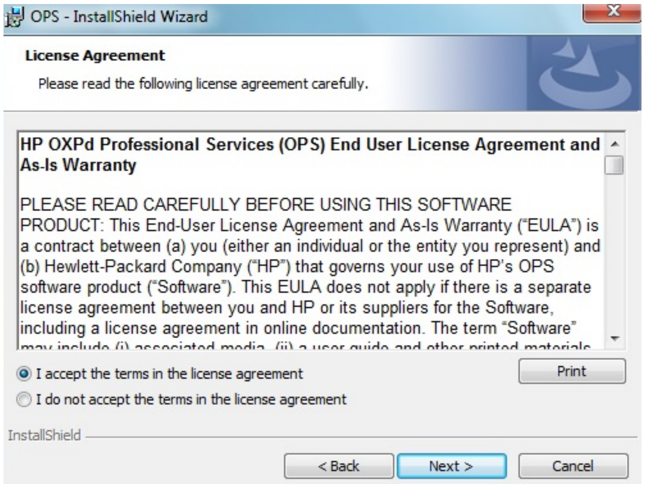
OPS - InstallShield Wizard

Welcome to the InstallShield Wizard for OPS

The InstallShield(R) Wizard will install OPSv0.4.7 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



OPS - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

HP OXPd Professional Services (OPS) End User License Agreement and As-Is Warranty

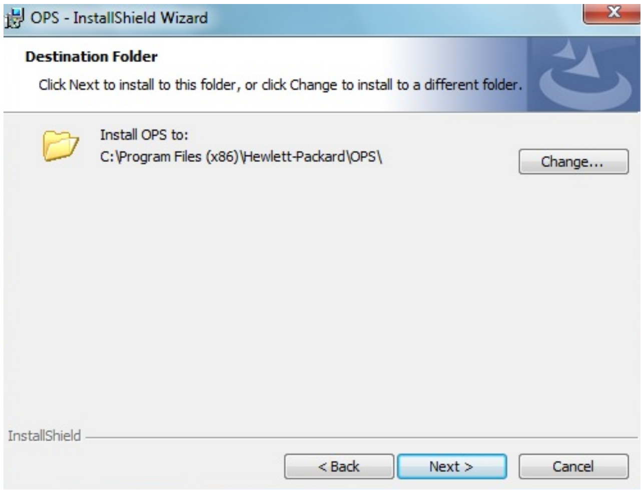
PLEASE READ CAREFULLY BEFORE USING THIS SOFTWARE PRODUCT: This End-User License Agreement and As-Is Warranty ("EULA") is a contract between (a) you (either an individual or the entity you represent) and (b) Hewlett-Packard Company ("HP") that governs your use of HP's OPS software product ("Software"). This EULA does not apply if there is a separate license agreement between you and HP or its suppliers for the Software, including a license agreement in online documentation. The term "Software" may include (i) associated media, (ii) a user guide and other printed materials

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

8. Select **I accept the terms in the license agreement** and click **Next**.

The **Destination Folder** screen appears.



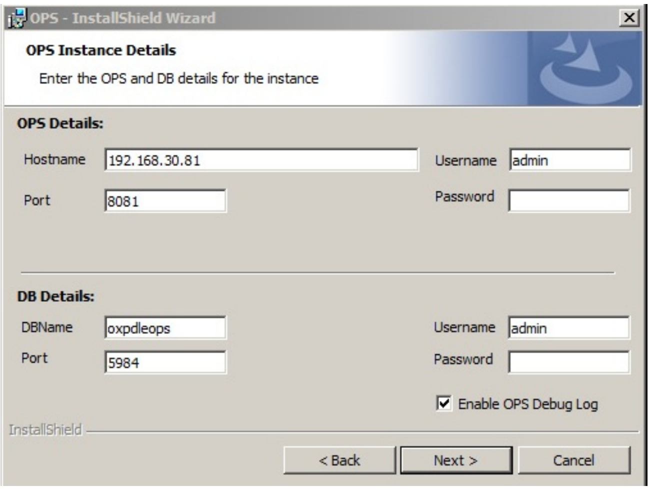
OPS - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install OPS to:
C:\Program Files (x86)\Hewlett-Packard\OPS\

9. Click **Next**. The **OPS Instance Details** screen appears.



OPS - InstallShield Wizard

OPS Instance Details

Enter the OPS and DB details for the instance

OPS Details:

Hostname: 192.168.30.81

Port: 8081

Username: admin

Password:

DB Details:

DBName: oxpdleops

Port: 5984

Username: admin

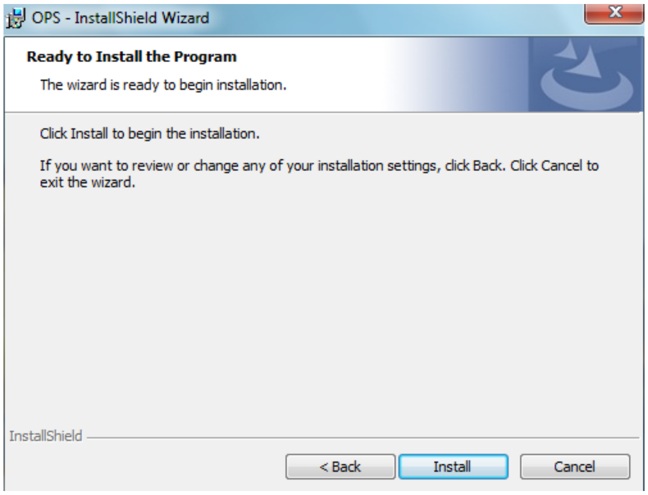
Password:

☑ Enable OPS Debug Log

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.



OPS - InstallShield Wizard

Ready to Install the Program

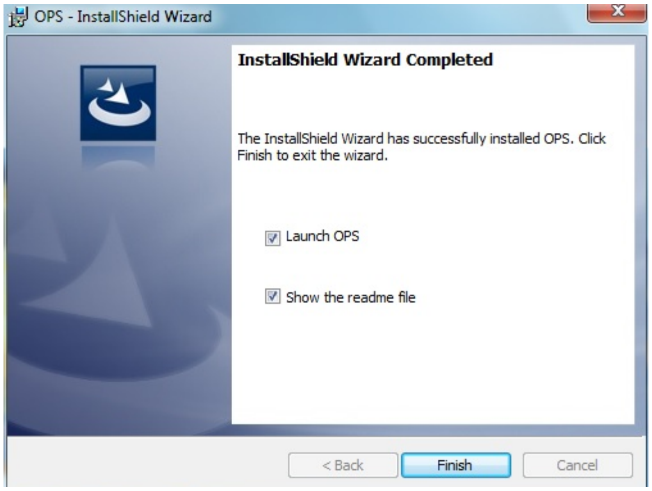
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

13. Click **Install**.

14. The **OPS InstallShield Wizard Completed** screen appears.



OPS - InstallShield Wizard

InstallShield Wizard Completed

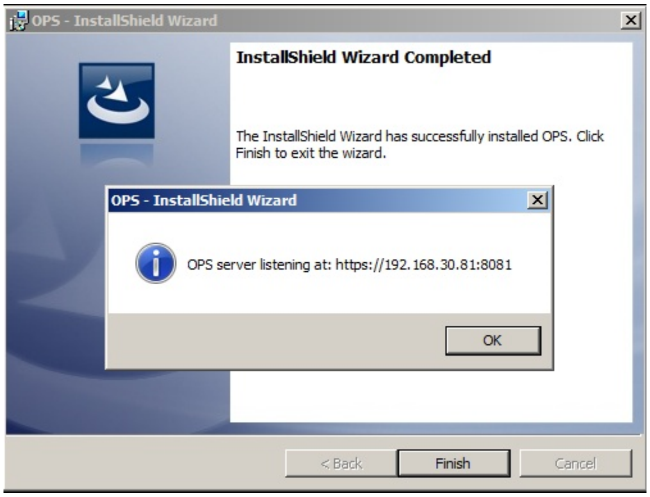
The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.

☑ Launch OPS

☑ Show the readme file

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 - InstallShield Wizard

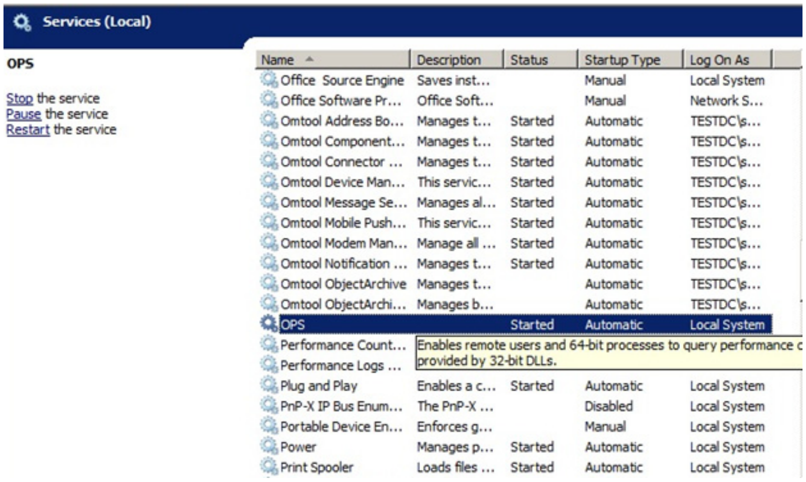
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.

OPS - InstallShield Wizard

OPS server listening at: https://192.168.30.81:8081

Click **OK**. OPS now appears as a Windows service.



Services (Local)

OPS

Stop the service
Pause the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Office Source Engine	Saves inst...		Manual	Local System
Office Software Pr...	Office Soft...		Manual	Network S...
Omtool Address Bo...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Component...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Connector ...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Device Man...	This servic...	Started	Automatic	TESTDC\s...
Omtool Message Se...	Manages al...	Started	Automatic	TESTDC\s...
Omtool Mobile Push...	This servic...	Started	Automatic	TESTDC\s...
Omtool Modem Man...	Manage all ...	Started	Automatic	TESTDC\s...
Omtool Notification ...	Manages t...	Started	Automatic	TESTDC\s...
Omtool ObjectArchive	Manages t...		Automatic	TESTDC\s...
Omtool ObjectArchi...	Manages b...		Automatic	TESTDC\s...
OPS		Started	Automatic	Local System
Performance Count...				
Performance Logs ...				
Plug and Play	Enables a c...	Started	Automatic	Local System
PnP-X IP Bus Enum...	The PnP-X ...		Disabled	Local System
Portable Device En...	Enforces g...		Manual	Local System
Power	Manages p...	Started	Automatic	Local System
Print Spooler	Loads files ...	Started	Automatic	Local System

Enables remote users and 64-bit processes to query performance c provided by 32-bit DLLs.

5-2 Exporting the OPS server certificate from the Trusted Root Certificate Authorities store for HP Pro devices

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**.
6. The **Certificate Export** wizard appears. Select **Next**.
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`.
10. Select **Next** and then click **Finish**.

5-3 Exporting the certificate to the Embedded Device Client directory for FutureSmart and OZ devices

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.

5-4 Importing the OPS certificate into the device EWS

1. Open and log into the EWS of the Pro Device.
2. On the **Network** tab select **Advanced settings > Certificates**.
3. Select **Import > Choose File**.
4. Browse to the location where the OPS certificate was saved and select **Open** and then **Finish**.

5-5 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 kit on the server (29).
5. Enter the **OPS server URL** you want to register. 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 kit on the server (29).

7. The following message appears:

   ```
   OPS Registered successfully
   ```

Your local OPS server is now installed. See Creating a group of devices (part 1) (39) for more information on creating device groups.

5-6 HTTPS support for HP Pro devices

NOTE: When using a remote OPS server, to use the OPS-created certificate for an HTTPS environment, make sure the OPS server is installed *on* the remote system.

5-6-1 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.

5-6-2 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**.

5-6-3 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.

5-6-4 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**.

5-6-5 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/`
12. Select **Continue to this website (not recommended)**.

5-6-6 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://OPS Servername or IP/WebAPI/FileTransfer/
   </FileTransfer>
   ```

   This OPS Servername is based on the value from Step 10 of Installing the OPS kit on the server.

NOTE: XML files can be edited using Microsoft Notepad.

3. Save the file.

5-6-7 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 kit on the server.

3. Save the file.
4. Reset IIS.

6 Required Configuration

This section describes:

See also Section 8: Testing (79) and the HP CR administrator on-line help (for additional information including optional configurations, testing, and troubleshooting).

6-1 Adding devices using the HP CR Server Administrator

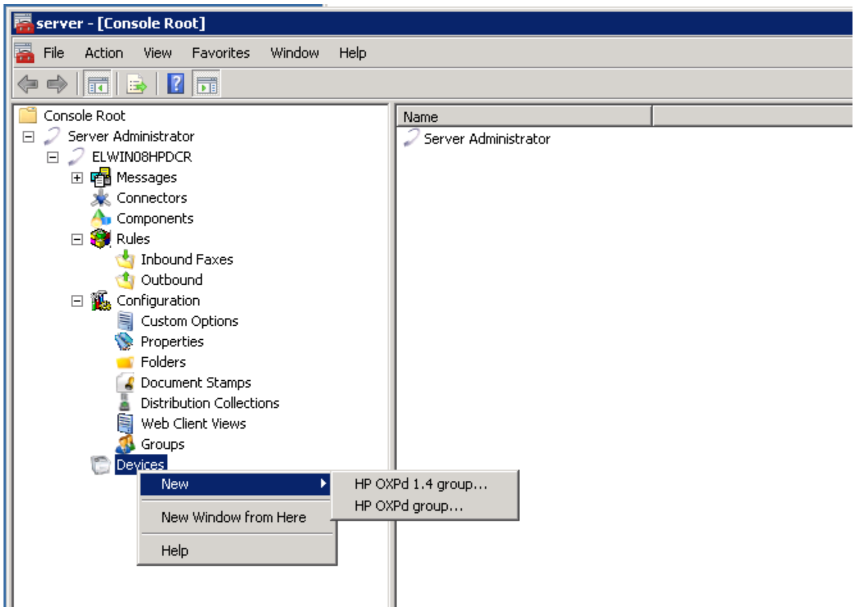
This section describes the procedures for:

6-1-1 Creating a group of devices (part 1)

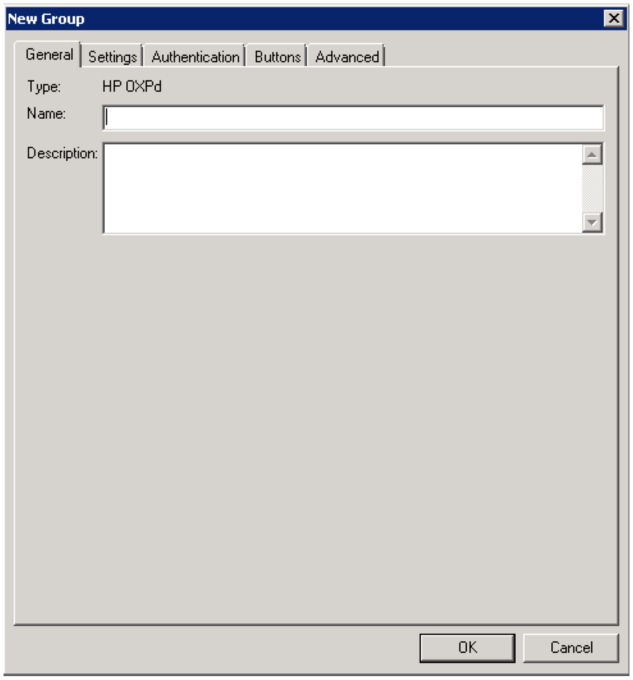
Create a new Group for each group of devices. While each group may have the same configuration, you can configure a group to have a configuration that is completely different from another group. For example, you might create a group named “Marketing” and configure it to use only the Routing Sheets and 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 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**.



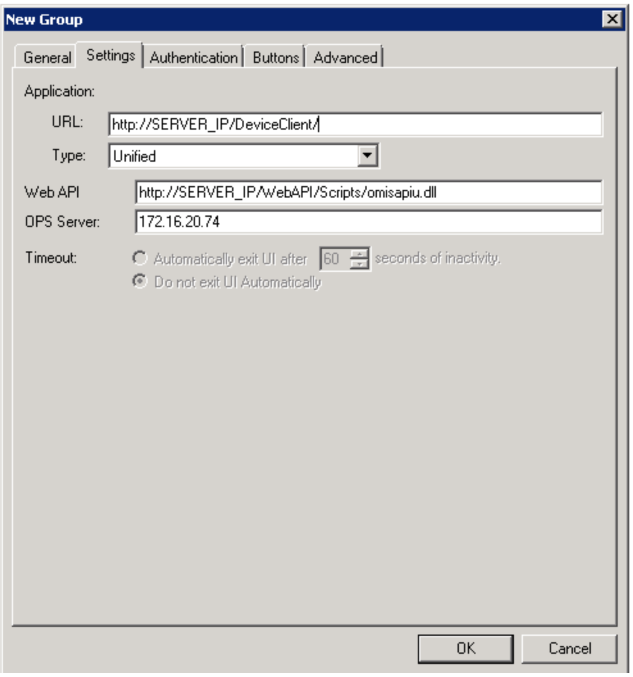
The **New Group** page opens.



Type: HP OXPd

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.



Application:

URL: http://SERVER_IP/DeviceClient/

Type: Unified

Web API http://SERVER_IP/WebAPI/Scripts/omisapiu.dll

OPS Server: 172.16.20.74

Timeout: ○ Automatically exit UI after 60 seconds of inactivity.
● Do not exit UI Automatically

- If you are configuring for HTTPS, change 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 (41) through to Editing the OmISAPIU.xml file (43).

Otherwise, continue these steps below at Creating a group of devices (part 2) (43).

IMPORTANT: The following sub-sections are for users with a local OPS server and an OPS-created certificate for HTTPS environments.

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.

Requiring SSL for the virtual web sites

1. Open the IIS Manager.
2. Expand **Local Machine > Default Web Site** and select **OXP DeviceClient**.
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**.

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.

Enabling directory browsing in IIS

1. Open the IIS Manager.
2. Expand **Local Machine > Default Web Site** and select **OXP1.6**.
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**.

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)**.

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`.

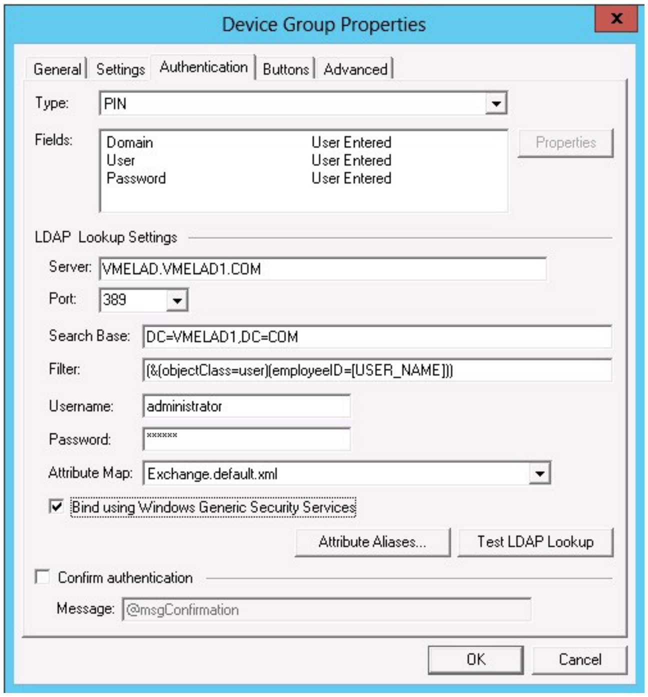
   ```
   <FileTransfer>https://fully_qualified_domain_name/WebAPI/FileTransfer/
   </FileTransfer>
   ```

NOTE: XML files can be edited using Microsoft Notepad.

3. Save the file and continue with Creating a group of devices (part 2) below.

6-1-2 Creating a group of devices (part 2)

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



Device Group Properties

Type: PIN

Fields:

Domain	User Entered
User	User Entered
Password	User Entered

LDAP Lookup Settings

Server: VMELAD.VMELAD1.COM

Port: 389

Search Base: DC=VMELAD1,DC=COM

Filter: (&(objectClass=user)(employeeID=[USER_NAME]))

Username: administrator

Password: ******

Attribute Map: Exchange.default.xml

☑ Bind using Windows Generic Security Services

□ Confirm authentication

Message: @msgConfirmation

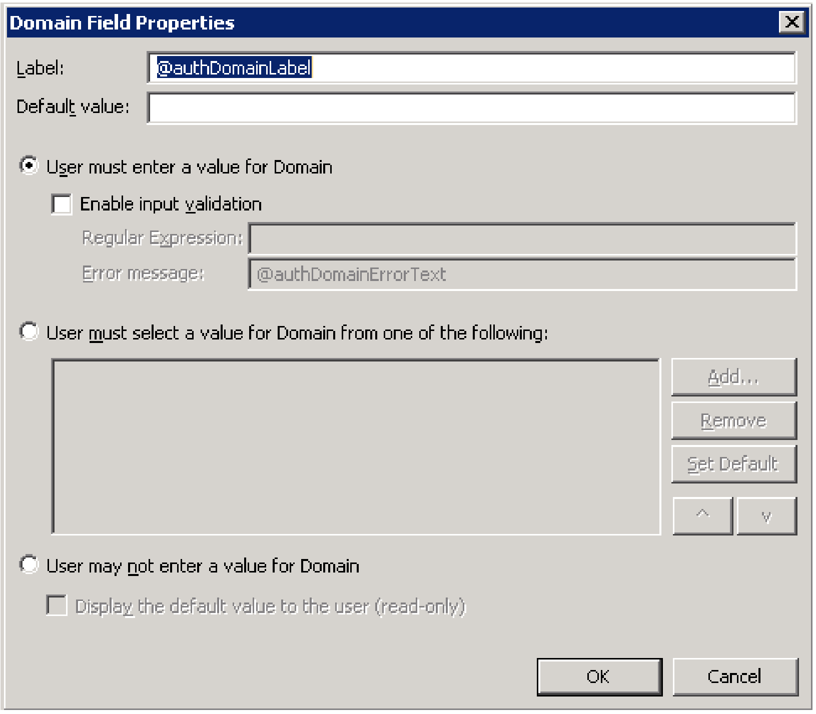
2. From the **Type** drop-down, select one of the three authentication options: **Email**, **Login**, or **PIN**.

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

   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 Properties

Label: @authDomainLabel

Default value:

● User must enter a value for Domain

□ Enable input validation

Regular Expression:

Error message: @authDomainErrorText

○ User must select a value for Domain from one of the following:

○ User may not enter a value for Domain

□ Display the default value to the user (read-only)

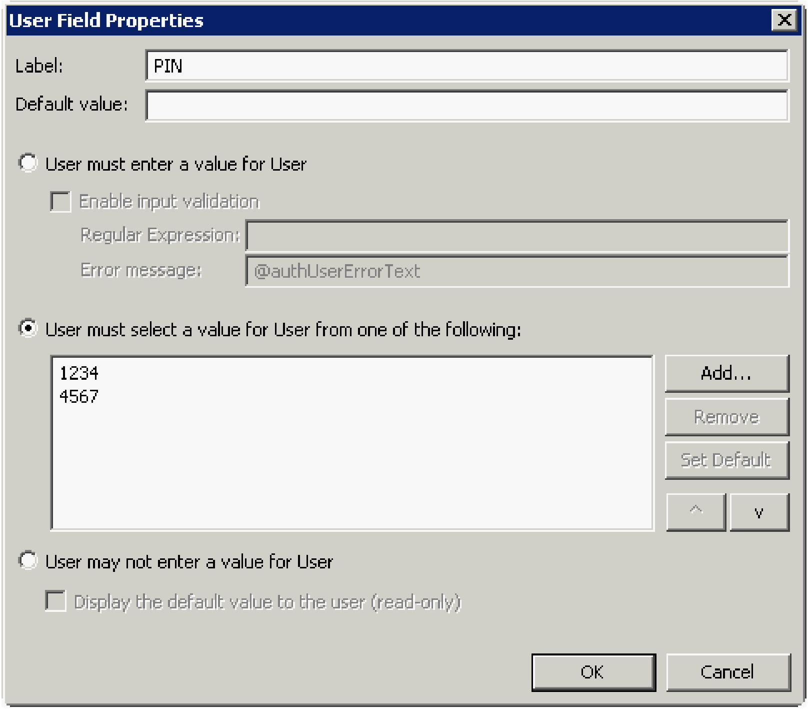
When you define a domain, you can specify a **Default value** (domain) that will be displayed at the device. In addition, you can specify one of the following:

- **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 Properties

Label: PIN

Default value:

○ User must enter a value for User

□ Enable input validation

Regular Expression:

Error message: @authUserErrorText

● User must select a value for User from one of the following:

1234
4567

○ User may not enter a value for User

□ Display the default value to the user (read-only)

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:

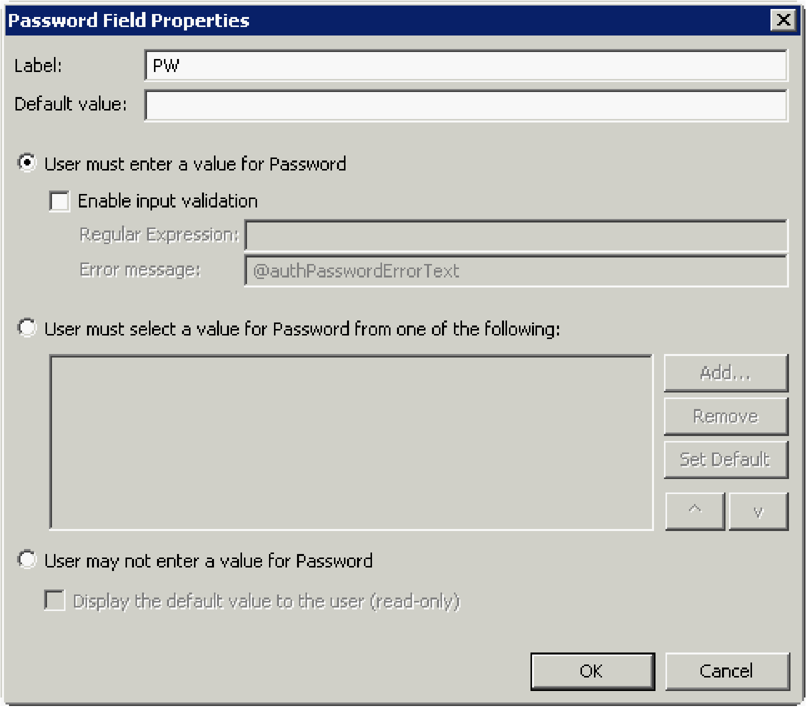
- **User must enter a value for User** - The device user will need to enter a user for authentication during login at the device.
- **User must select a value for User from one of the following** - If there are multiple users in the environment, use this option to create a list from which the user can 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 enter a value for Password

□ Enable input validation

Regular Expression:

Error message: @authPasswordErrorText

○ User must select a value for Password from one of the following:

○ User may not enter a value for Password

□ Display the default value to the user (read-only)

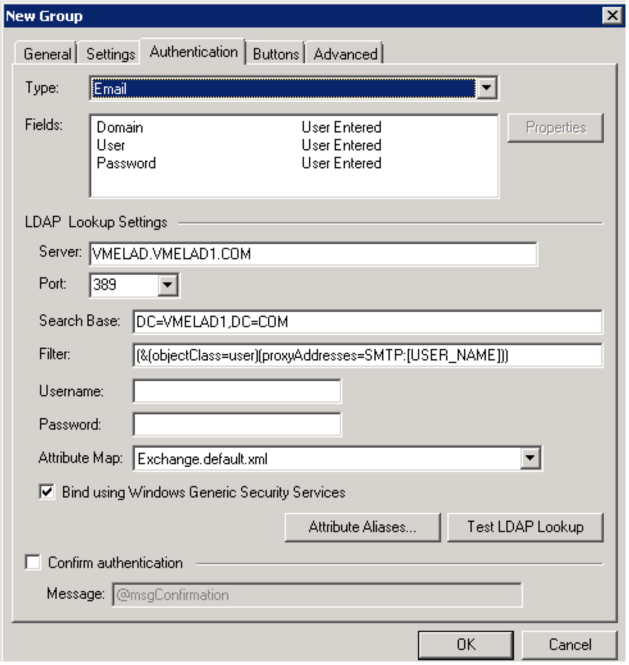
When you define a password, you can specify a **Default value** (password) that will be displayed at the device. In addition, you can specify one of the following:

- **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.

3. After you define **Domain**, **User**, and/or **Password** properties, click **OK** to return to the **Device Group Properties** page. For example



New Group

Type: Email

Fields:

Domain	User Entered
User	User Entered
Password	User Entered

LDAP Lookup Settings

Server: VMELAD.VMELAD1.COM

Port: 389

Search Base: DC=VMELAD1,DC=COM

Filter: (&(objectClass=user)(proxyAddresses=SMTP:[USER_NAME]))

Username:

Password:

Attribute Map: Exchange.default.xml

☑ Bind using Windows Generic Security Services

□ Confirm authentication

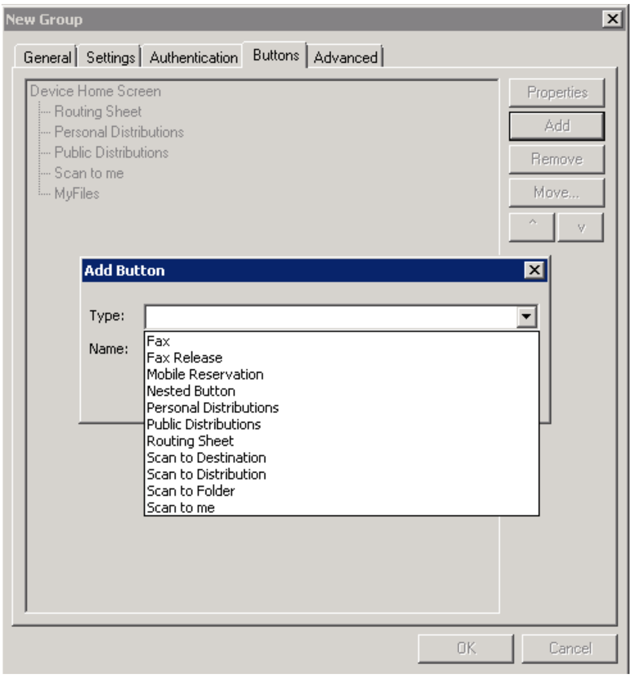
Message: @msgConfirmation

4. In the **Username** text box, enter the name of a Windows user who has permissions to query the active directory.

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

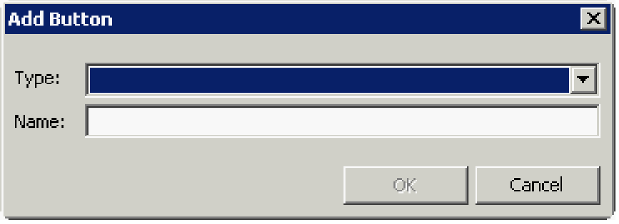
6. Select the **Confirm authentication** option if you want to display a prompt on the device to verify the user's information when authenticating.

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



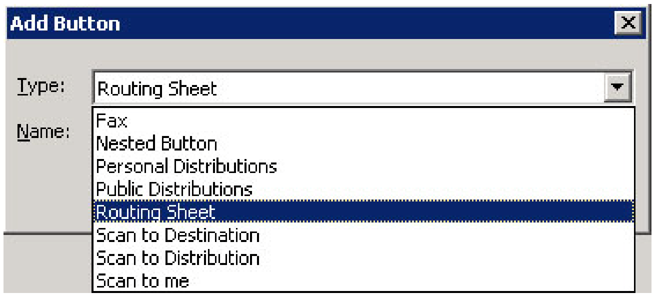
NOTE: It is best to add or remove buttons before installing to the device. Otherwise, if buttons are added or removed, or if button text is modified, it will be necessary to uninstall and run the installation again.

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



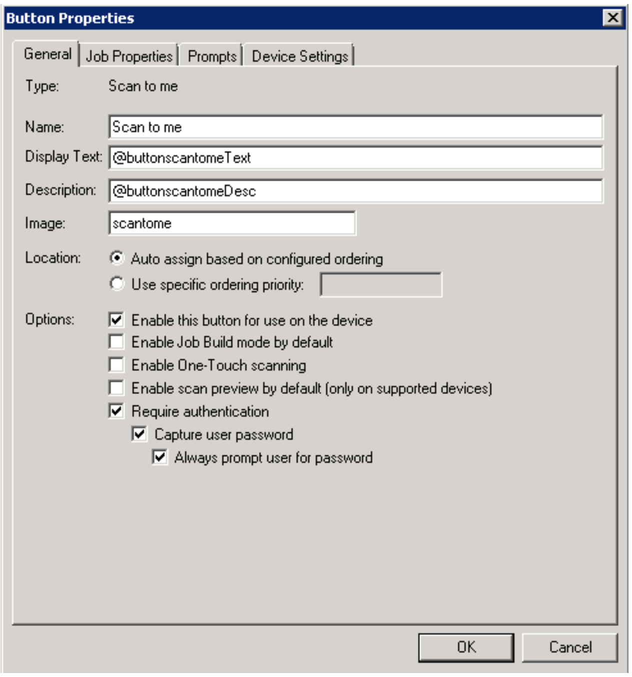
NOTE: If the **Add** button is not active, click on **Device Home Screen**.

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


Type: Routing Sheet

10. Enter a **Name** for the button. Then, click **OK**.

11. You will need to define properties for the button. With the button highlighted on the list, click **Properties**.



Type: Scan to me

Name: Scan to me

Display Text: @buttonscantomeText

Description: @buttonscantomeDesc

Image: scantome

Location:
● Auto assign based on configured ordering
○ Use specific ordering priority:

Options:
☑ Enable this button for use on the device
☐ Enable Job Build mode by default
☐ Enable One-Touch scanning
☐ Enable scan preview by default (only on supported devices)
☑ Require authentication
☑ Capture user password
☑ Always prompt user for password

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

NOTE: Do not change Image from the default value.

NOTE: For buttons requiring authentication, select **Capture user password** for the credential pass-through feature and **Always prompt user for password** for use with HPAC authentication.

12. 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.

13. Select addition options for the button:

- **Enable this button for use on the device** - Self-explanatory.

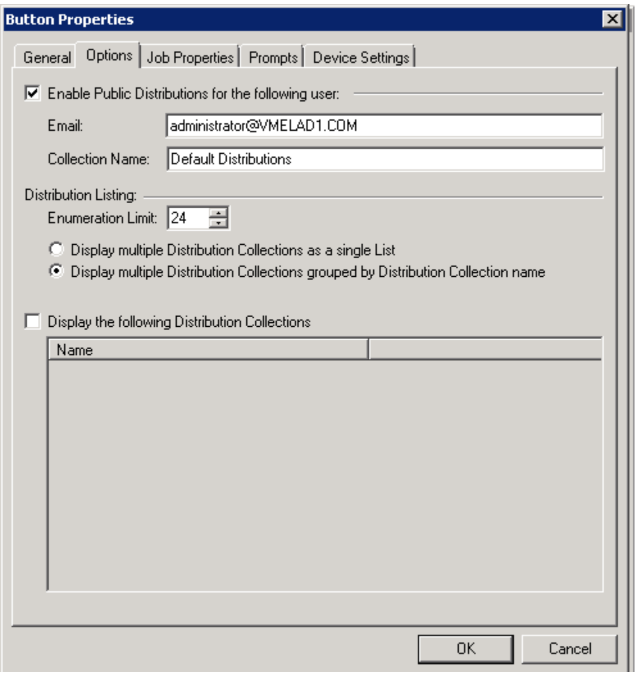
- **Enable job build** - This option enables the Scan More feature.

- **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.

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



Button Properties

☑ Enable Public Distributions for the following user:

Email: administrator@VMELAD1.COM

Collection Name: Default Distributions

Distribution Listing:

Enumeration Limit: 24

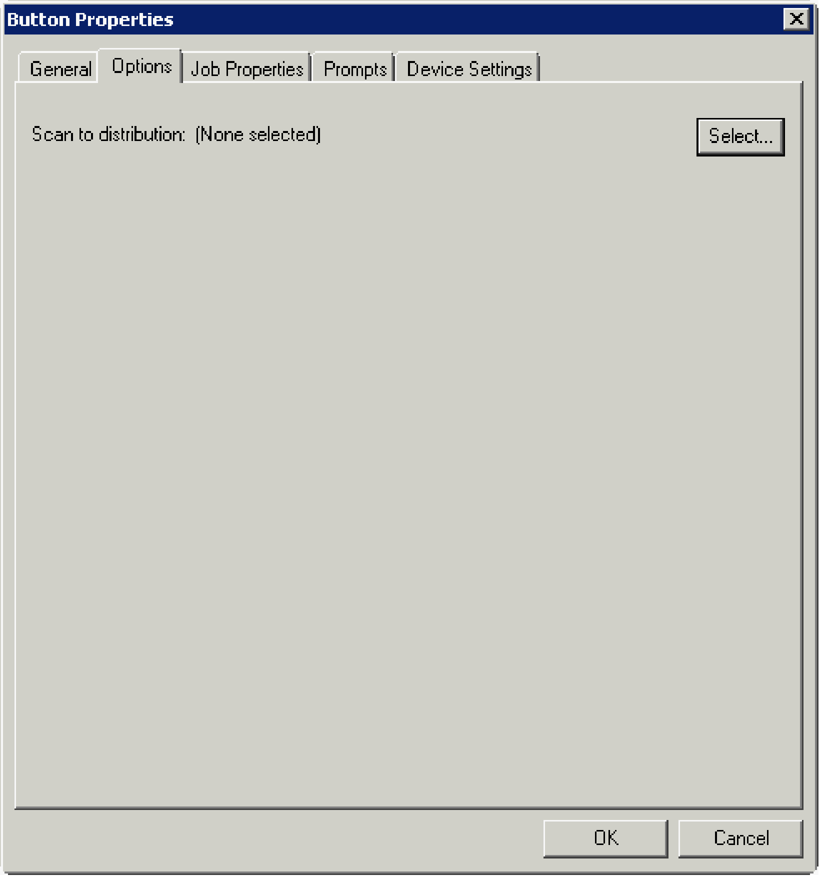
○ Display multiple Distribution Collections as a single List

● Display multiple Distribution Collections grouped by Distribution Collection name

☐ Display the following Distribution Collections

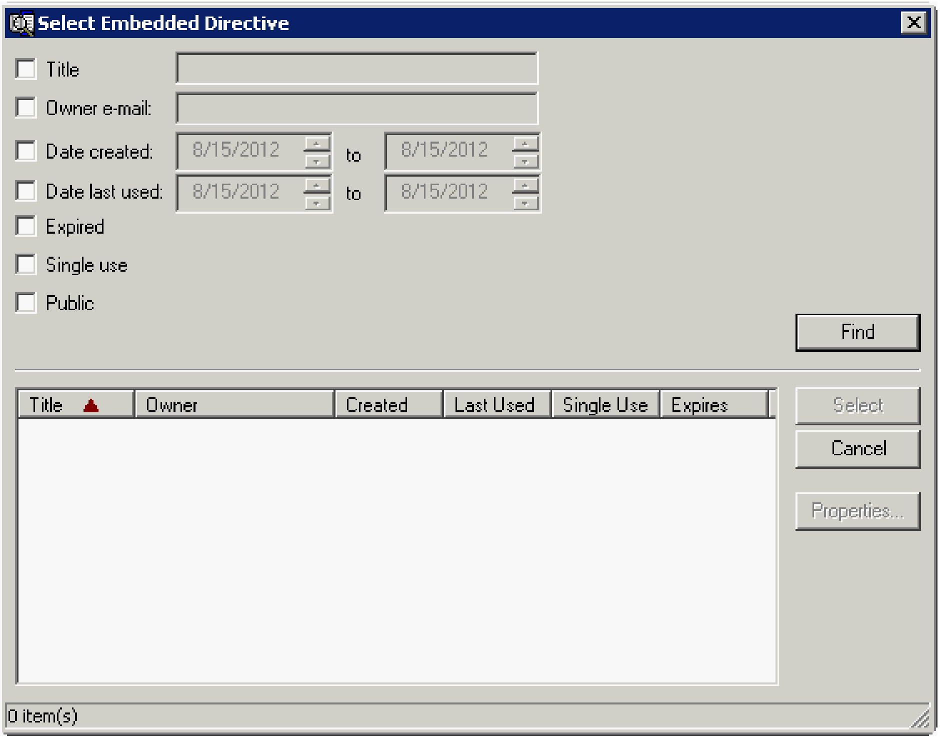
Enter a **Public Email** address (if applicable) and set the **Enumeration Limit** for distributions (the maximum number of distributions allowable).

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



Scan to distribution: (None selected)

Click **Select** and the **Select Embedded Directive** dialog is displayed.



☐ 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

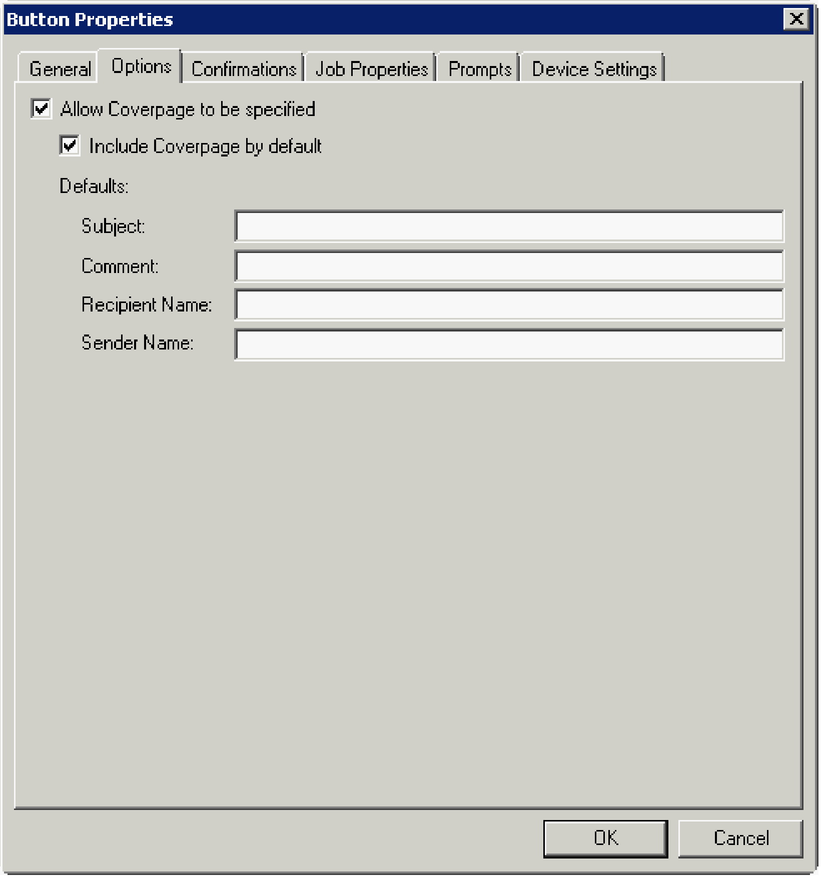
☐ Public

0 item(s)

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.

16. 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.



☑ Allow Coverpage to be specified

☑ Include Coverpage by default

Defaults:

Subject:

Comment:

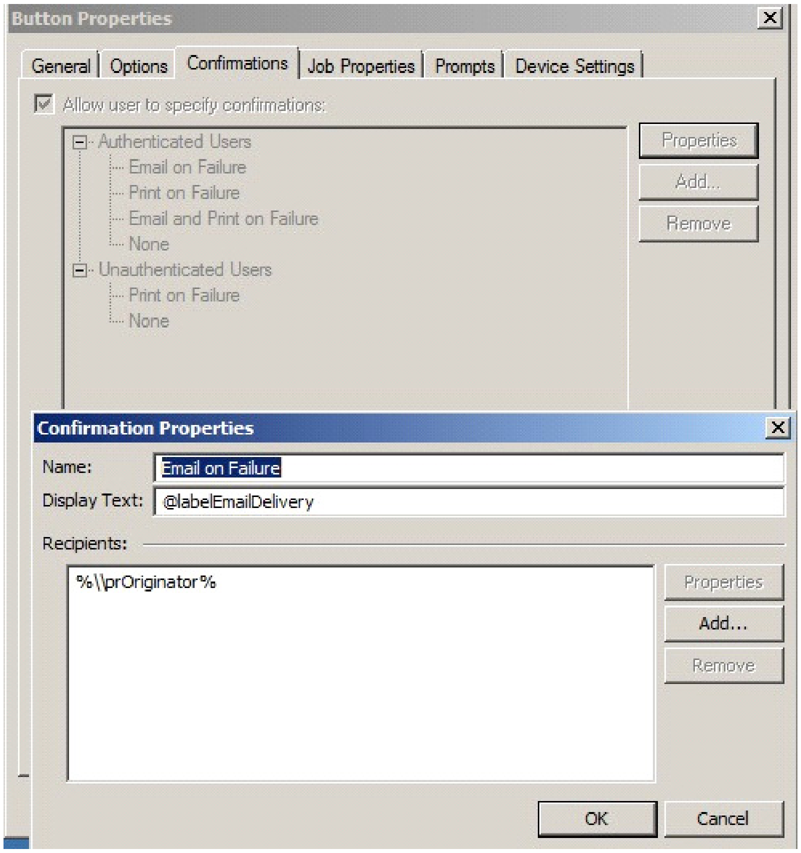
Recipient Name:

Sender Name:

17. 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).

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

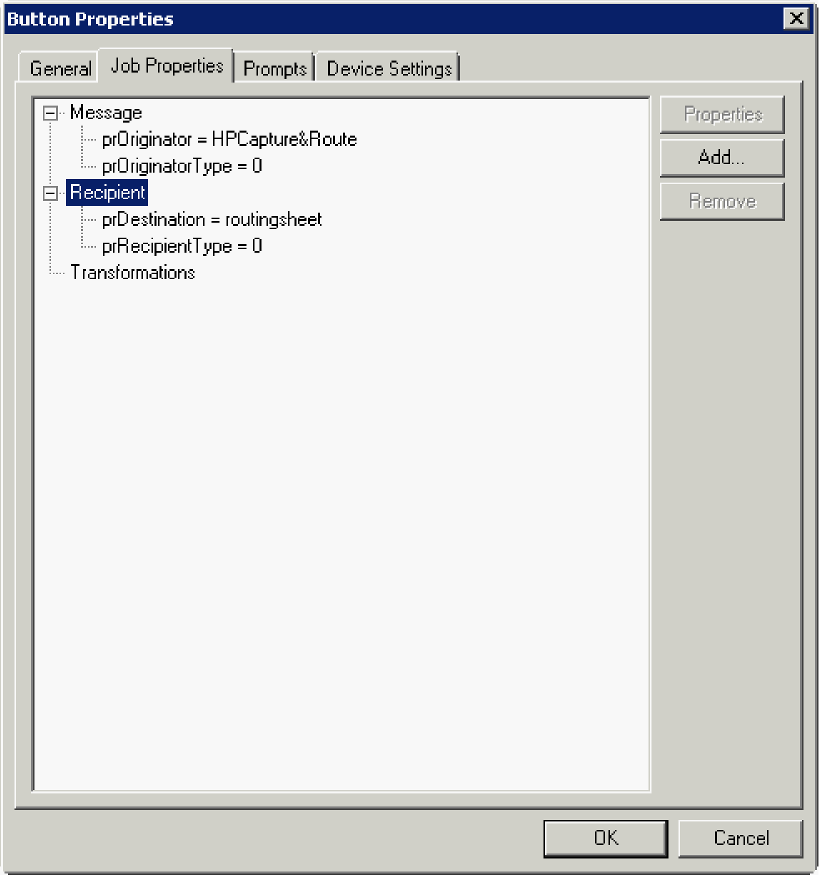


Name: Email on Failure

Display Text: @labelEmailDelivery

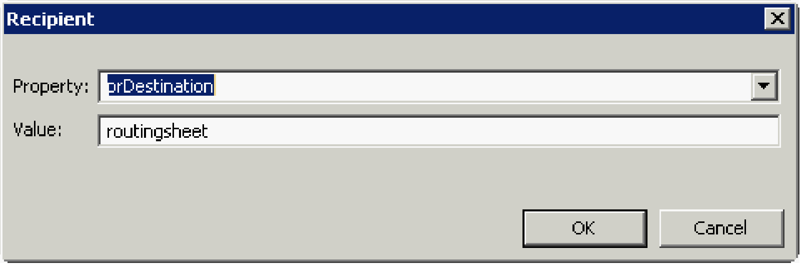
Recipients: %\\prOriginator%

18. 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.



```
Message
    prOriginator = HPCapture&Route
    prOriginatorType = 0
Recipient
    prDestination = routingsheet
    prRecipientType = 0
Transformations
```

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



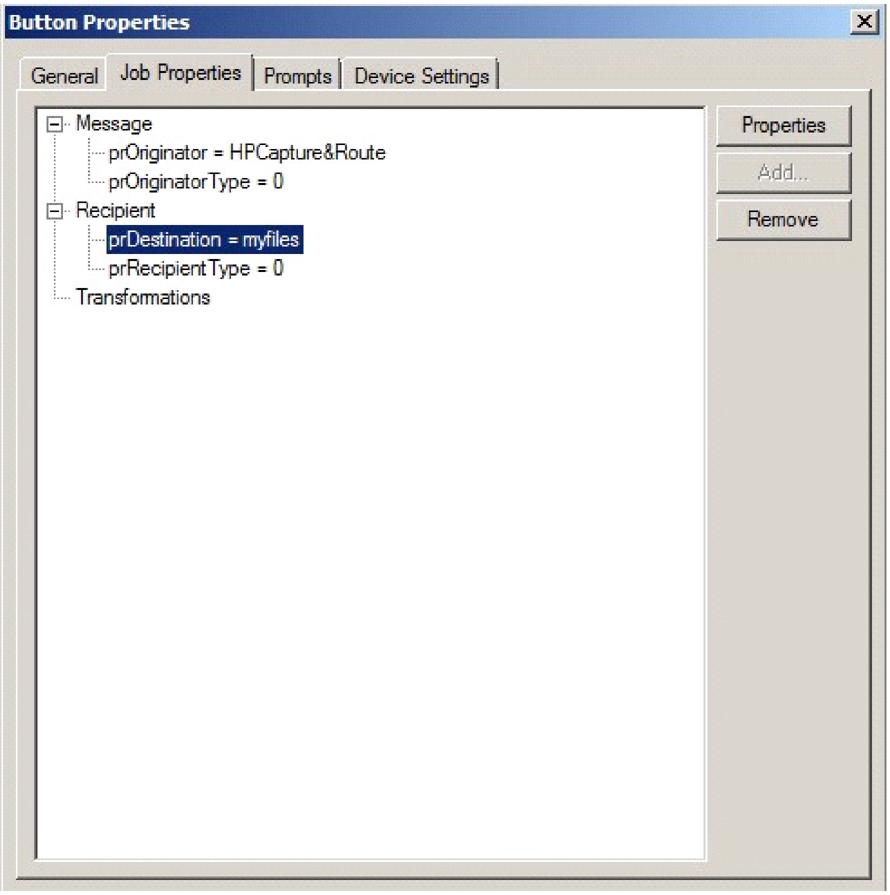
Property: prDestination

Value: routingsheet

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.).

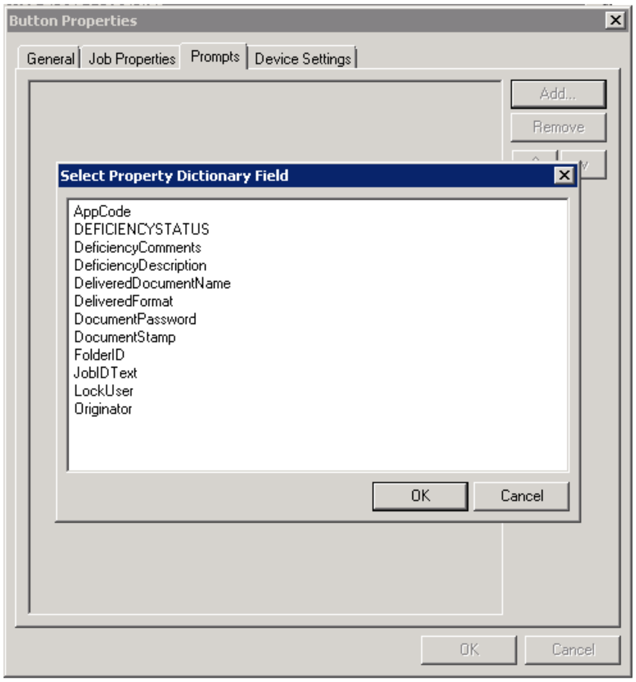
Note that the **Scan to Destination** button allows for message routing based on routing rules.

- 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.



Message
prOriginator = HPCapture&Route
prOriginatorType = 0
Recipient
prDestination = myfiles
prRecipientType = 0
Transformations

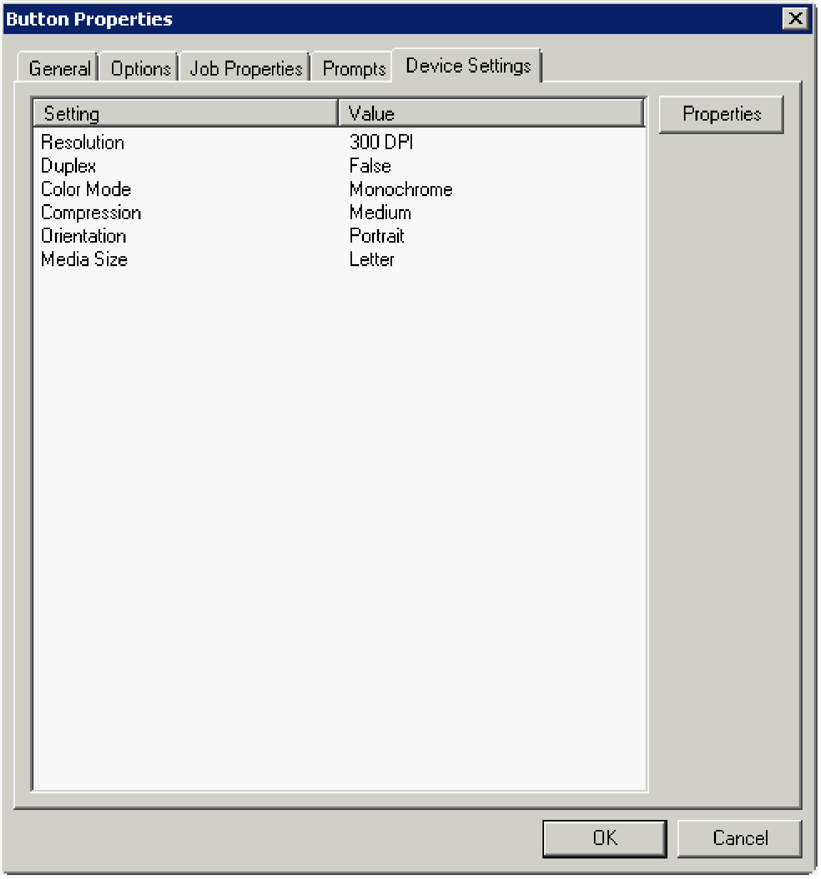
19. Click the **Prompts** tab. Click **Add** to select a prompt configured on the HP CR server. The **Select Property Dictionary Field** is displayed.



AppCode
DEFICIENCYSTATUS
DeficiencyComments
DeficiencyDescription
DeliveredDocumentName
DeliveredFormat
DocumentPassword
DocumentStamp
FolderID
JobIDText
LockUser
Originator

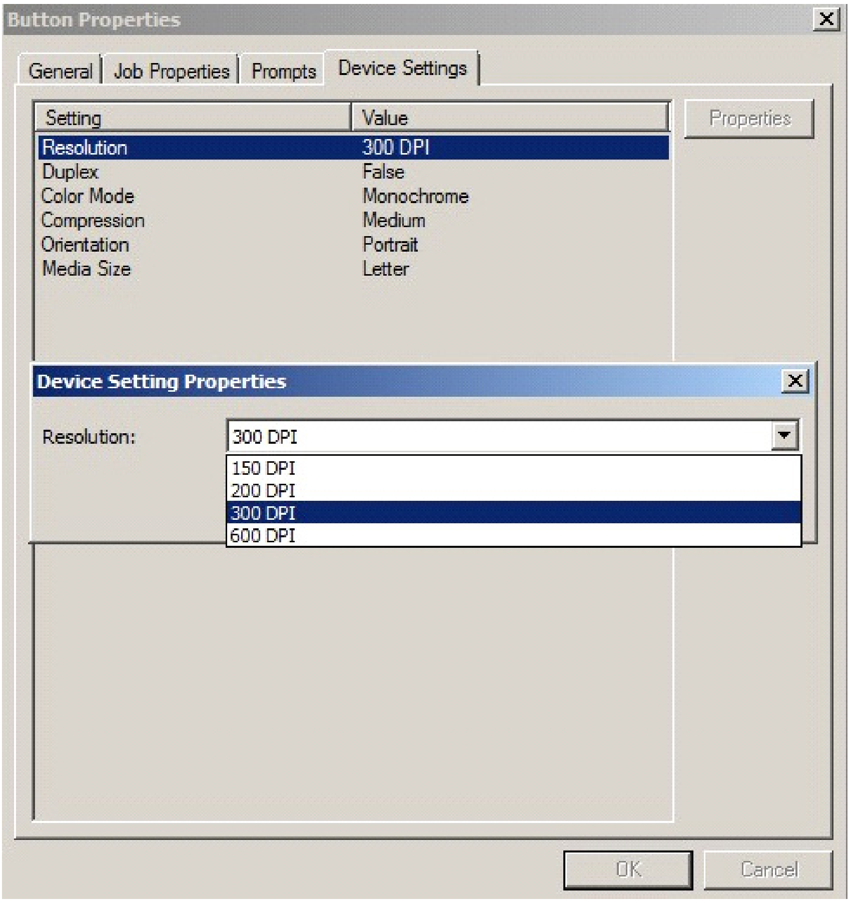
Select a prompt and click **OK**.

20. 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.



Setting	Value
Resolution	300 DPI
Duplex	False
Color Mode	Monochrome
Compression	Medium
Orientation	Portrait
Media Size	Letter

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



Setting	Value
Resolution	300 DPI
Duplex	False
Color Mode	Monochrome
Compression	Medium
Orientation	Portrait
Media Size	Letter

Resolution: 300 DPI

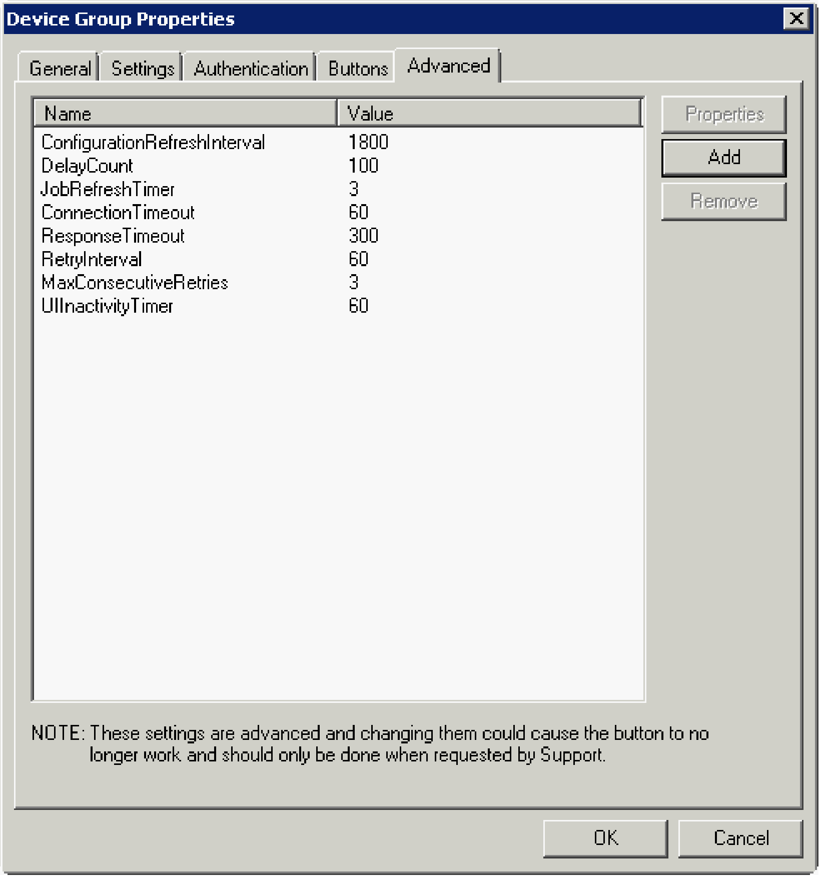
NOTE: The HP Officejet Pro 276dw does not support 600 x 600 scanning with the HP CR Embedded Device Client.

21. 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.

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

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



Name	Value
ConfigurationRefreshInterval	1800
DelayCount	100
JobRefreshTimer	3
ConnectionTimeout	60
ResponseTimeout	300
RetryInterval	60
MaxConsecutiveRetries	3
UIInactivityTimer	60

NOTE: These settings are advanced and changing them could cause the button to no longer work and should only be done when requested by Support.

23. Click **OK** to end your work with the **Device Group Properties**.

24. 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 Installing HP CR Embedded Device Client buttons (68).

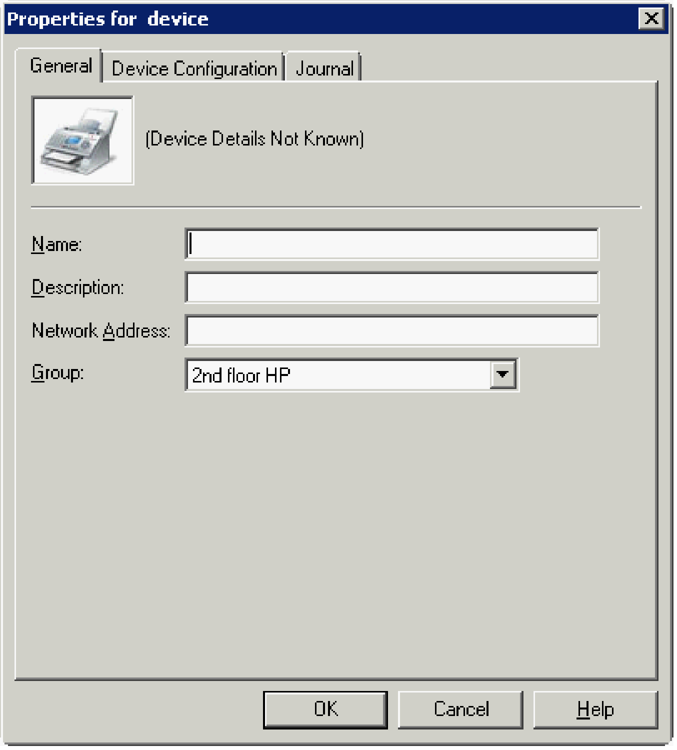
6-1-3 Updating the Deviceloader.xml to support new devices

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

6-1-4 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

Name:

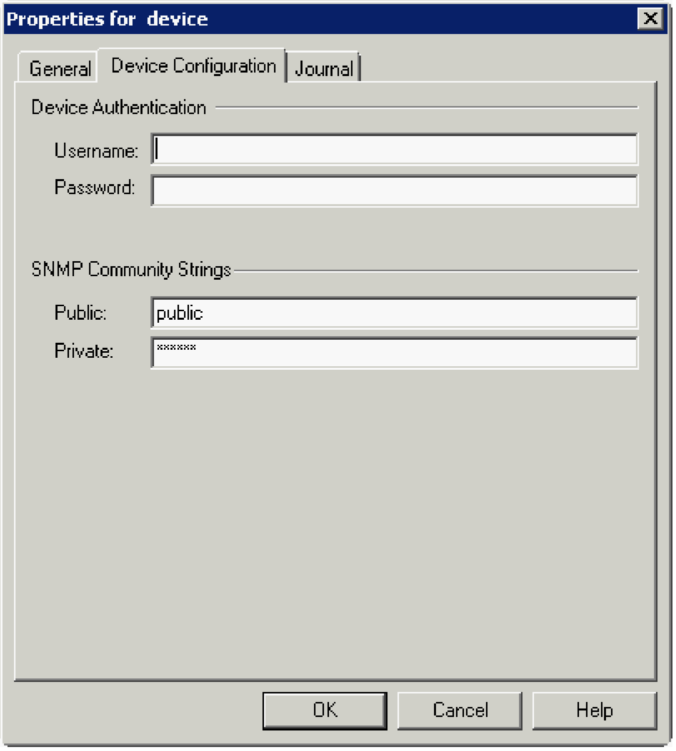
Description:

Network Address:

Group: 2nd floor HP

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:



Device Authentication

Username:

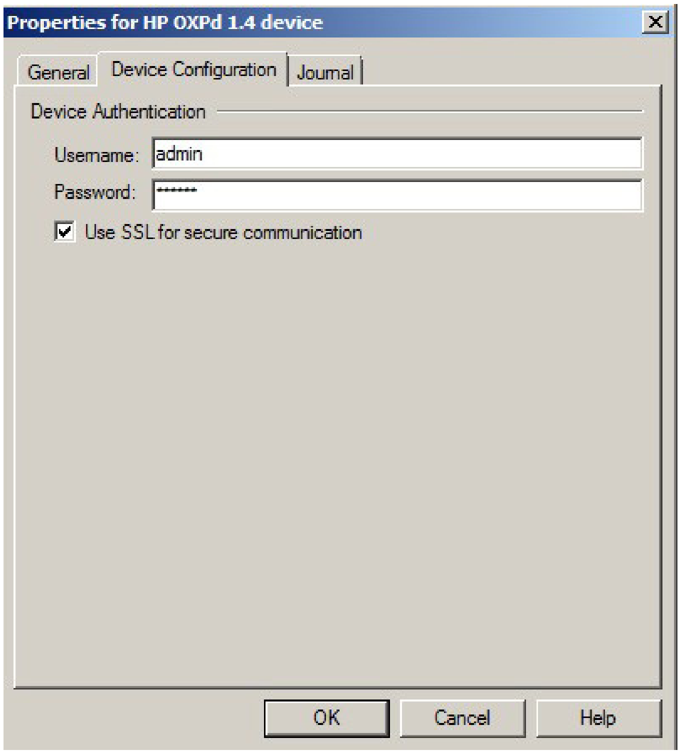
Password:

SNMP Community Strings

Public: public

Private: ******

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



Device Authentication

Username: admin

Password: ******

☑ Use SSL for secure communication

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.

6-2 Choosing an authentication method

The HP CR Embedded Device Client must be able to authenticate the device user when the **Personal Distributions** or **Scan to My Files** options are used.

You can configure:

- LDAP authentication
- HP authentication at the device

NOTE: HP Pro devices do not support LDAP authentication.

6-2-1 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.

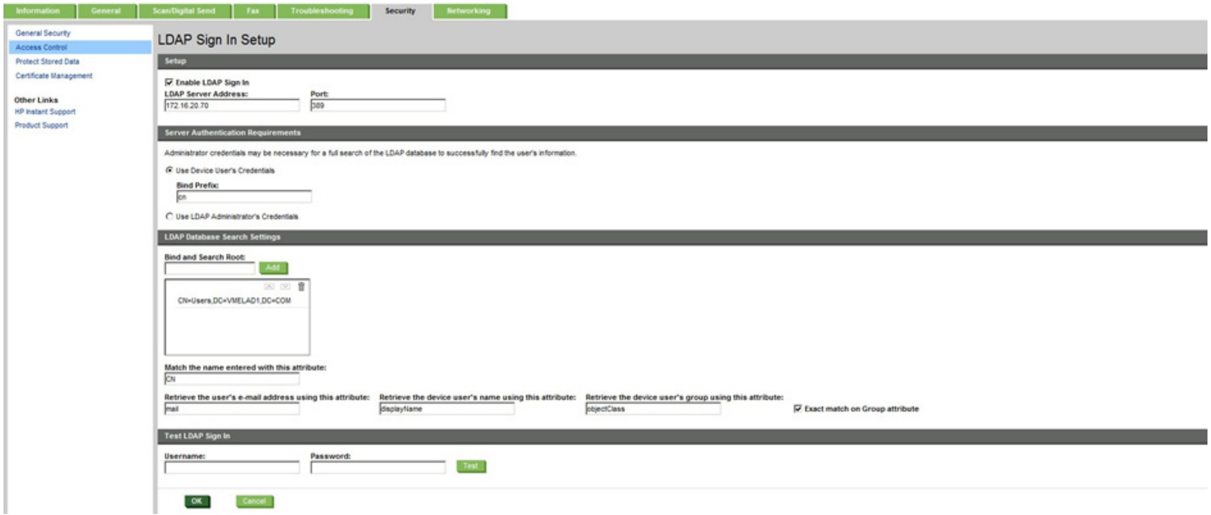
Both the email username and password are required to identify the device user, and the credentials are validated via LDAP authentication. This method provides increased security.

NOTE: With **LDAP Authentication** configured for the device group on the Administrator, the LDAP lookup only appears on the device once **Require Authentication** is enabled for the relevant device button. See step 6 of Defining Password Properties (46) for details.

The following figure is an example of an LDAP Authentication configuration for Active Directory. (For information on configuring LDAP Authentication, consult HP documentation.)

Figure 6-1 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)



LDAP Sign In Setup

Setup

☑ Enable LDAP Sign In

LDAP Server Address: 172.16.20.70

Port: 389

Server Authentication Requirements

Administrator credentials may be necessary for a full search of the LDAP database to successfully find the user's information.

● Use Device User's Credentials

Bind Prefix: cn

○ Use LDAP Administrator's Credentials

LDAP Database Search Settings

Bind and Search Root: Add

CN=Users,DC=VMELAD1,DC=COM

Match the name entered with this attribute: CN

Retrieve the user's e-mail address using this attribute: mail

Retrieve the device user's name using this attribute: displayName

Retrieve the device user's group using this attribute: objectClass

☑ Exact match on Group attribute

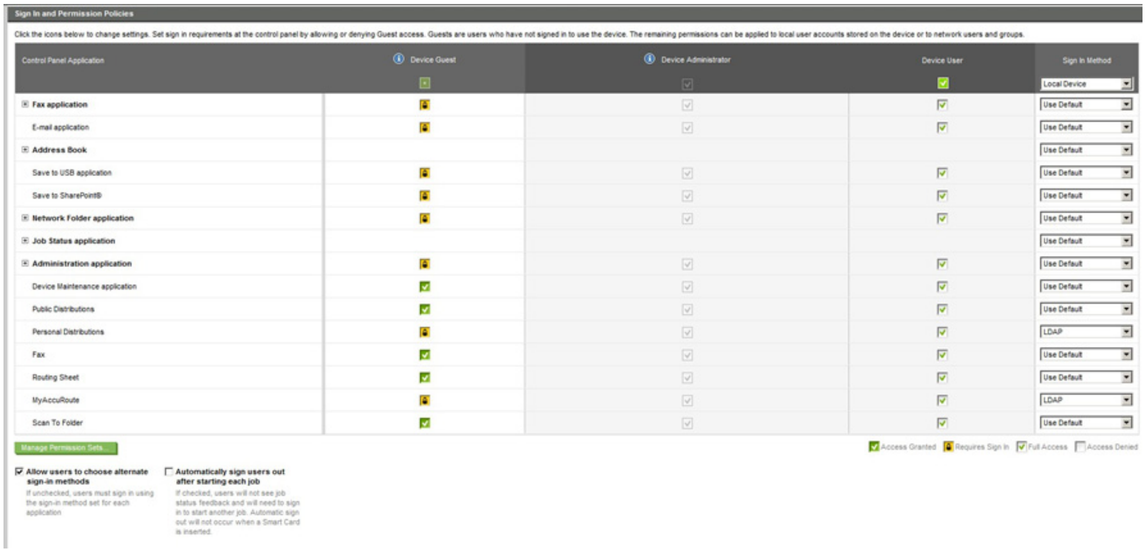
Test LDAP Sign In

Username:

Password:

Test

OK Cancel



Sign In and Permission Policies

Click the icons below to change settings. Set sign in requirements at the control panel by allowing or denying Guest access. Guests are users who have not signed in to use the device. The remaining permissions can be applied to local user accounts stored on the device or to network users and groups.

Control Panel Application	Device Guest	Device Administrator	Device User	Sign In Method
		☑	✓	Local Device
⊞ **Fax application**	🔒	☑	☑	Use Default
E-mail application	🔒	☑	☑	Use Default
⊞ **Address Book**				Use Default
Save to USB application	🔒	☑	☑	Use Default
Save to SharePoint®	🔒	☑	☑	Use Default
⊞ **Network Folder application**	🔒	☑	☑	Use Default
⊞ **Job Status application**				Use Default
⊞ **Administration application**	🔒	☑	☑	Use Default
Device Maintenance application	✓	☑	☑	Use Default
Public Distributions	✓	☑	☑	Use Default
Personal Distributions	🔒	☑	☑	LDAP
Fax	✓	☑	☑	Use Default
Routing Sheet	✓	☑	☑	Use Default
MyAccuRoute	🔒	☑	☑	LDAP
Scan To Folder	✓	☑	☑	Use Default

✓ Access Granted 🔒 Requires Sign In ☑ Full Access □ Access Denied

Manage Permission Sets...

☑ **Allow users to choose alternate sign-in methods**
If unchecked, users must sign in using the sign-in method set for each application

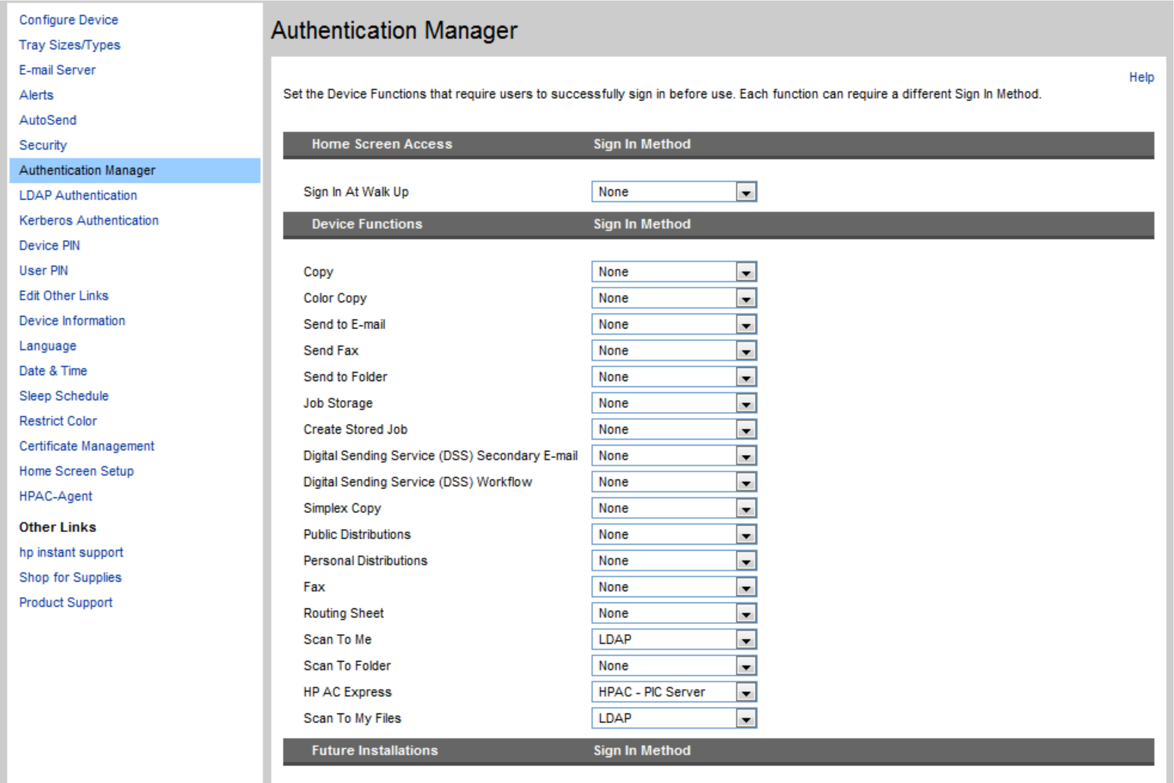
□ **Automatically sign users out after starting each job**
If checked, users will not see job status feedback and will need to sign in to start another job. Automatic sign out will not occur when a Smart Card is inserted.

6-2-2 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

   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.



Authentication Manager

Set the Device Functions that require users to successfully sign in before use. Each function can require a different Sign In Method.

Home Screen Access	Sign In Method
Sign In At Walk Up	None

Device Functions	Sign In Method
Copy	None
Color Copy	None
Send to E-mail	None
Send Fax	None
Send to Folder	None
Job Storage	None
Create Stored Job	None
Digital Sending Service (DSS) Secondary E-mail	None
Digital Sending Service (DSS) Workflow	None
Simplex Copy	None
Public Distributions	None
Personal Distributions	None
Fax	None
Routing Sheet	None
Scan To Me	LDAP
Scan To Folder	None
HP AC Express	HPAC - PIC Server
Scan To My Files	LDAP

Future Installations	Sign In Method

7. Click **Apply**.

6-3 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 8: Testing (79).

7 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:

7-1 Supported devices

The following devices are supported:

Table 1 HP Device Series Matrix

Device	Operating System
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
Color LaserJet CM 3530 MFP	Oz
Color LaserJet CM 4540 MFP	FutureSmart
ScanJet 7000n	FutureSmart

Device	**Operating System**
ScanJet 8500	FutureSmart
LaserJet Flow M525 MXP	FutureSmart
LaserJet Flow M575 MXP	FutureSmart
LaserJet M775 MFP	FutureSmart
LaserJet M4555 MFP	FutureSmart
HP Color Laserjet Flow MFP M880	FutureSmart
HP Color Laserjet Flow MFP M830	FutureSmart
HP Laserjet MFP M725	FutureSmart

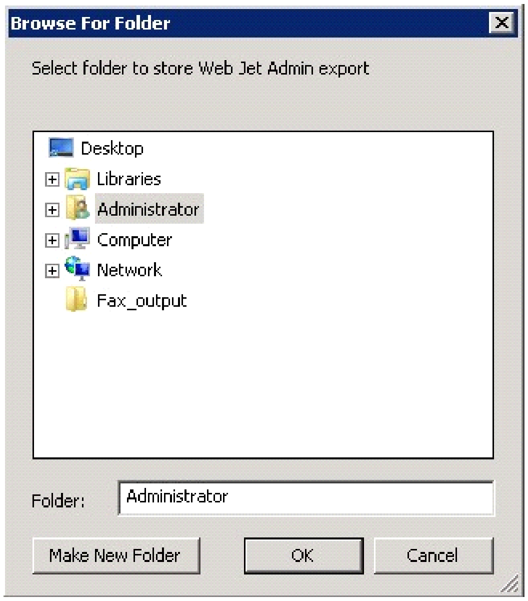
7-2 Exporting the XML files

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 2: HP CR Embedded Device Client Installation and Section 6: Required Configuration), 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:

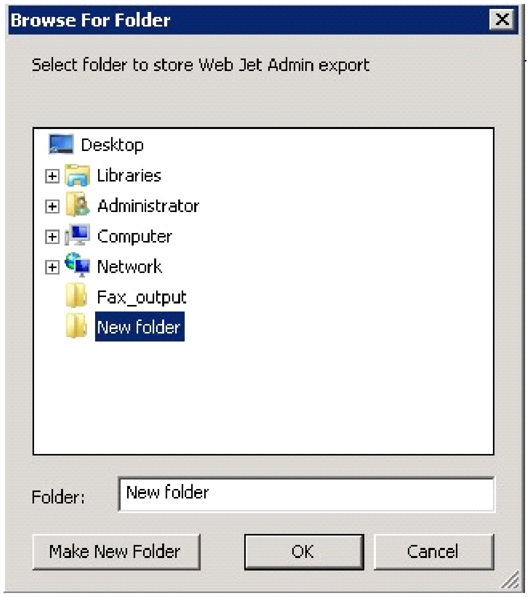


Browse For Folder

Select folder to store Web Jet Admin export

Folder: Administrator

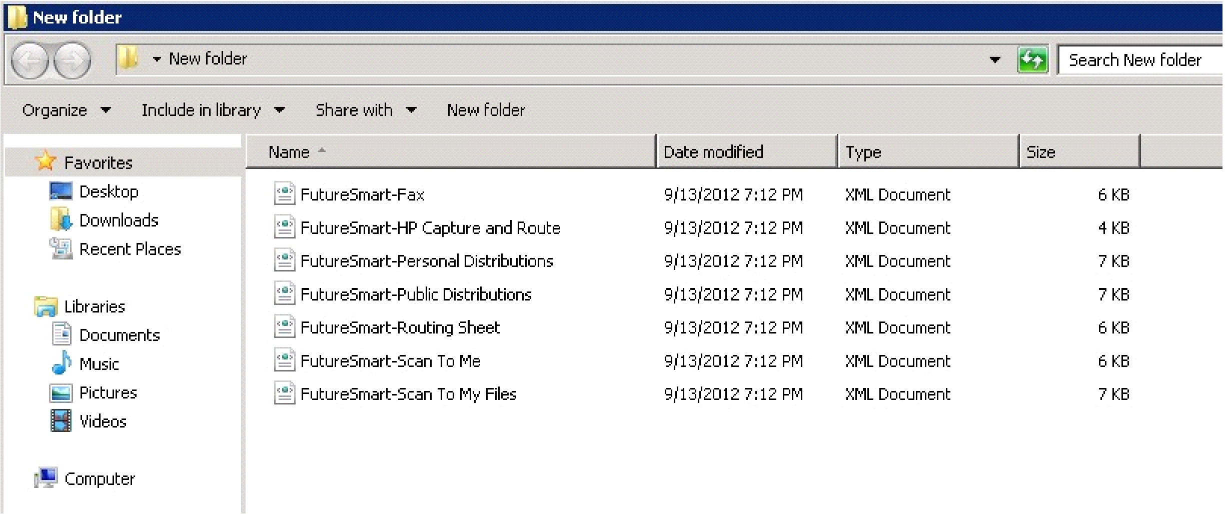
Make New Folder:



Select folder to store Web Jet Admin export

Folder: New folder

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



Name	Date modified	Type	Size
FutureSmart-Fax	9/13/2012 7:12 PM	XML Document	6 KB
FutureSmart-HP Capture and Route	9/13/2012 7:12 PM	XML Document	4 KB
FutureSmart-Personal Distributions	9/13/2012 7:12 PM	XML Document	7 KB
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
FutureSmart-Scan To Me	9/13/2012 7:12 PM	XML Document	6 KB
FutureSmart-Scan To My Files	9/13/2012 7:12 PM	XML Document	7 KB

7-3 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.
3. In the **Security** tab, select **Certificate Management**.
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.

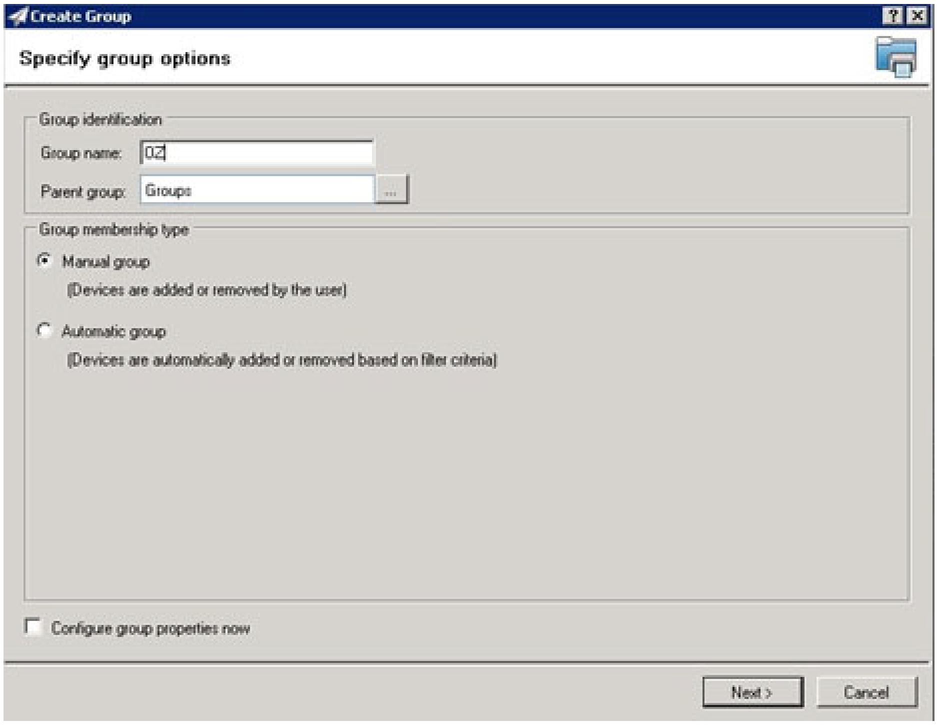
7-4 Installing HP CR Embedded Device Client buttons

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.



Create Group

Specify group options

Group identification

Group name: OZ

Parent group: Groups

Group membership type

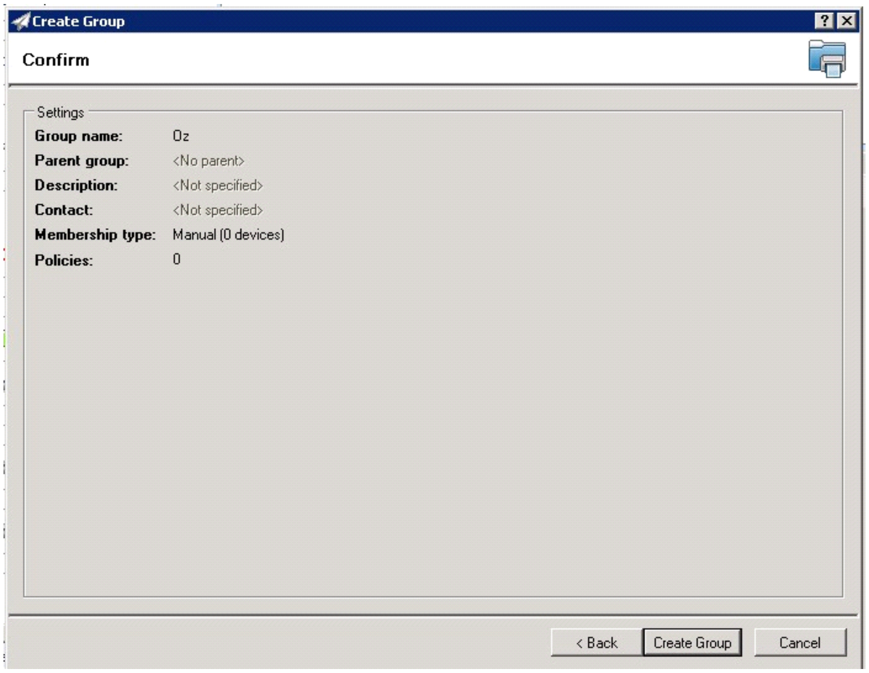
● Manual group
(Devices are added or removed by the user)

○ Automatic group
(Devices are automatically added or removed based on filter criteria)

□ Configure group properties now

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.

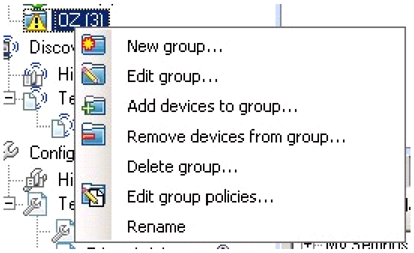


Settings

Group name: Oz
Parent group: <No parent>
Description: <Not specified>
Contact: <Not specified>
Membership type: Manual (0 devices)
Policies: 0

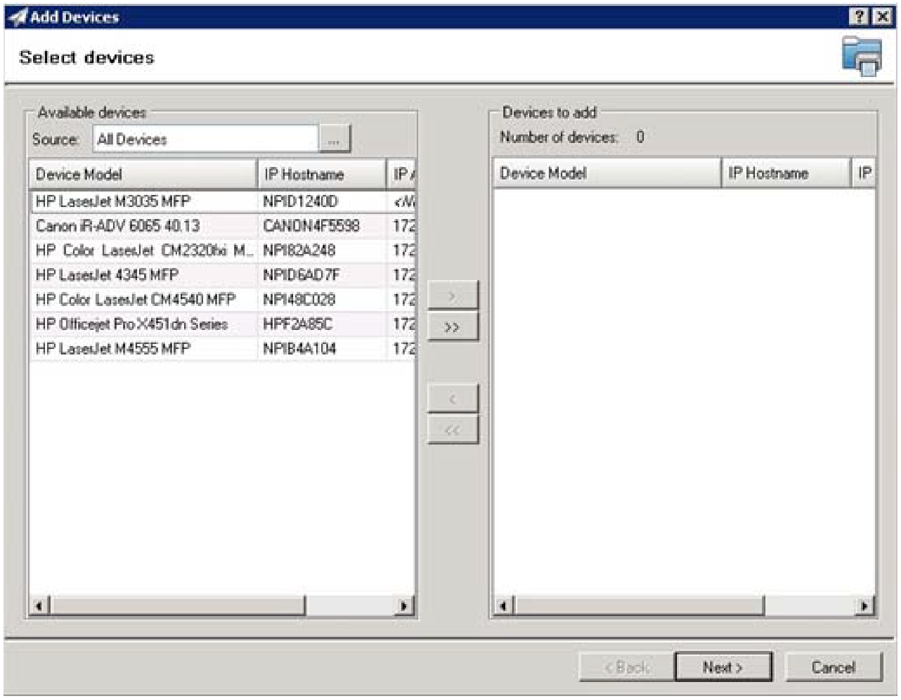
4. Click **Create Group** and then **Done**.

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



NOTE: For more options 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.

The **Select Devices** page appears.



Available devices

Source: All Devices

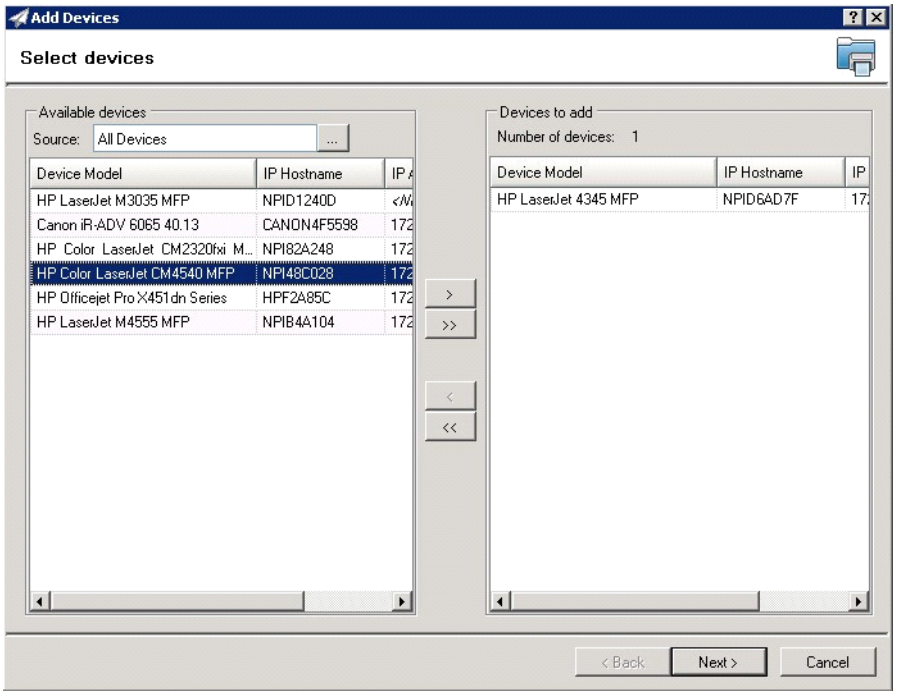
Device Model	IP Hostname	IP A
HP LaserJet M3035 MFP	NPID1240D	<M
Canon iR-ADV 6065 40.13	CANON4F5598	172
HP Color LaserJet CM2320fxi M...	NPI82A248	172
HP LaserJet 4345 MFP	NPID6AD7F	172
HP Color LaserJet CM4540 MFP	NPI48C028	172
HP Officejet Pro X451dn Series	HPF2A85C	172
HP LaserJet M4555 MFP	NPIB4A104	172

Devices to add

Number of devices: 0

Device Model	IP Hostname	IP

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).



Available devices

Source: All Devices

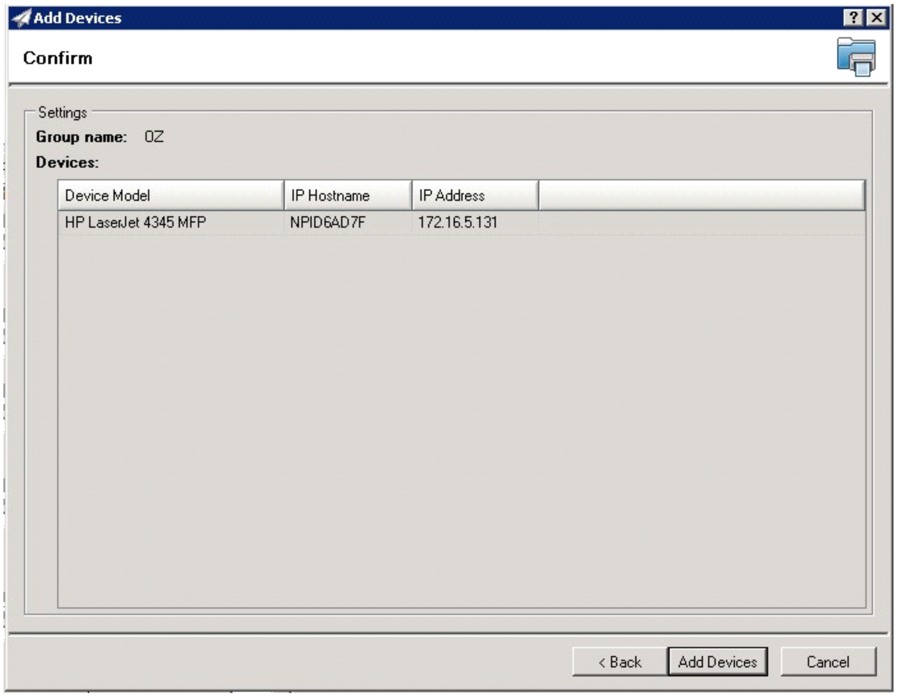
Device Model	IP Hostname	IP A
HP LaserJet M3035 MFP	NPID1240D	<M
Canon iR-ADV 6065 40.13	CANON4F5598	172
HP Color LaserJet CM2320fxi M...	NPI82A248	172
HP Color LaserJet CM4540 MFP	NPI48C028	172
HP Officejet Pro X451dn Series	HPF2A85C	172
HP LaserJet M4555 MFP	NPIB4A104	172

Devices to add

Number of devices: 1

Device Model	IP Hostname	IP
HP LaserJet 4345 MFP	NPID6AD7F	17

7. Click **Next**. The **Confirm** page appears.



Add Devices

Confirm

Settings

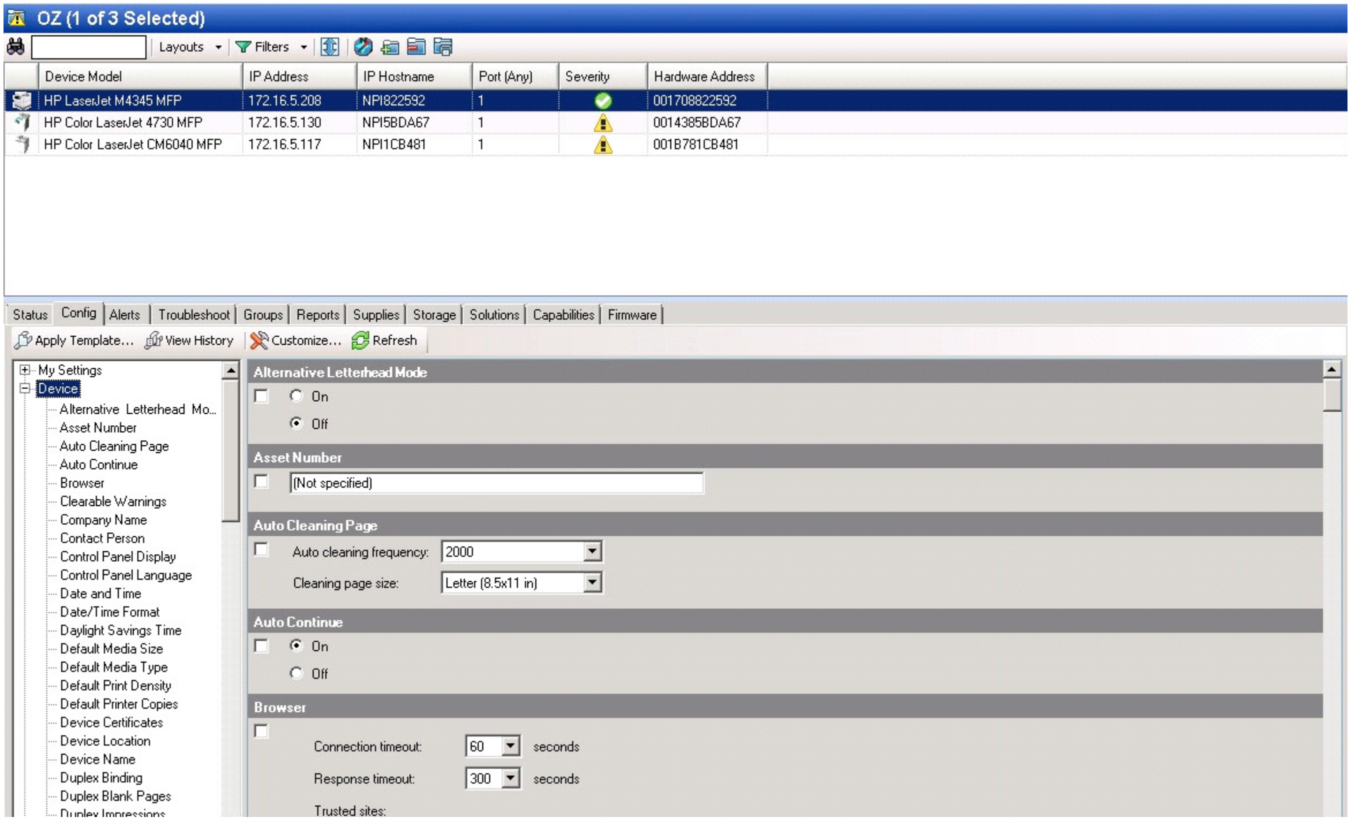
Group name: OZ

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** page.

9. Highlight the device(s) on which you want to install buttons.



OZ (1 of 3 Selected)

Device Model	IP Address	IP Hostname	Port (Any)	Severity	Hardware Address
HP LaserJet M4345 MFP	172.16.5.208	NPI822592	1	✓	001708822592
HP Color LaserJet 4730 MFP	172.16.5.130	NPI5BDA67	1	⚠	0014385BDA67
HP Color LaserJet CM6040 MFP	172.16.5.117	NPI1CB481	1	⚠	001B781CB481

Alternative Letterhead Mode

□ ○ On

● Off

Asset Number

□ (Not specified)

Auto Cleaning Page

□ Auto cleaning frequency: 2000

Cleaning page size: Letter (8.5x11 in)

Auto Continue

□ ● On

○ Off

Browser

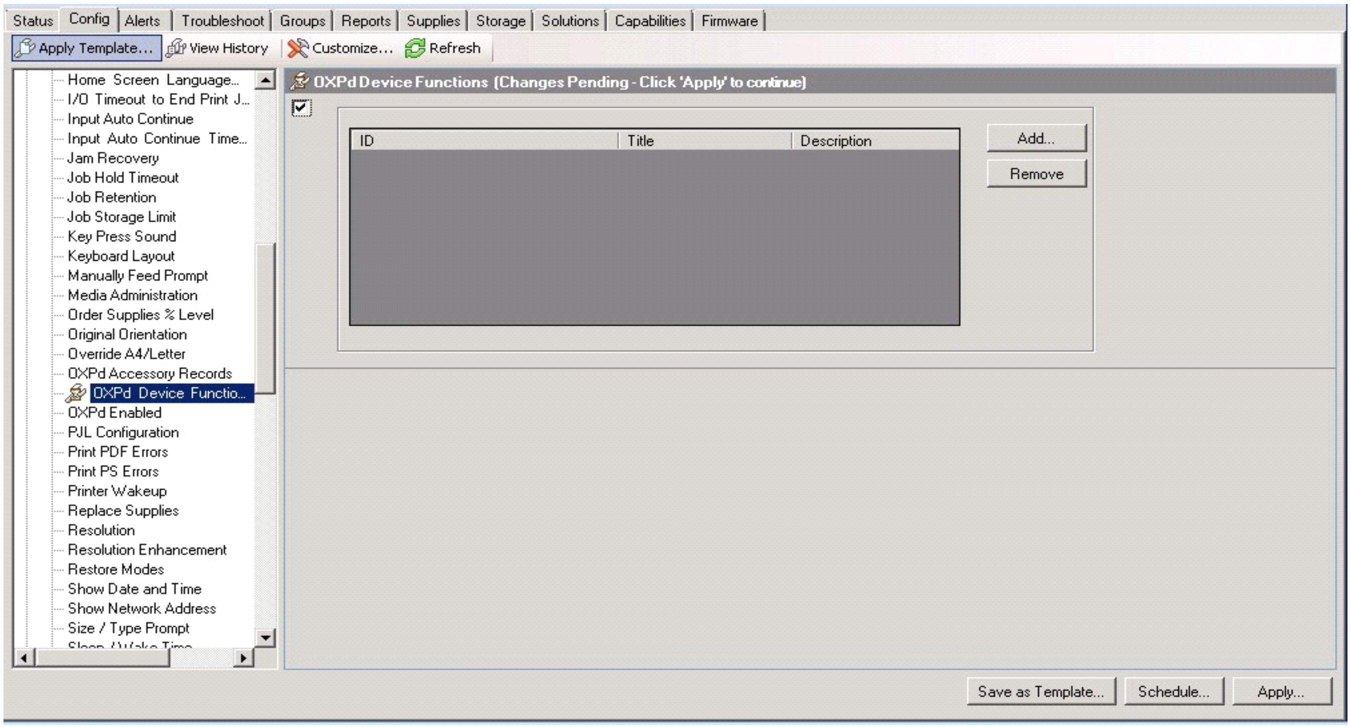
□

Connection timeout: 60 seconds

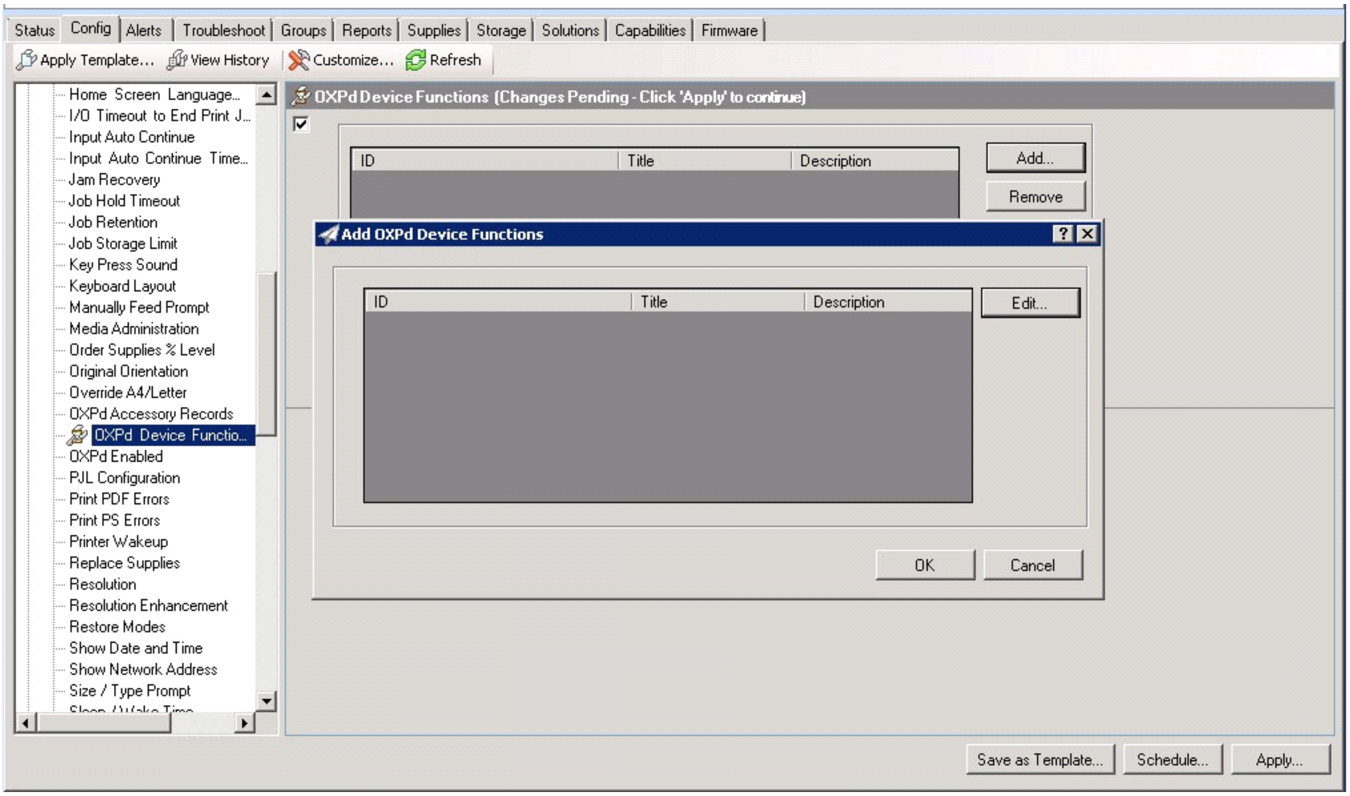
Response timeout: 300 seconds

Trusted sites:

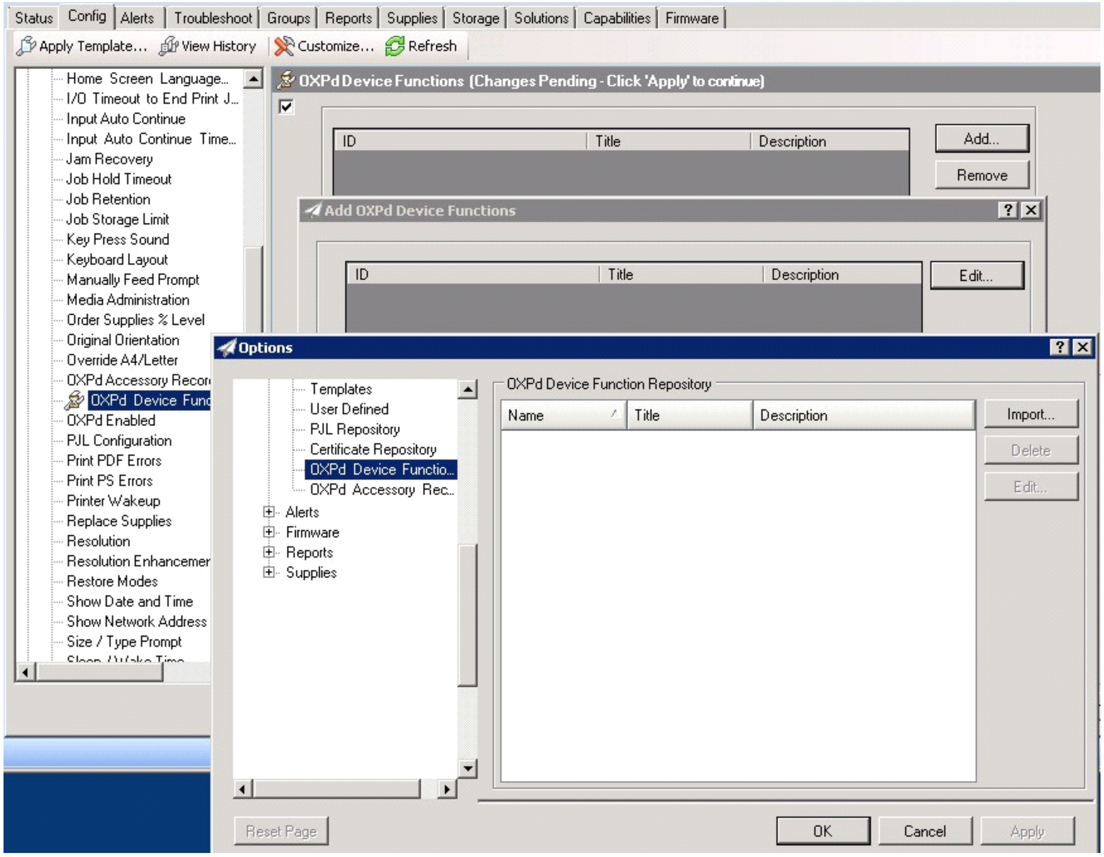
10. Click the **Config** tab and scroll to the **OXPd Device Functions** subset (as shown below). Check the box in the upper left corner of the center screen. The title bar of that area will read: *OXPd Device Functions (Changes Pending - Click ‘Apply’ to continue)*.



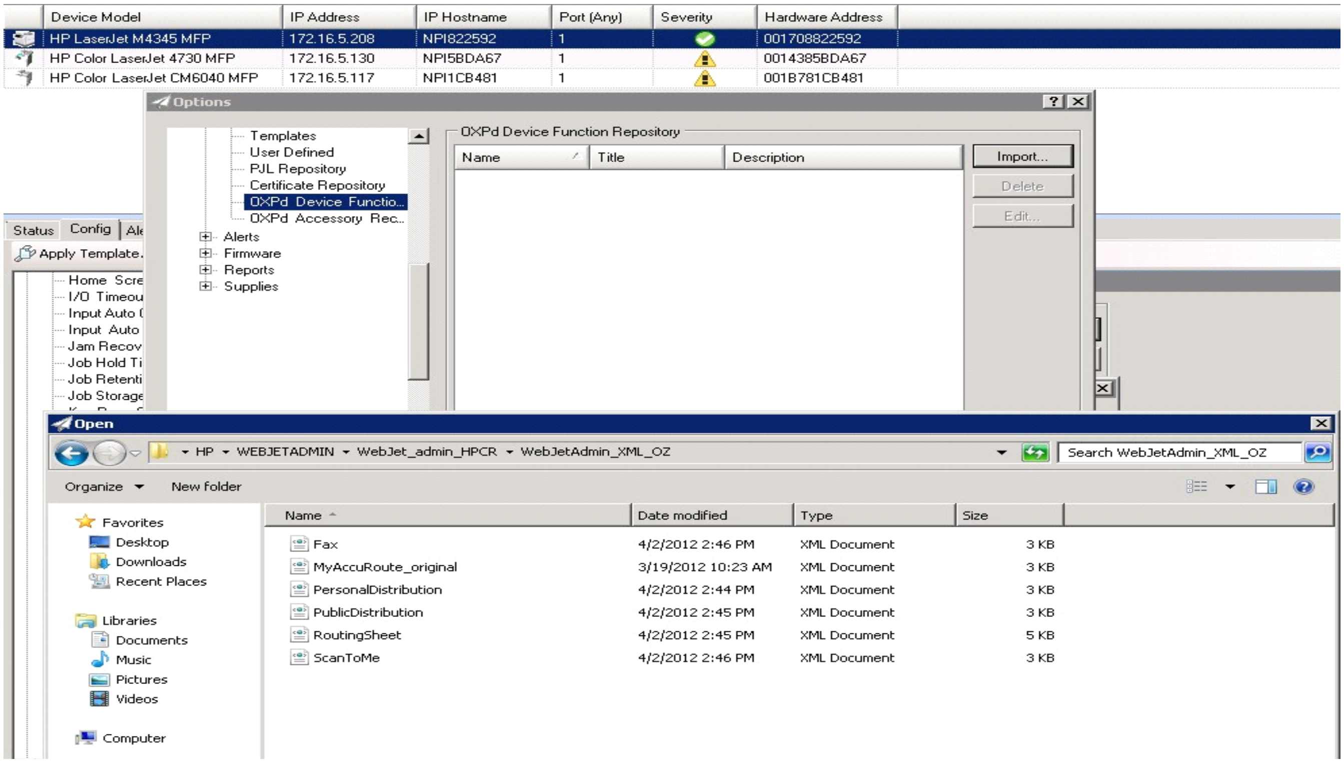
11. Click the **Add** button. The **Add OXPd Device Functions** page appears.



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 66).



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

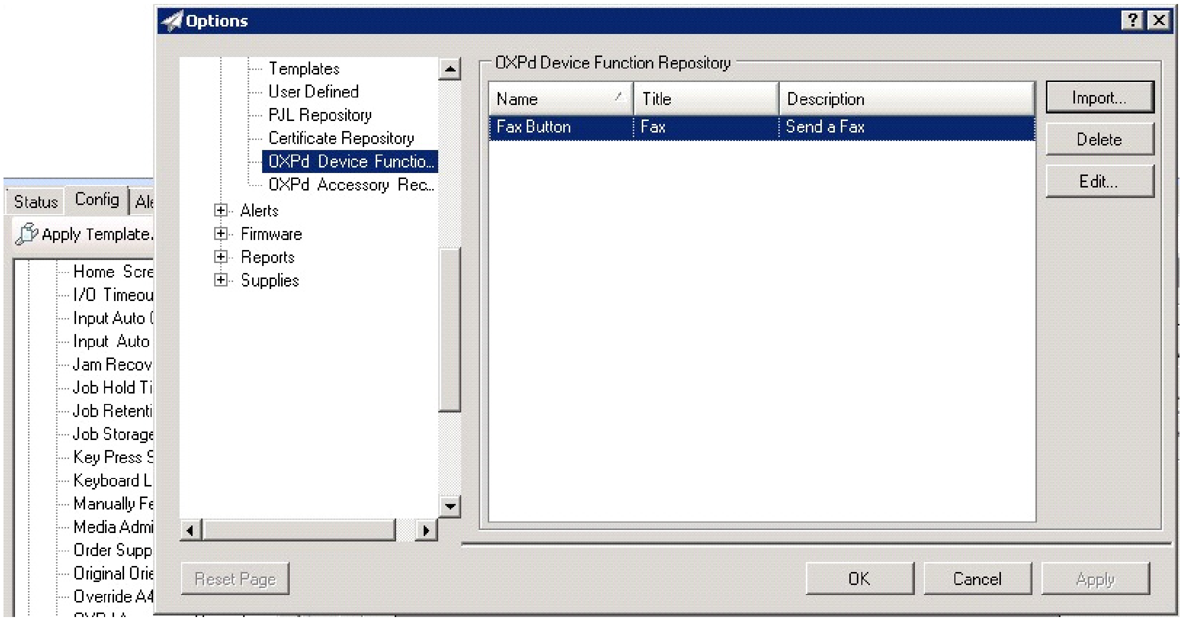


Device Model	IP Address	IP Hostname	Port (Any)	Severity	Hardware Address
HP LaserJet M4345 MFP	172.16.5.208	NPI822592	1	✓	001708822592
HP Color LaserJet 4730 MFP	172.16.5.130	NPI5BDA67	1	⚠	0014385BDA67
HP Color LaserJet CM6040 MFP	172.16.5.117	NPI1CB481	1	⚠	001B781CB481

Name	Date modified	Type	Size
Fax	4/2/2012 2:46 PM	XML Document	3 KB
MyAccuRoute_original	3/19/2012 10:23 AM	XML Document	3 KB
PersonalDistribution	4/2/2012 2:44 PM	XML Document	3 KB
PublicDistribution	4/2/2012 2:45 PM	XML Document	3 KB
RoutingSheet	4/2/2012 2:45 PM	XML Document	5 KB
ScanToMe	4/2/2012 2:46 PM	XML Document	3 KB

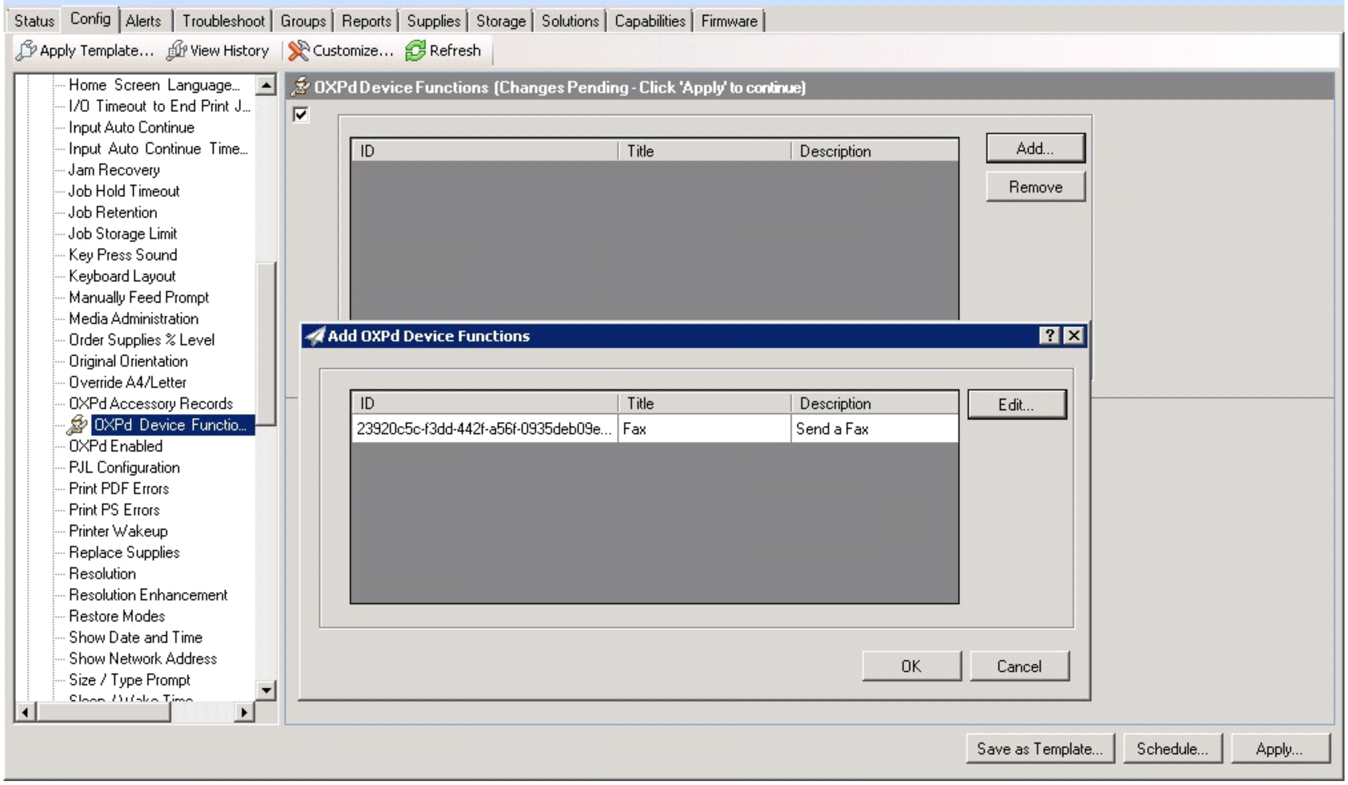
14. Select and highlight the file and then click **Open** to add the file. (You can import only one file at a time in the **Open** page.)

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



Name	Title	Description
Fax Button	Fax	Send a Fax

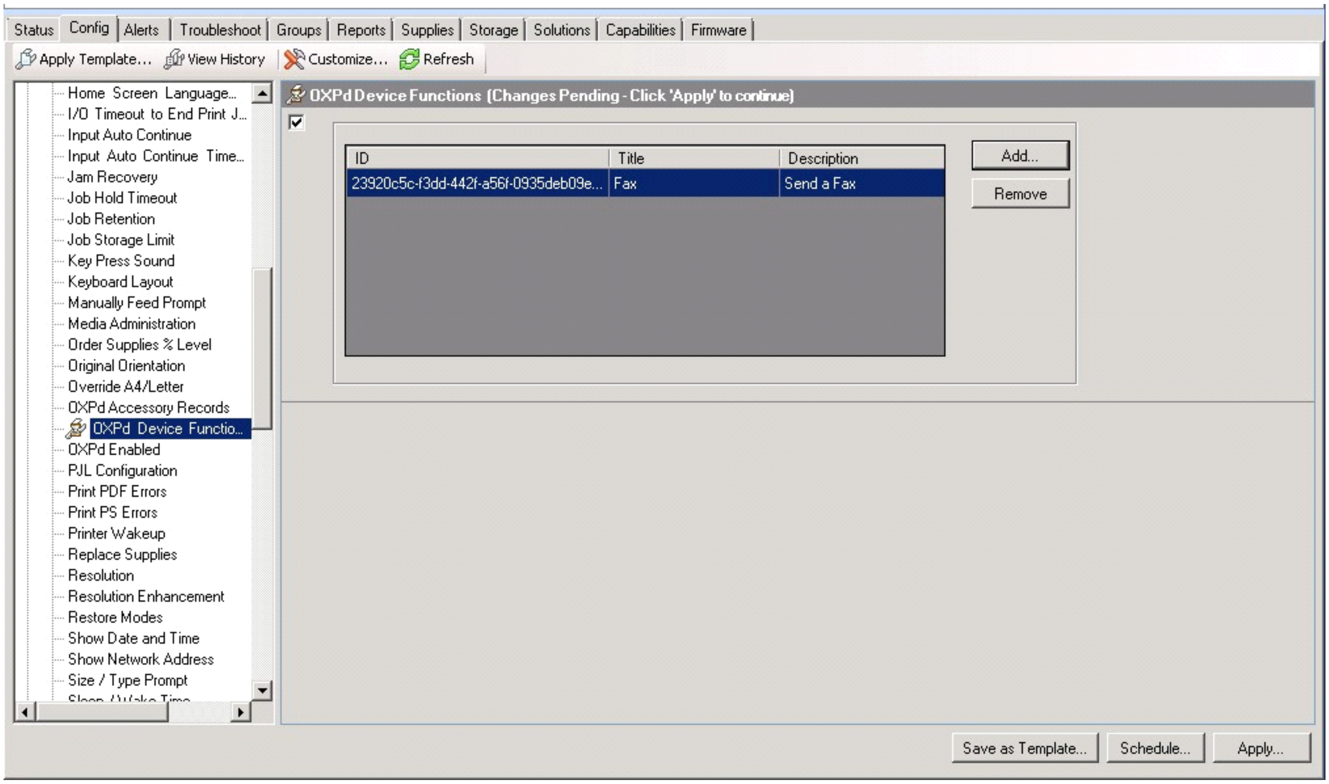
16. Click **OK**. The **Add OXPd Device Functions** page appears.



ID	Title	Description
23920c5c-f3dd-442f-a56f-0935deb09e...	Fax	Send a Fax

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).

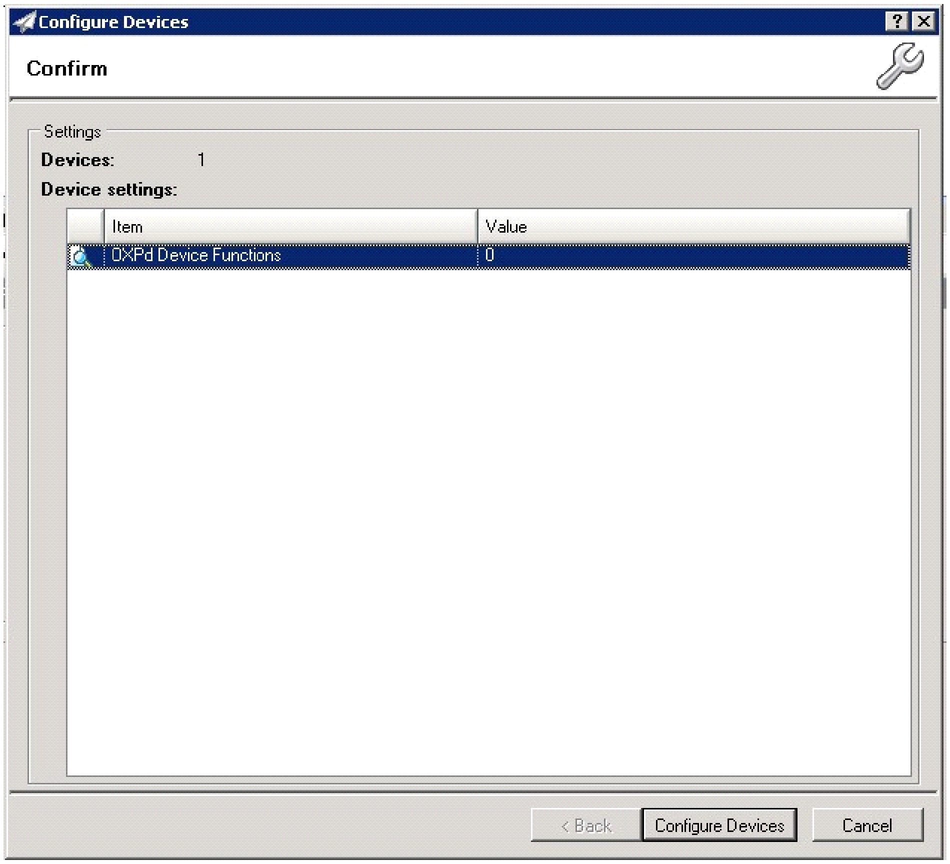


OXPd Device Functions (Changes Pending - Click 'Apply' to continue)

☑

ID	Title	Description
23920c5c-f3dd-442f-a56f-0935deb09e...	Fax	Send a Fax

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



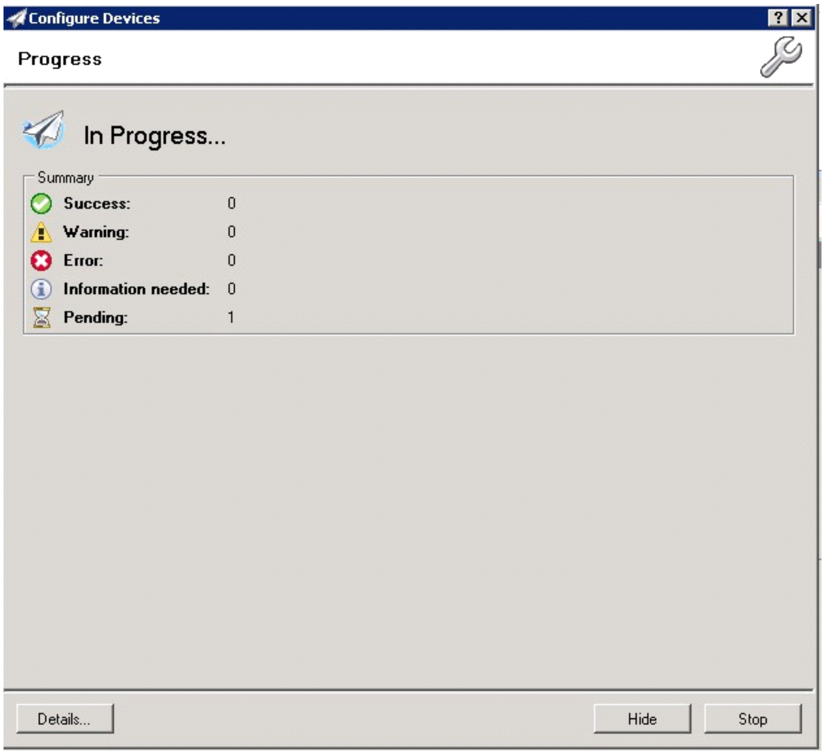
Settings

Devices: 1

Device settings:

Item	Value
OXPd Device Functions	0

19. Click the **Configure Devices** button. The **In Progress** page appears.

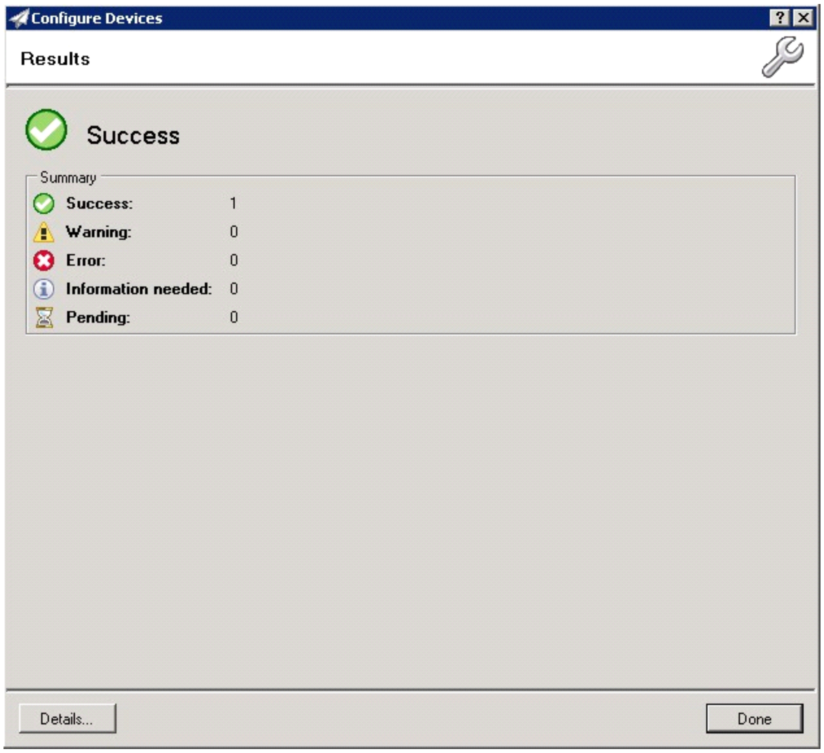


In Progress...

Summary

Success:	0
Warning:	0
Error:	0
Information needed:	0
Pending:	1

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



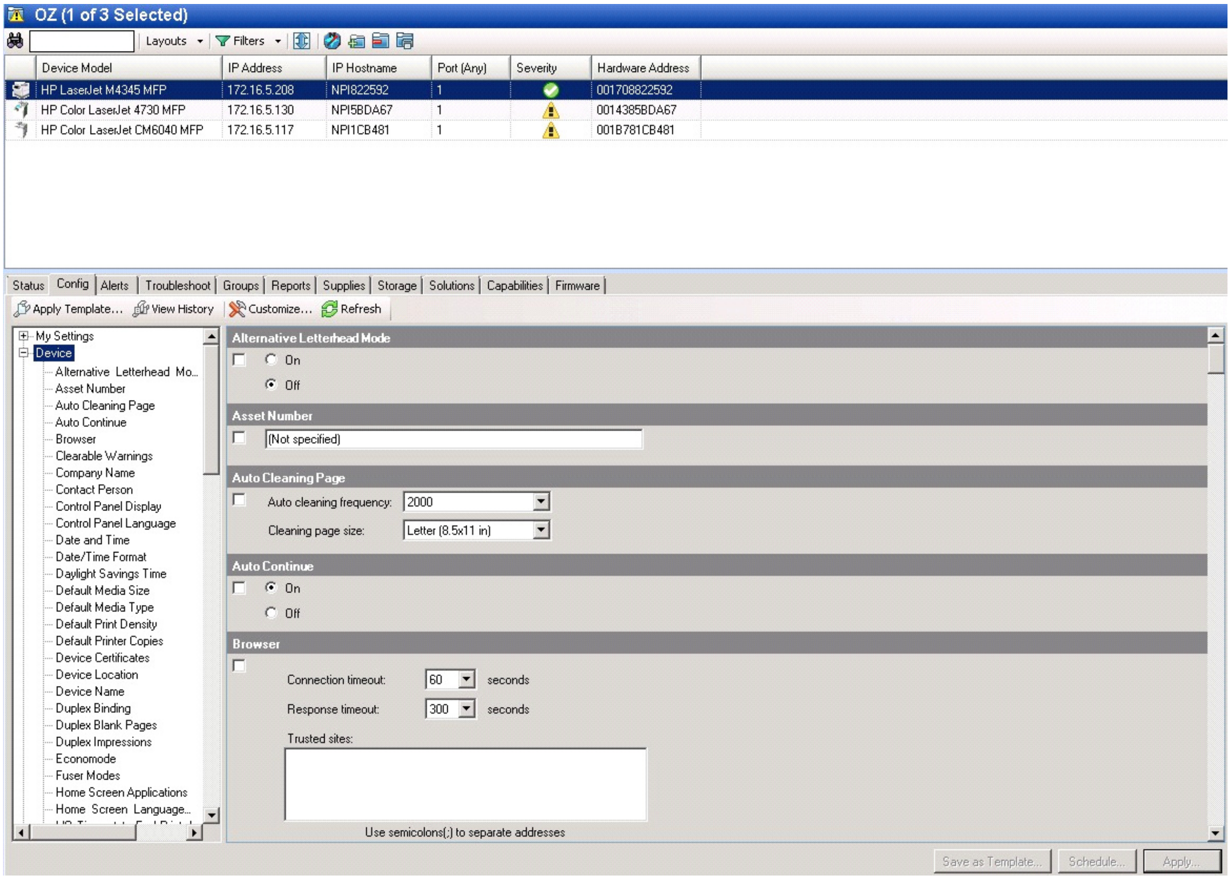
Success

Summary

Success:	1
Warning:	0
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** page, which defaults to the **Device** subset node.



OZ (1 of 3 Selected)

Device Model	IP Address	IP Hostname	Port (Any)	Severity	Hardware Address
HP LaserJet M4345 MFP	172.16.5.208	NPI822592	1	✓	001708822592
HP Color LaserJet 4730 MFP	172.16.5.130	NPI5BDA67	1	⚠	0014385BDA67
HP Color LaserJet CM6040 MFP	172.16.5.117	NPI1CB481	1	⚠	001B781CB481

Alternative Letterhead Mode

□ ○ On
● Off

Asset Number

□ (Not specified)

Auto Cleaning Page

□ Auto cleaning frequency: 2000

Cleaning page size: Letter (8.5x11 in)

Auto Continue

□ ● On
○ Off

Browser

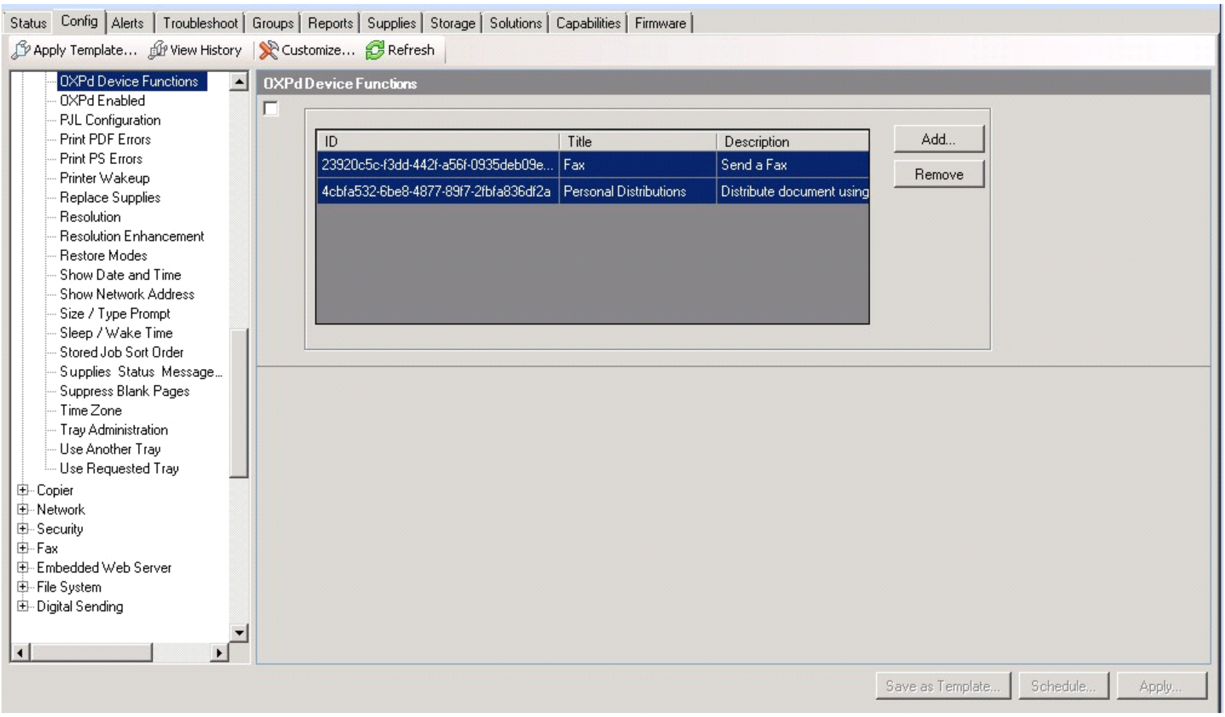
□ Connection timeout: 60 seconds

Response timeout: 300 seconds

Trusted sites:

Use semicolons(;) to separate addresses

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



OXPd Device Functions

ID	Title	Description
23920c5c-f3dd-442f-a56f-0935deb09e...	Fax	Send a Fax
4cbfa532-6be8-4877-89f7-2fbfa836df2a	Personal Distributions	Distribute document using

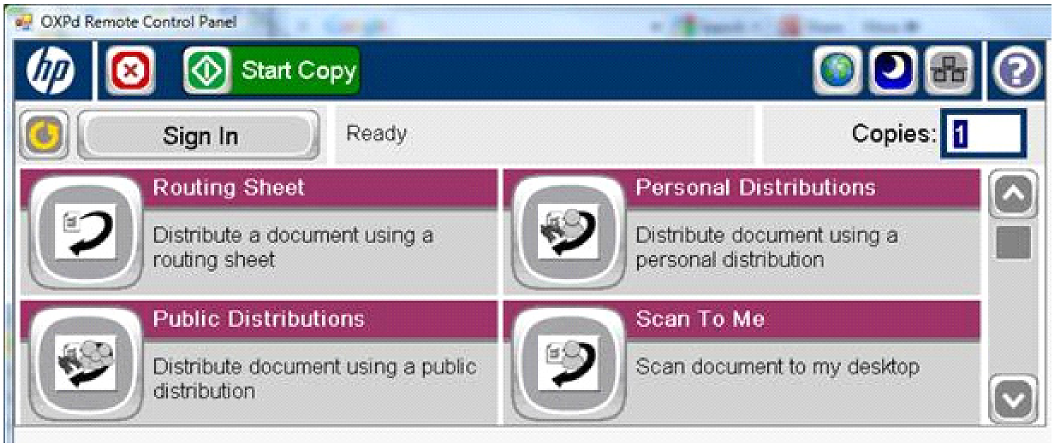
22. Test the buttons on the device panel to verify all functionality.

8 Testing

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.

8-1 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 Remote Control Panel
Start Copy
Sign In
Ready
Copies: 1
Routing Sheet
Distribute a document using a routing sheet
Personal Distributions
Distribute document using a personal distribution
Public Distributions
Distribute document using a public distribution
Scan To Me
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 HP CR administrator on-line help.

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 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 🏠 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.

8-2 Testing the Device Administrator user interface

To test the Device Administrator user interface, complete the procedure for Creating a group of devices (part 1) (39).

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
- 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.

A Configuring HP Pro Devices on a Remote OPS Server with HTTPS Support

This appendix describes the installation and configuration process for HP Pro devices on a remote OPS Server with HTTPS support, which is installed on a system remote from the HP CR server. This includes HTTPS support on a remote IIS server.

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.

This process includes the following steps:

NOTE: In these steps, *System A* represents the local system. *System B* represents the remote system.

A-1 Installing the HP CR Embedded Device Client on the local server

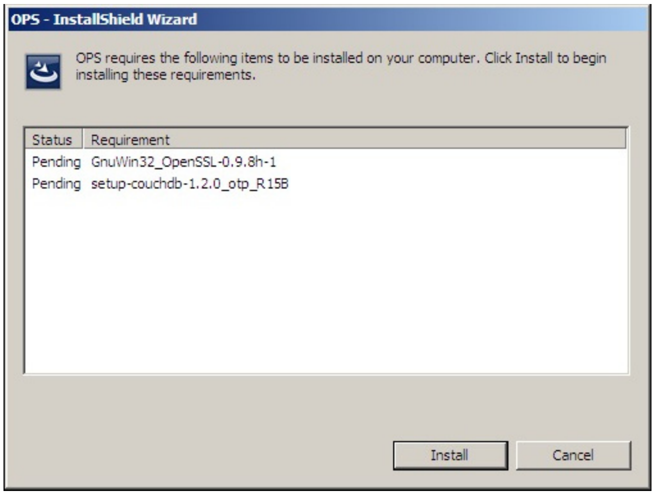
On the local system (System A) running the HP CR server, install the HP CR Embedded Device Client. See HP CR Embedded Device Client Installation (11) for more information.

NOTE: If you want HTTPS support with your remote OPS server installation, the OPS server must be installed on the system where the IIS server is installed. To use the HTTPS certificate, the OPS server must be installed on the IIS server.

A-2 Installing the OPS kit on the remote server

1. From the local server (System A), navigate to the `\Tools` folder on the remote server (System B).
2. Right-click and select **Run as Administrator**.
3. Run `setup.exe` for OPS on System B.
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`



OPS - InstallShield Wizard

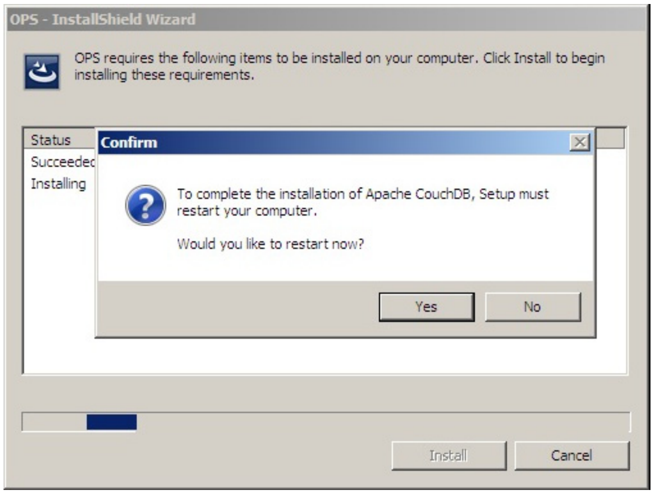
OPS requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	GnuWin32_OpenSSL-0.9.8h-1
Pending	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?



OPS - InstallShield Wizard

OPS requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status
Succeeded
Installing

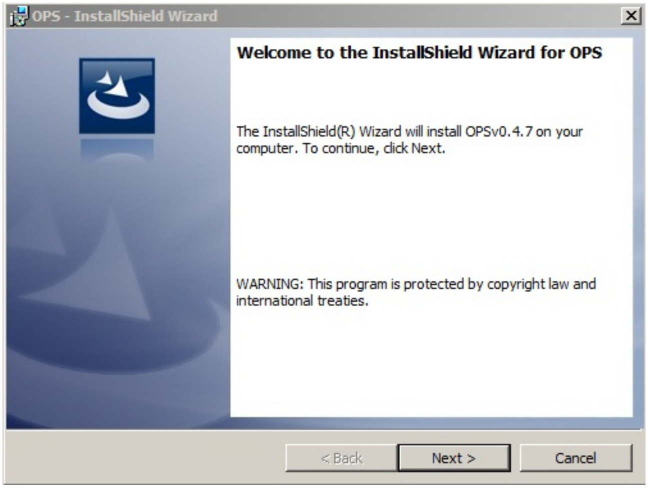
Confirm

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.

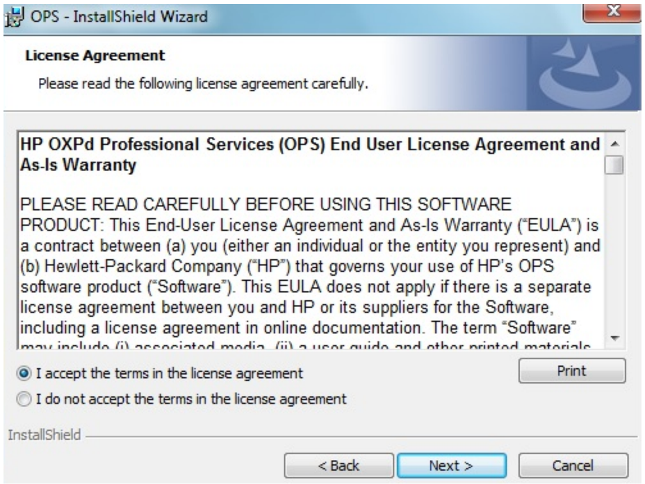


Welcome to the InstallShield Wizard for OPS

The InstallShield(R) Wizard will install OPSv0.4.7 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



License Agreement

Please read the following license agreement carefully.

HP OXPd Professional Services (OPS) End User License Agreement and As-Is Warranty

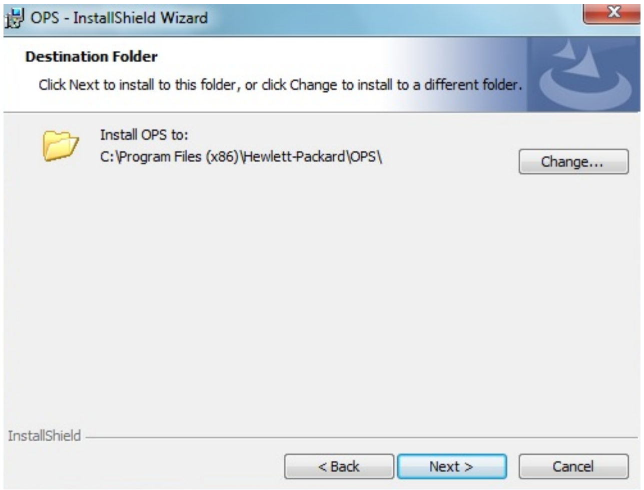
PLEASE READ CAREFULLY BEFORE USING THIS SOFTWARE PRODUCT: This End-User License Agreement and As-Is Warranty ("EULA") is a contract between (a) you (either an individual or the entity you represent) and (b) Hewlett-Packard Company ("HP") that governs your use of HP's OPS software product ("Software"). This EULA does not apply if there is a separate license agreement between you and HP or its suppliers for the Software, including a license agreement in online documentation. The term "Software" may include (i) associated media, (ii) a user guide and other printed materials

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

8. Select **I accept the terms in the license agreement** and click **Next**.

   The **Destination Folder** screen appears.

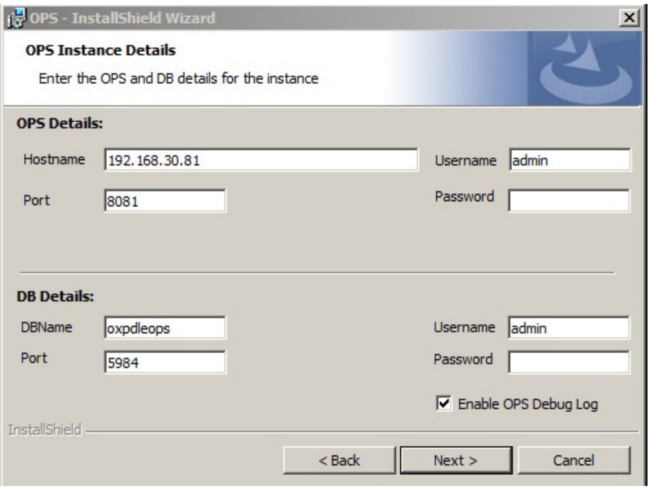


Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install OPS to:
C:\Program Files (x86)\Hewlett-Packard\OPS\

9. Click **Next**. The **OPS Instance Details** screen appears.



OPS - InstallShield Wizard

OPS Instance Details

Enter the OPS and DB details for the instance

OPS Details:

Hostname 192.168.30.81

Username admin

Port 8081

Password

DB Details:

DBName oxpdleops

Username admin

Port 5984

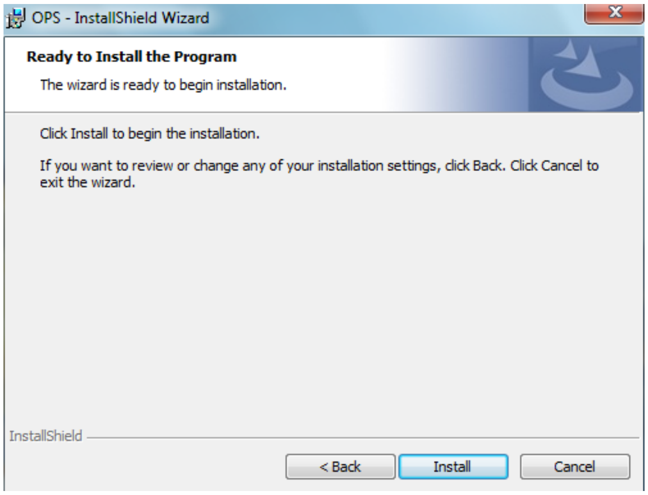
Password

☑ Enable OPS Debug Log

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.



OPS - InstallShield Wizard

Ready to Install the Program

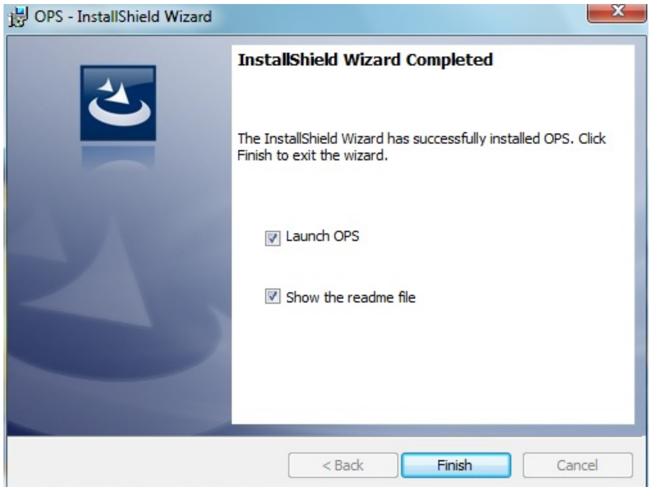
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

13. Click **Install**.

14. The **OPS InstallShield Wizard Completed** screen appears.



OPS - InstallShield Wizard

InstallShield Wizard Completed

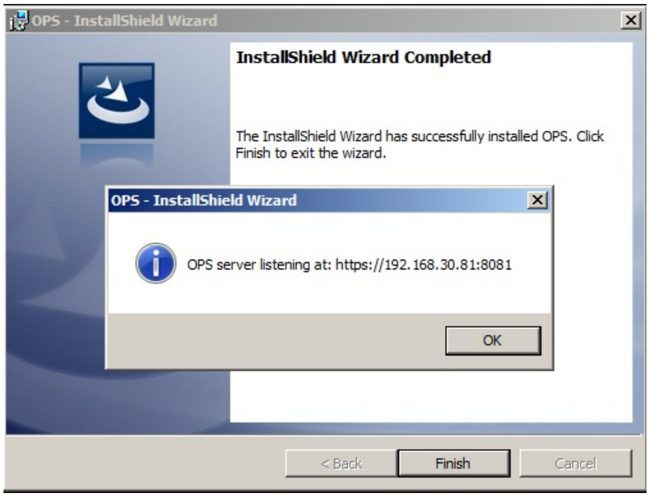
The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.

☑ Launch OPS

☑ Show the readme file

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 - InstallShield Wizard

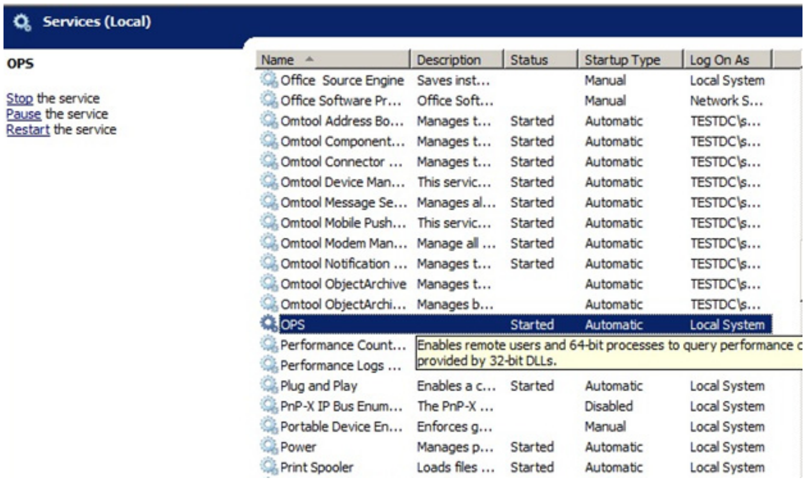
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.

OPS - InstallShield Wizard

OPS server listening at: https://192.168.30.81:8081

Click **OK**. OPS now appears as a Windows service.



Services (Local)

OPS

Stop the service
Pause the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Office Source Engine	Saves inst...		Manual	Local System
Office Software Pr...	Office Soft...		Manual	Network S...
Omtool Address Bo...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Component...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Connector ...	Manages t...	Started	Automatic	TESTDC\s...
Omtool Device Man...	This servic...	Started	Automatic	TESTDC\s...
Omtool Message Se...	Manages al...	Started	Automatic	TESTDC\s...
Omtool Mobile Push...	This servic...	Started	Automatic	TESTDC\s...
Omtool Modem Man...	Manage all ...	Started	Automatic	TESTDC\s...
Omtool Notification ...	Manages t...	Started	Automatic	TESTDC\s...
Omtool ObjectArchive	Manages t...		Automatic	TESTDC\s...
Omtool ObjectArchi...	Manages b...		Automatic	TESTDC\s...
OPS		Started	Automatic	Local System
Performance Count...	Enables remote users and 64-bit processes to query performance c			
Performance Logs ...	provided by 32-bit DLLs.			
Plug and Play	Enables a c...	Started	Automatic	Local System
PnP-X IP Bus Enum...	The PnP-X ...		Disabled	Local System
Portable Device En...	Enforces g...		Manual	Local System
Power	Manages p...	Started	Automatic	Local System
Print Spooler	Loads files ...	Started	Automatic	Local System

A-3 Exporting the OPS server certificate

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**.
6. The **Certificate Export** wizard appears. Select **Next**.
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**.

A-4 Importing the OPS certificate into the device EWS

1. Open and log into the EWS of the Pro Device.
2. On the **Network** tab select **Advanced settings > Certificates**.
3. Select **Import > Choose File**.
4. Browse to the location where the OPS certificate was saved and select **Open** and then **Finish**.

A-5 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 Step 10 of Installing the OPS kit on the remote server (81).
5. Enter the **OPS server URL** you want to register. For example, `123.456.78.9:8765`.
6. Enter the **username** and **password** for the OPS server.

NOTE: The OPS server URL and username can be obtained above from Steps 8 and 9 in Installing the OPS kit on the remote server (81). All devices will be using this Certificate for HTTPS communication.

7. The following message appears:

```
OPS Registered successfully
```

Your remote OPS server is now installed. See Creating a group of devices (part 1) (39) for more information on creating device groups.

A-6 HTTPS support using the OPS-created certificate

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.

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**.

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.

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**.

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)**.

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>
   ```
3. This OPS Servername is based on the value noted from Step 10 of Installing the OPS kit on the remote server (81).

NOTE: XML files can be edited using Microsoft Notepad.

4. Save the file.

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>
   ```
3. This OPS Servername is based on the value from noted from Step 10 of Installing the OPS kit on the remote server (81).
4. Save the file and reset IIS.

A-7 Troubleshooting

If you try to query the device when the OPS and Intelligent Device Client are remote from the HP CR server, an error message appears.

There are several workarounds:

- As the Best Practice, allow the traffic to Certificate Authorities to validate the certificates. If this is not possible, the network rejects the requests and returns an error message indicating that the host cannot be reached.
- As an alternative, you can configure ASP.NET to not check the certificates. To do so, you need to edit the `aspnet.config` files in these two locations:
  - `c:\Windows\Microsoft.NET\Framework64\v2.0.50727`
  - `c:\Windows\Microsoft.NET\Framework\v2.0.50727`

  At both locations, add the tag `<generatePublisherEvidence enabled="false"/>` to the runtime section, as follows:

  ```
  <runtime>
  <generatePublisherEvidence enabled="false"/>
  </runtime>
  ```

  Then save the files and reboot the server.
- Also, there is another check for certificates controlled by Group Policy. If the server is not regularly updated, the server may force an attempt to update, adding another delay. There is a Microsoft Support article detailing this situation and how to change the setting.