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

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

Edition: September 2012

Legal notices

Printed in the US

Revision history

Table 1 Revisions

Date	Edition	Revision
September 2012	1	Version 1.2.0

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

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

This section describes:

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

1-1 Embedded Device Client for HP OXPd overview

Embedded Device Client for HP OXPd brings the versatile document routing capabilities of HP CR to supported HP devices running OXPd SDK library v1.6.x as well as a limited set of devices running OXPd SDK library v1.4.x. These capabilities are founded in Distribution Rule technology.

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

Figure 1-1 HP CR Scanning Features on the HP Device Running Embedded Device Client for HP OXPd

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

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

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 (6) 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 the HP CR folder via HTTP/HTTPS protocol. The HP CR server picks up the scanned document from the network folder, processes it and delivers it to the intended folder.	No	
Fax	This option allows the user to do a walk-up fax. The user enters the fax number and can additionally add a cover page to fax. The device scans and delivers the document to the HP CR server via HTTP/HTTPS protocol. The HP CR server sends the fax to the intended recipients.	No	
Scan to My Files	The user selects Scan to My Files button and logs in to the device. The device scans and delivers the document to the HP CR server (via HTTP/HTTPS protocol) where it is processed and distributed to the My Files section of the user End User Interface client.	Yes	All jobs scan.

Feature	Description	Login Required	Notes
Nested Buttons	The Nested Buttons feature provides the ability to configure one top-level button that all other HP CR buttons will display under, minimizing the front panel home screen real estate. For example, one button can be configured and labeled “HP CR.” This button would be the only HP CR button to display on the home screen. Pressing this button would then display any other enabled buttons (such as Routing Sheets, Personal Distributions, etc.).	No	

1-1-1 Main components of the environment

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

- **HP CR Server** - The HP CR server is the main back-end server for processing and routing documents.

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

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

1-1-2 Installation components

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

Table 2 Description of installation components with locations and functions

Component	Location	Function
Embedded Device Client for HP OXPd Install	`\HP\HPCR\Clients`	The setup contains the setup.exe file for both HP OXPd v1.4 and HP OXPd v1.6. Use this file to install the Embedded Device Client for HP OXPd.
Embedded Device Client for HP OXPd Configuration Manager	Devices node in the HP CR Server Administrator	The Device Client Configuration node is a management tool installed with the HP CR Server Administrator, and is used to manage settings and options that will be available on the HP MFP Device.

1-1-3 Document workflow

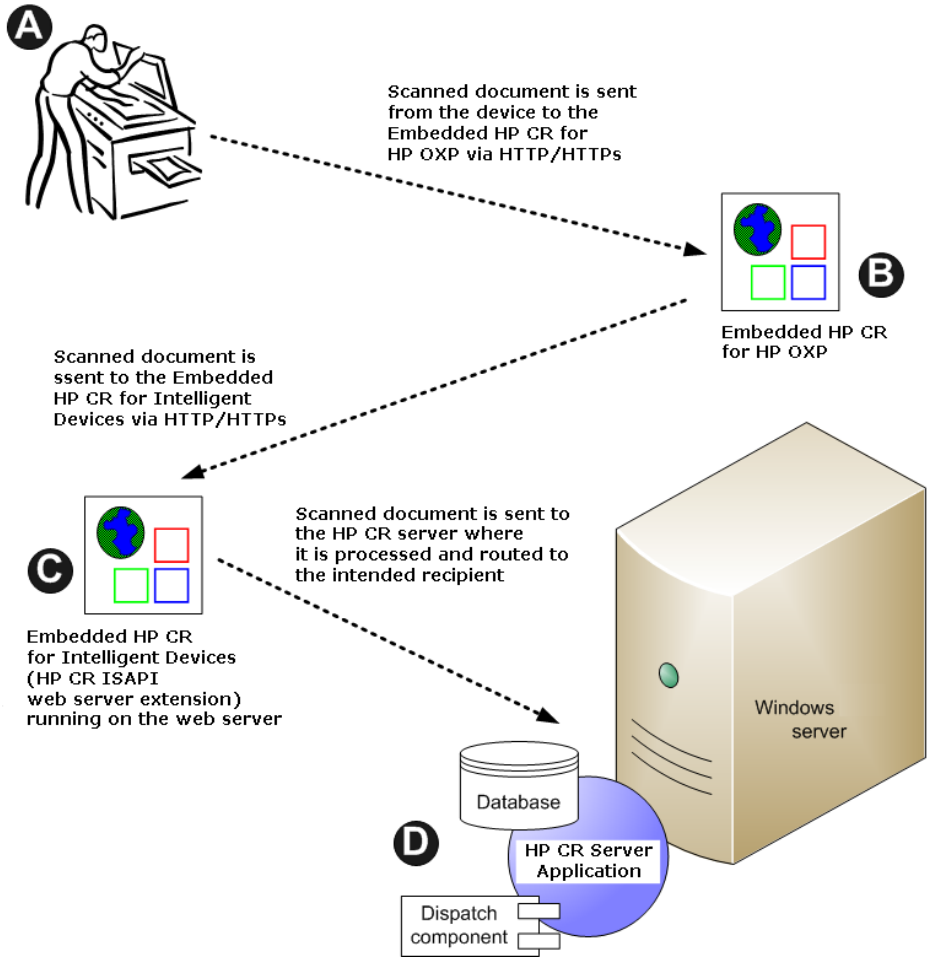
The workflow that moves a document from the device to its final destination involves the user, the device, the Embedded Device Client for HP OXPd, Embedded HP CR for Intelligent Devices (HP CR ISAPI web server extension), and the HP CR server. An understanding of this workflow can be helpful in troubleshooting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

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

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

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

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



A-The user selects an HP CR scanning feature and scans a document.

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

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

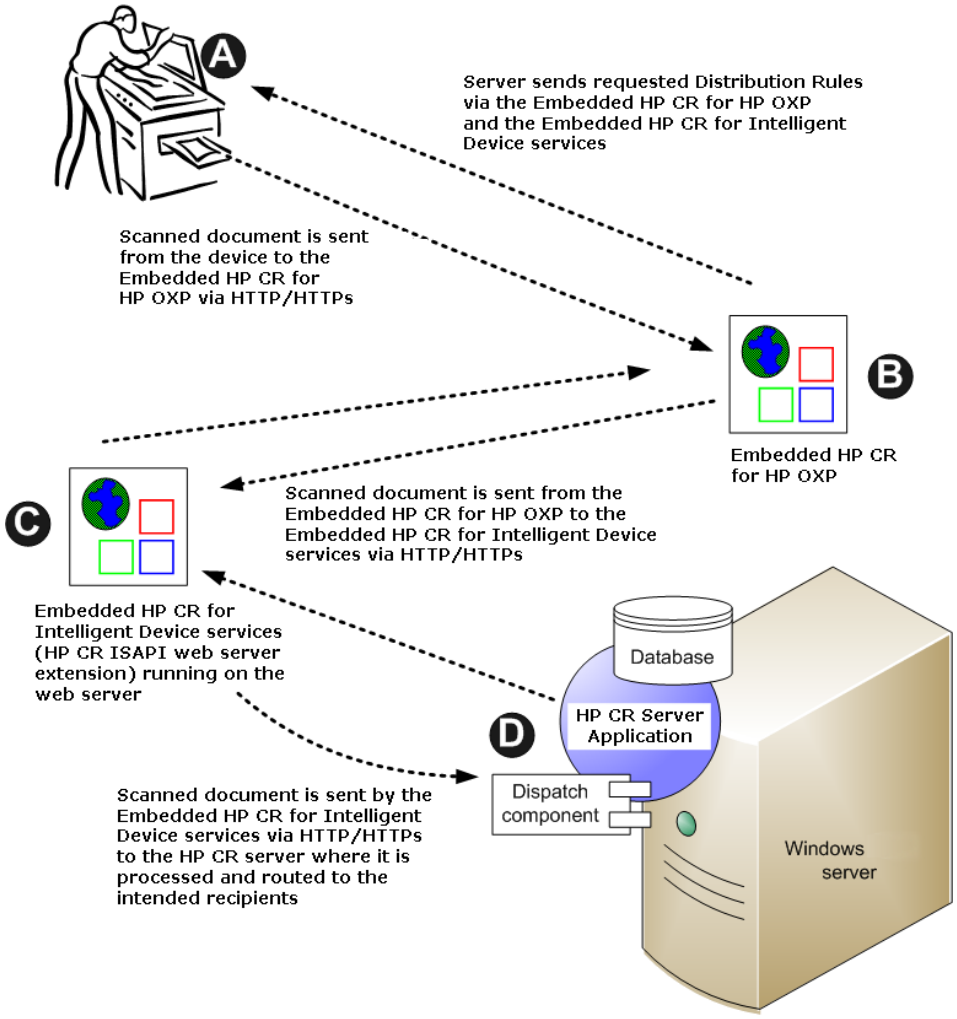
D-The Dispatch component applies rules to the message, and the server processes the message accordingly.

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

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

The Embedded Device Client for HP OXPd then submits a request to Embedded HP CR for Intelligent Devices (HP CR ISAPI web server extension) which retrieves the data from the HP CR server and supplies it to the Embedded Device Client for HP OXPd. As soon as the Embedded Device Client for HP OXPd returns the data to the device, the basic workflow resumes.

Figure 1-3 Workflow for Personal Distributions and Public Distributions



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

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

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

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

1-1-4 Deploying Embedded Device Client for HP OXPd

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

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

2. Install the Embedded Device Client for HP OXPd. See Installing Embedded Device Client for HP OXPd v1.6 (9) or Installing Embedded Device Client for HP OXPd v1.4 (10).
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 administrator on-line help.
6. Test the HP CR scanning features on the device. Refer to Section 6: Testing (71).
7. Troubleshoot the setup if necessary. Refer to the HP CR administrator on-line help.

1-2 Basic requirements

1-2-1 Supported devices

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

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

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

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

NOTE: All LaserJet models listed here are part of the “mfp series”. Other LaserJet models that are part of the “printer series” do not have the scanning capabilities required to support Embedded Device Client for HP OXPd.

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

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

1-2-2 Server requirements

Embedded Device Client for HP OXPd requires:

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

1-2-3 Device authentication requirements

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

The types of authentication are:

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

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

1-2-4 Configuring to use HTTPS

In order to use HTTPS protocol communication when sending documents from the device to the HP CR server, you must create a CA Certificate using Microsoft Certificate Services and enable Secure Socket Layer (SSL). You must create this certificate before installing the Embedded Device Client for HP OXPd. This configuration is necessary to allow administrators to export the file and install it on the device to enable HTTPS communication.

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

- The administrator will need to create and export the certificate for the Web server as a file named “WebServer.cer” and copy it to the Certificate folder created during the Embedded Device Client for HP OXPd install.
- During the registration process for the OXPd application onto the device, the webserver.cer will be installed into the device.

NOTE: No error will be generated if the file does not exist,
It will not be possible to configure the device for HTTPS until that file has been installed into the device.

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

1-2-5 Custom configuration

The HP CR Server Administrator Devices node gives the administrator the ability to manage devices and create groups of devices with customized buttons. Refer to Creating a group of devices (29).

1-3 On-line help and related documentation

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

2 Embedded Device Client for HP OXPd installation

This section describes:

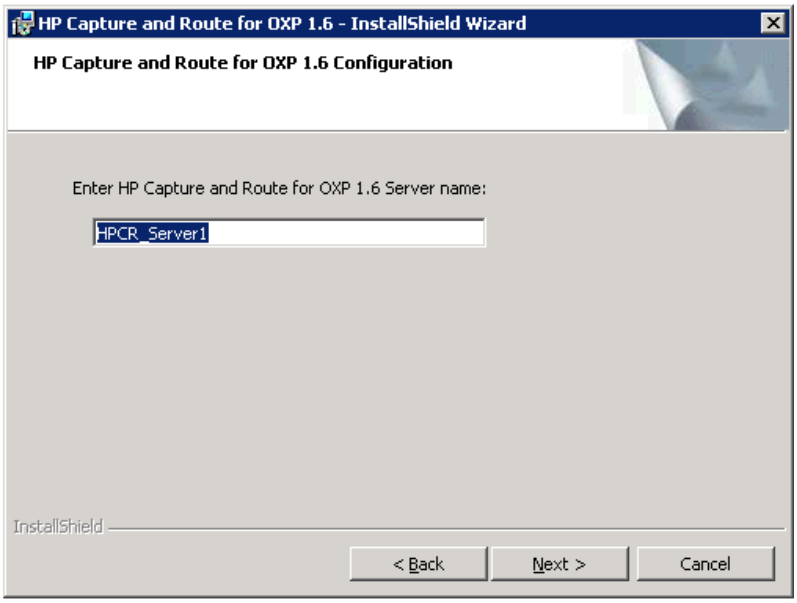
See also Section 4: Required configuration (29), Section 6: Testing (71), and the HP CR administrator on-line help (for additional information including optional configurations, testing, and troubleshooting).

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

1. Logon to the system running the HP CR server using an account that belongs to the local Administrators group.
2. Navigate to the folder:

   `C:\Program Files (x86)\HP\HPCR\Clients\HPOXP1.6` and run `setup.exe`.

   The InstallShield wizard launches with the **Welcome** message.
3. Click **Next**. The **Destination Folder** page opens.
4. Keep the default location and click Next. The **HP Capture and Route for OXP 1.6** InstallShield Wizard opens.



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

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

2-2 Installing Embedded Device Client for HP OXPd v1.4

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

   Navigate to the folder:

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

   If you are installing on a non-default drive:

   a Open a command prompt window (run as Administrator).

   b Navigate to the HP CR Clients directory:

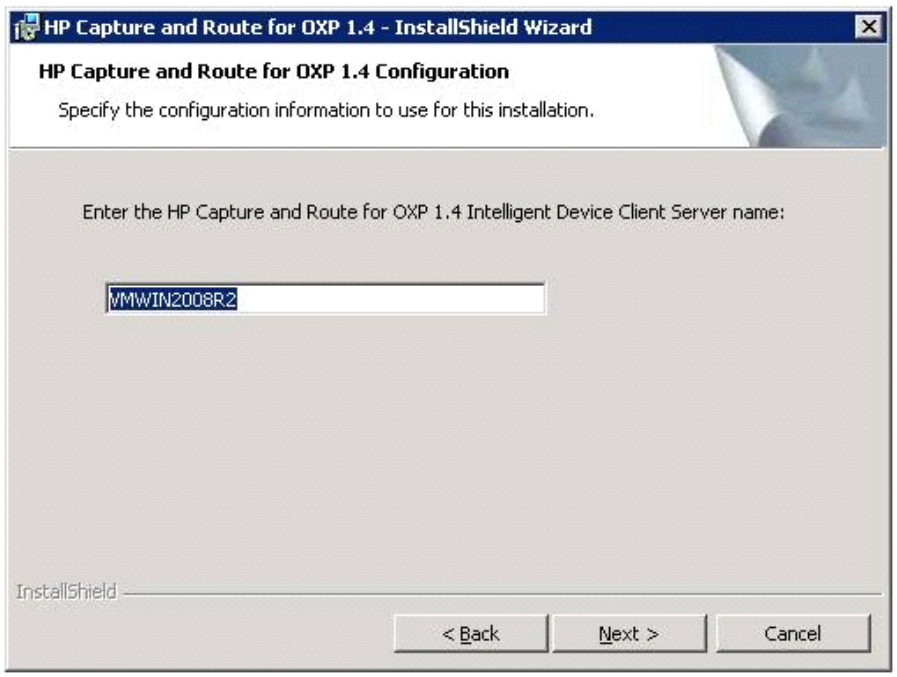
   `\\HP\HPCR\Clients\HPOXP1.4`

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

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

   The Device Client will be installed on the D drive.
3. The InstallShield wizard launches with the **Welcome** page. Click **Next**.

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



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

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

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

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

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

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

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

3 Configuration for HTTPS support

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

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

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

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

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

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

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

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

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

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

The remainder of this section provides procedures for:

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

3-1-2 Downloading the MakeCert executable

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

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

3-1-3 Creating the certificate

1. Open a command prompt and navigate to the directory where you saved the makecert executable (makecert.exe) on your local computer (typically on the C drive).
2. Run the following command (as Administrator):

   ```
   makecert.exe -r -pe -n "CN=fully_qualified_domain_name_of_iis_server" -b
   01/01/2006 -e 01/01/2013 -ss my -sr localMachine -sky exchange -sp
   "Microsoft RSA SChannel Cryptographic Provider" -sy 12
   "fully_qualified_domain_name_of_iis_server.cer"
   ```

   fully_qualified_domain_name_of_iis_server should be in this format:
   `servername.domain.com`

NOTE: You cannot copy and paste the command text above due to formatting issues. This text is available to copy in the Embedded Device Client for HP OXPd section of the 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.

3-1-4 Installing the certificate to Internet Information Services (IIS)

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

1. Select and right-click the certificate.
2. Select **Install Certificate**. The **Certificate Import** wizard is displayed.
3. Select **NEXT**.
4. Select **Place all certificates in the following store** and select **BROWSE**.
5. Select **Trusted Root Certification Authorities** and select **OK**.
6. You will be prompted with a security warning:

   You are about to install a certificate from a certification authority(CA) claiming to represent…
   Do you want to install this certificate?

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

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

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

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

    `C:\Program Files (86)\HP\OXP1.6\Certificate`
12. In the **File Name** field, enter **WebServer.cer with DER Encoded Binary X.509 (*.cer)** as the **Save Type**.
13. Click **Save** and then **Next**. The **Completing the Certificate Export** wizard opens.
14. Click **Finish**.
15. When a message appears stating that the export was successful, click **OK**.

3-1-6 Creating an SSL binding

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

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

1. Open the IIS Manager.
2. Expand **Local Machine > Default Web Site** and select **OXP1.6** (or **OXP1.4**).
3. Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.
4. Expand **Local machine > Default Web Site** and select **WebAPI**.
5. Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.

3-1-8 Verifying the SSL binding

1. Open the IIS Manager.
2. Expand **Local Machine > Default Web Site** and select **WebAPI**.
3. Click on **Browse *:443 (HTTPS)** under **Manage Application/Browse Application** (located at the top right corner of the IIS dialog).

   You will see this message: *There is a problem with this web site's security certificate.*

NOTE: This message is expected and safe to ignore.

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

3-1-9 Enabling directory browsing in IIS

1. Open the IIS Manager.
2. Expand **Local Machine > Default Web Site** and select **OXP1.6** (or **OXP1.4**).
3. Double-click on **Directory browsing**.
4. In the right **Actions** field, select **ENABLE**.
5. Expand **Local Machine > Default Web Site** and select **WebAPI**.
6. Double-click on **Directory browsing**.
7. In the right **Actions** field, select **ENABLE**.

3-1-10 Verifying HTTPS browsing

1. Open the IIS Manager.
2. Expand the **Default Web Site**.
3. Expand **OXP v1.6** (or **OXP v1.4**).
4. Select the **Configuration** folder.
5. In the actions pane, select **Browse*:443(https)**.
6. Select **Continue to this website (not recommended)**.
7. Verify that the local page is displayed.

   For HP OXPd v1.6:
   `.../OXP1.6/Configuration/`

   For HP OXPd v1.4:
   `.../OXP1.4/Configuration/`
8. In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
9. In the actions pane, select **Browse*:443(https)**.
10. Select **Continue to this website (not recommended)**.
11. Verify that the localhost page is displayed:

    `.../WebAPI/`
12. Select **Continue to this website (not recommended)**.

3-1-11 Editing the OmISAPIU.xml file

1. Navigate to the following path.

   `C:\Program Files (x86)\HP\HPCR\WebAPI\WebAPI\Scripts`

2. In OmISAPIU.xml, find the FileTransfer node. Replace the IP address with the fully qualified domain name. Also, change `http` to `https`.

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

NOTE: XML files can be edited using Microsoft Notepad.

3. Save the file.

3-1-12 Editing the Bootstrap.xml file

1. Navigate to the following path.

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

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

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

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

3. Save the file.
4. Reset IIS.

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

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

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

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

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

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

This section provides procedures for:

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

3-2-2 Downloading the MakeCert executable

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

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

3-2-3 Running the MakeCert executable and creating the certificate

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

   ```
   makecert.exe -r -pe -n "CN=fully_qualified_domain_name_of_iis_server" -b
   01/01/2006 -e 01/01/2013 -ss my -sr localMachine -sky exchange -sp
   "Microsoft RSA SChannel Cryptographic Provider" -sy 12
   "fully_qualified_domain_name_of_iis_server.cer"
   ```

   fully_qualified_domain_name_of_iis_server should be in this format:
   `servername.domain.com`

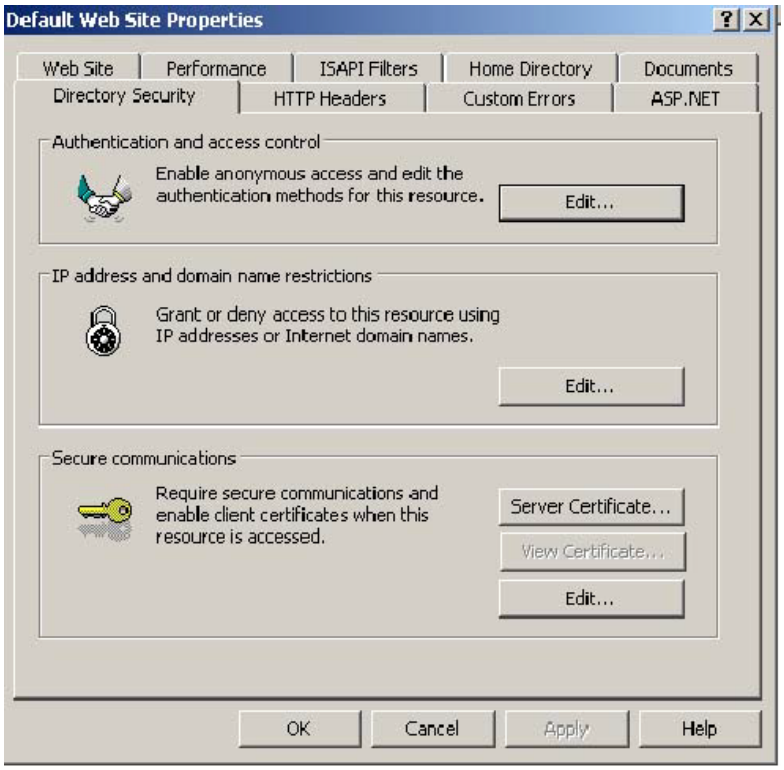
NOTE: You cannot copy and paste the command text above due to formatting issues. This text is available to copy in the Embedded Device Client for HP OXPd section of the On-line help for the administrator. If you key in the command text, note that there is a space at the end of the first three lines shown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

3-2-4 Exporting the certificate

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

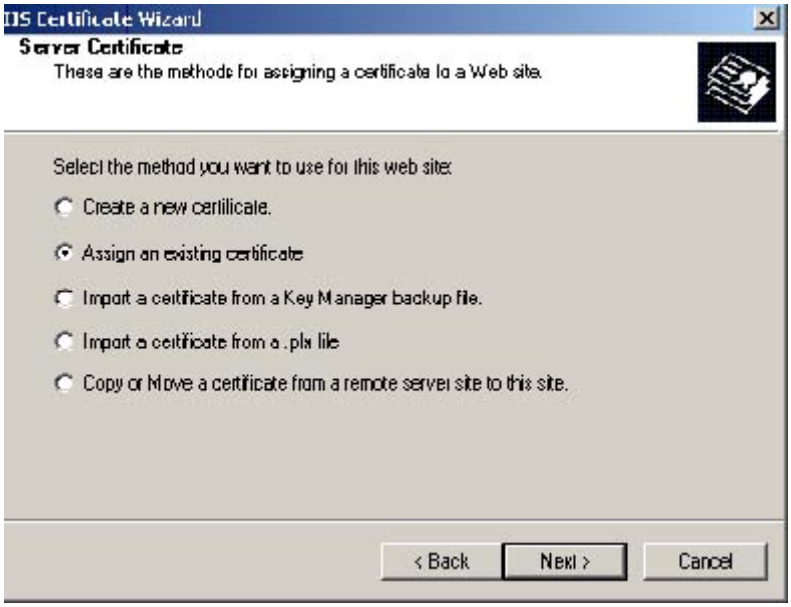
Using the Web Server Certification wizard:

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

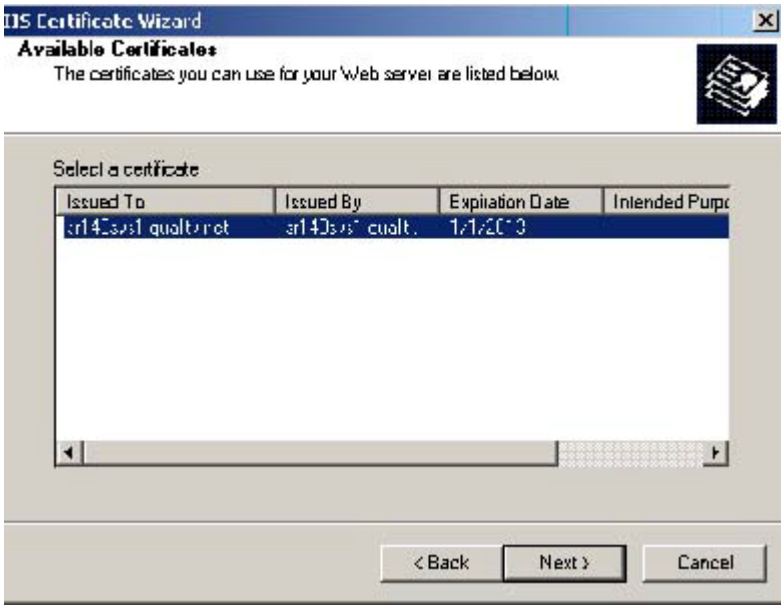


2. Click the **Server Certificate** button. The **Welcome to the Web Server Certification Wizard** page is displayed.

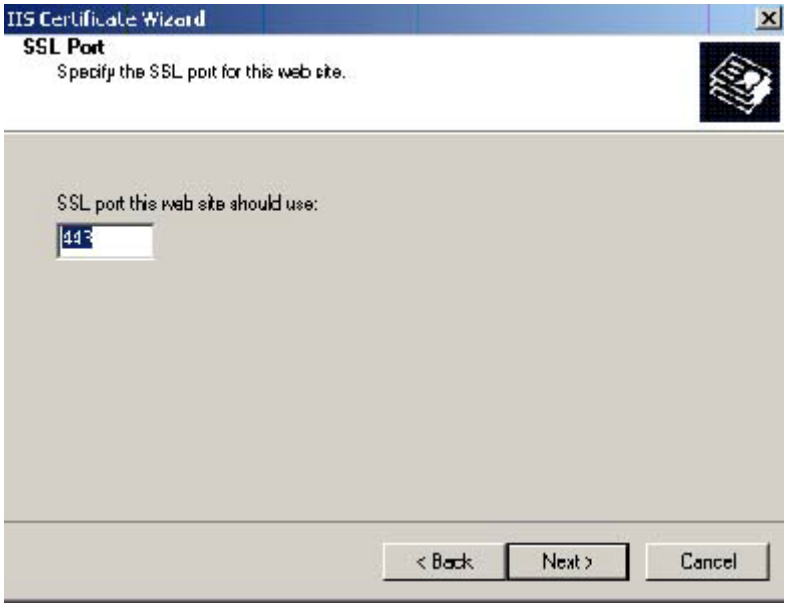
3. Click **Next**. The **IIS Certification Wizard** is displayed.



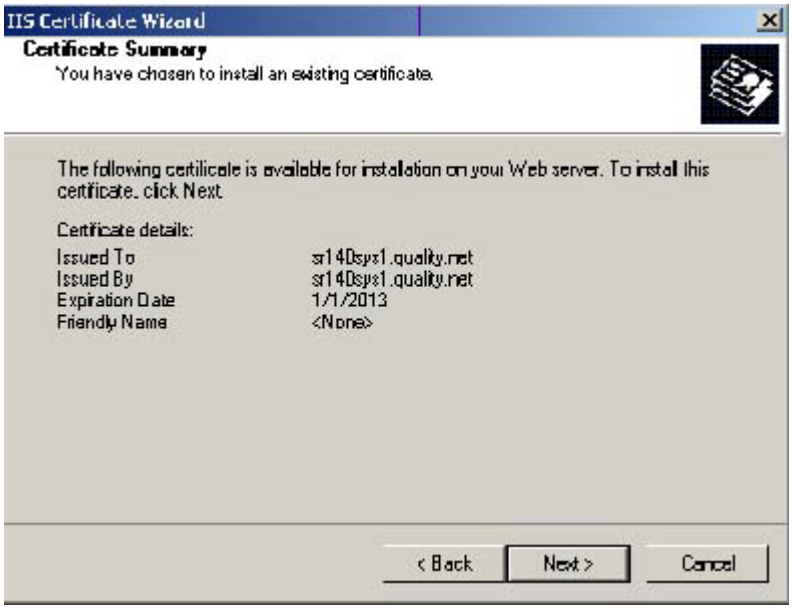
4. Select **Assign an existing certificate**. Click **Next**. The certificate created using MakeCert.exe is displayed.



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

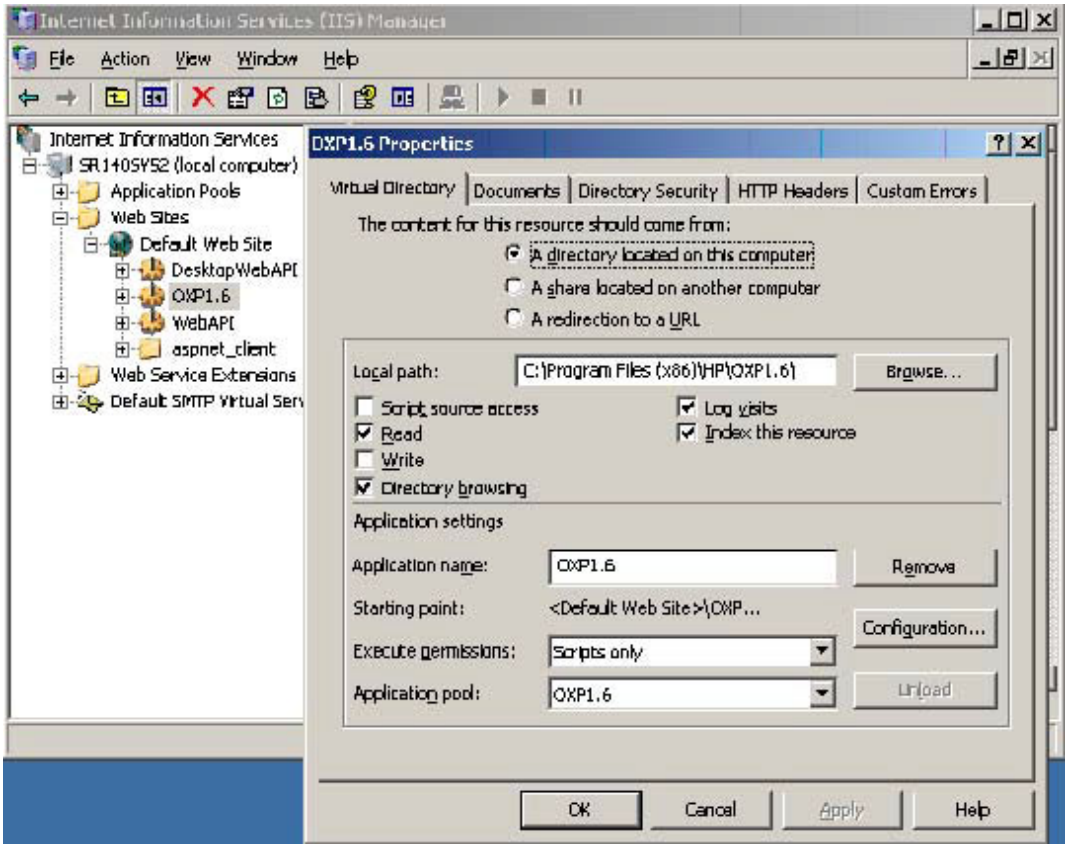


6. The port selected should be **443**. Click **Next**. The **Certificate Summary** is displayed.

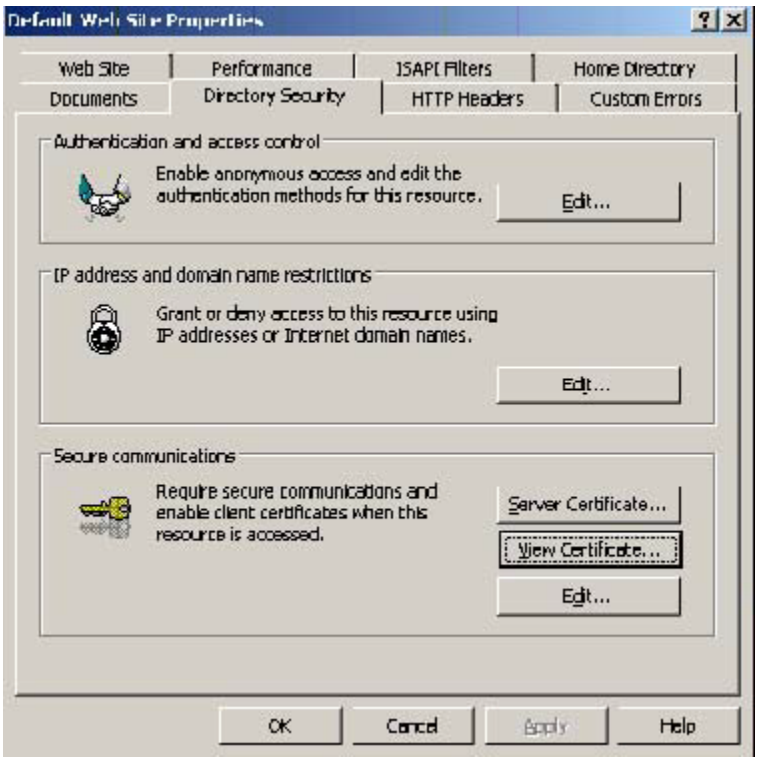


7. Click **Next**. A message indicates that the Web Server Certificate wizard is completed.
8. Click **Finish**. You are returned to the **Directory Security** page.
9. Export the certificate:
   - **a** Open IIS\local machine and navigate to the **Default Web Site** node.
   - **b** Select web site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

c Right-click and select **Properties**.

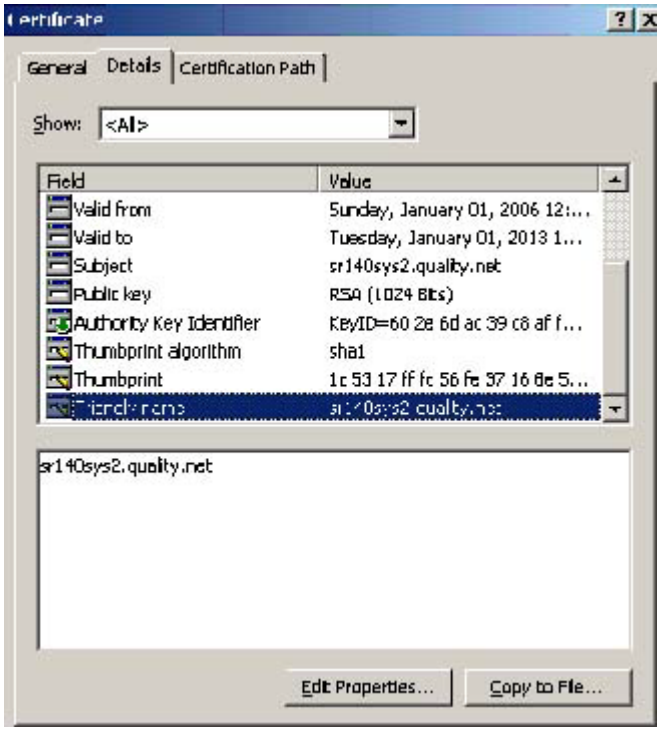


d Click the **Directory Security** tab.



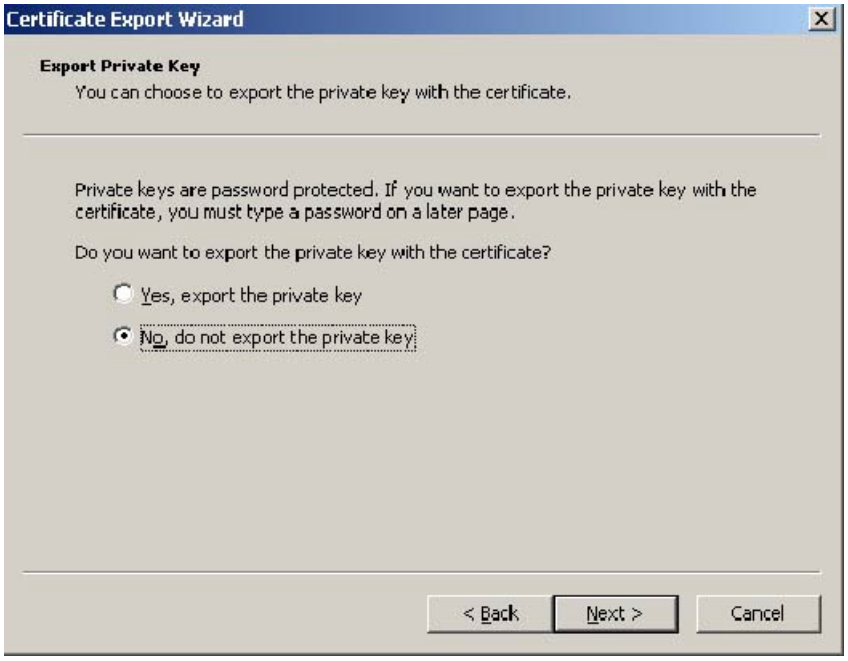
e In the **Secure communications** section, click the **View Certificate** button.

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

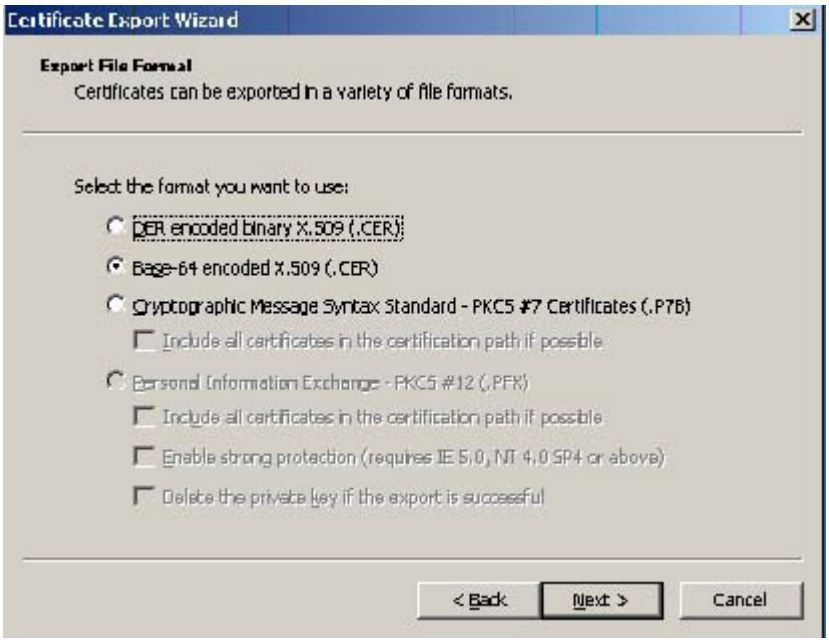


g Click the **Copy to File** button. The **Welcome to the Certificate Export Wizard** screen is displayed.

h Click **Next**. The **Export Private Key** page is displayed.



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



j Select **Base-64 encoded x.509 (CER)**. Click **Next**.

k Browse to this location.

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

l Enter the file name as:

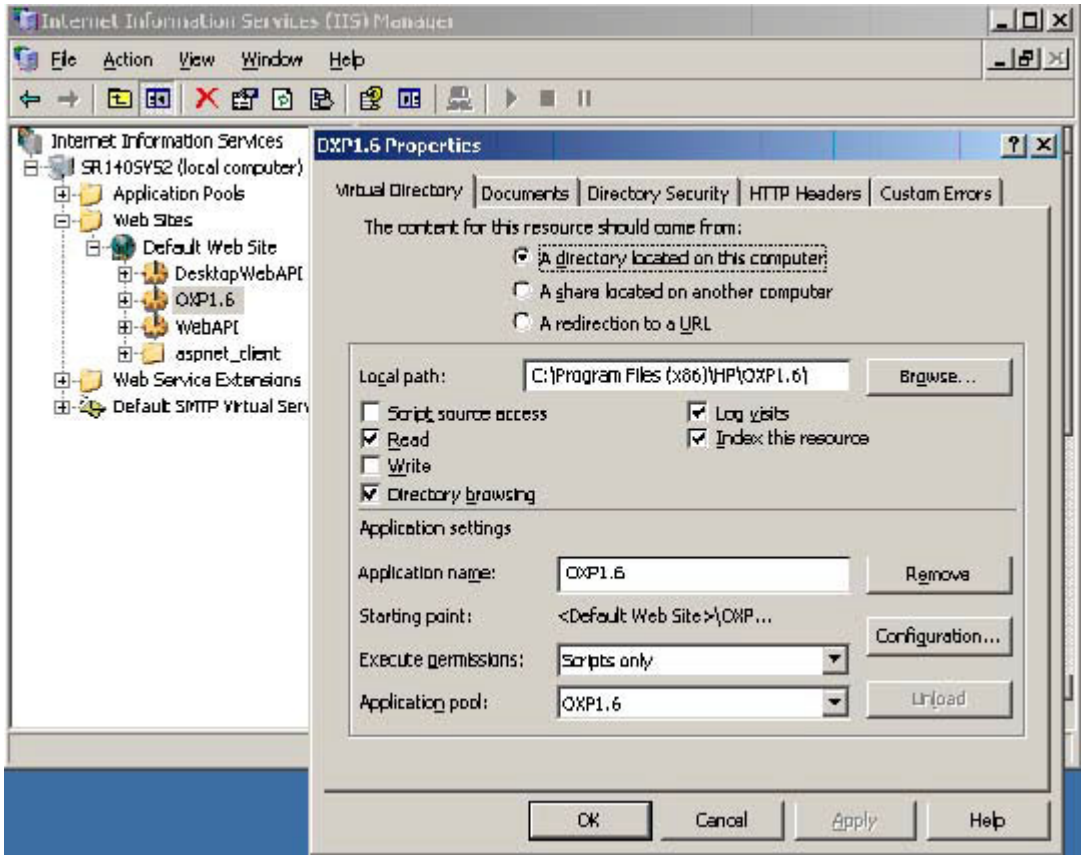
`Webserver.cer`

m Click **Save**. A message indicates the export was successful. Click **OK**.

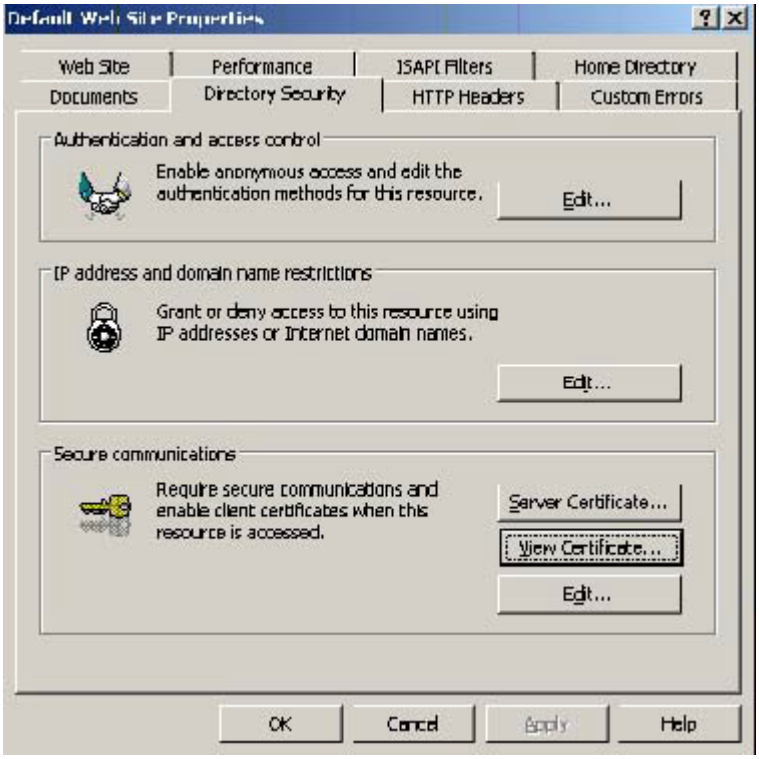
n Click **Finish** to exit the Certificate Export wizard.

3-2-5 Requiring SSL for Web Sites

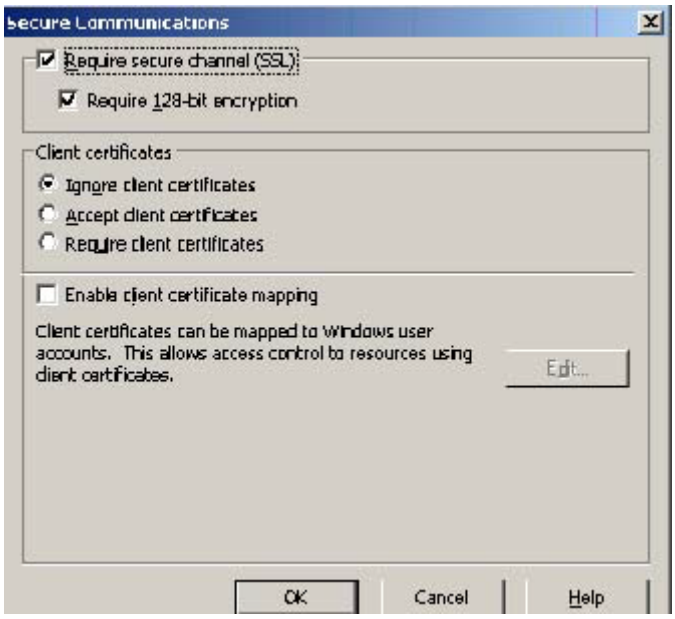
1. Open IIS\local machine and navigate to the **Default Web Site** node.
2. Select web site **OXP1.6** (or **OXP1.4**).
3. Right-click and select **Properties**.



4. Click the **Directory Security** tab.



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



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

3-2-6 Editing the OmISAPIU.xml file

1. Navigate to the following path.

   `C:\Program Files (x86)\HP\HPCR\WebAPI\WebAPI\Scripts`

2. In OmISAPIU.xml, find the FileTransfer node. Replace the IP address with the fully qualified domain name. Also, change `http` to `https`.

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

NOTE: XML files can be edited using Microsoft Notepad.

3. Save the file.

3-2-7 Editing the Bootstrap.xml file

1. Navigate to the following path.

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

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

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

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

3. Save the file.
4. Reset IIS.

4 Required configuration

This section describes:

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

4-1 Adding devices using the HP CR Server Administrator

This section describes the procedures for:

4-1-1 Creating a group of devices

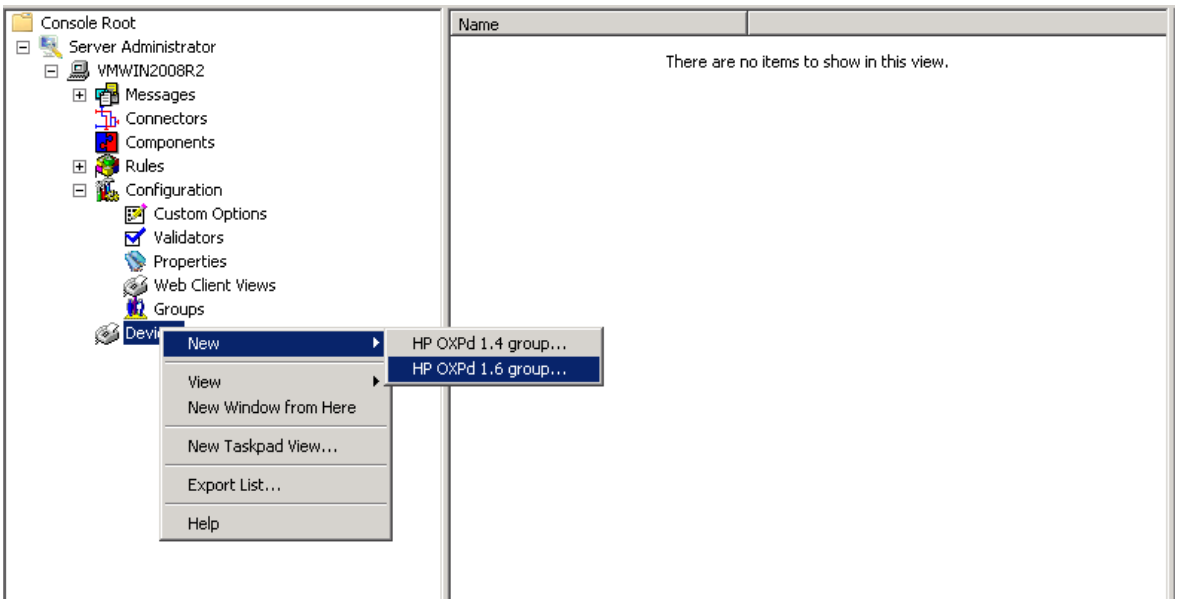
Create a new Group for each group of devices. While each group may have the same configuration, you can configure a group to have a configuration that is completely different from another group. For example, you might create a group named “Marketing” and configure it to use only the Routing Sheets and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

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

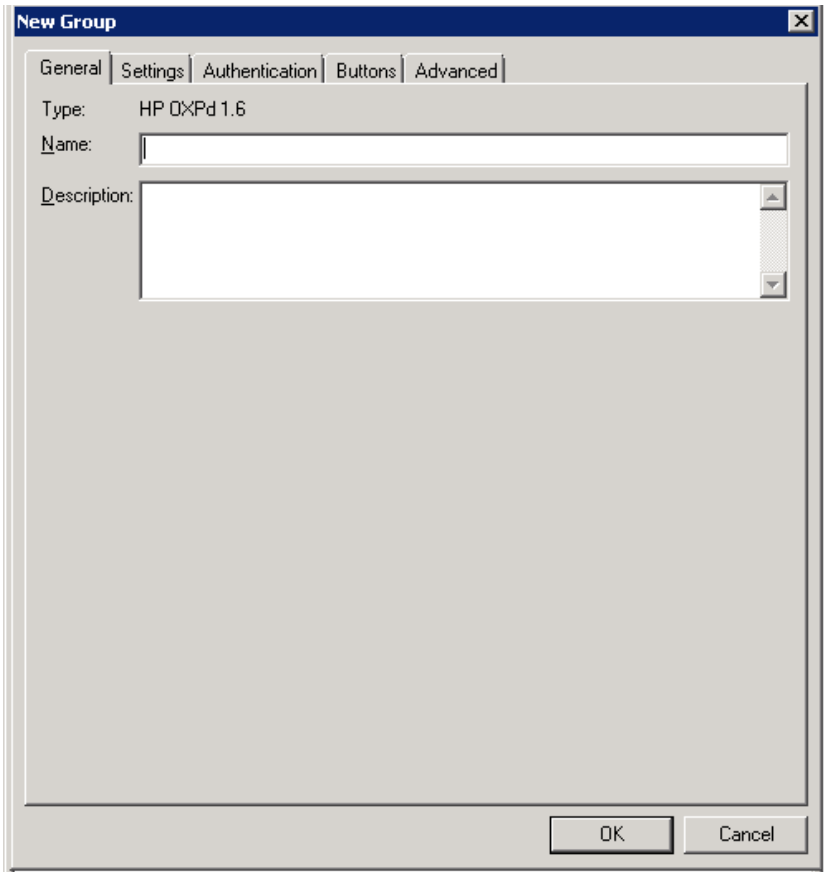
Correct: Group Name = **EastCoastSales**
Incorrect: Group Name = **East Coast Sales**

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

1. Click **Start > All Programs > HP Capture and Route > HP Capture & Route Server Administrator**.
2. In the console tree, expand the HP CR server.
3. Go to the **Devices** node.
4. Right-click and select **New > HP OXPd 1.6 group** (or **HP OXPd 1.4 group**).

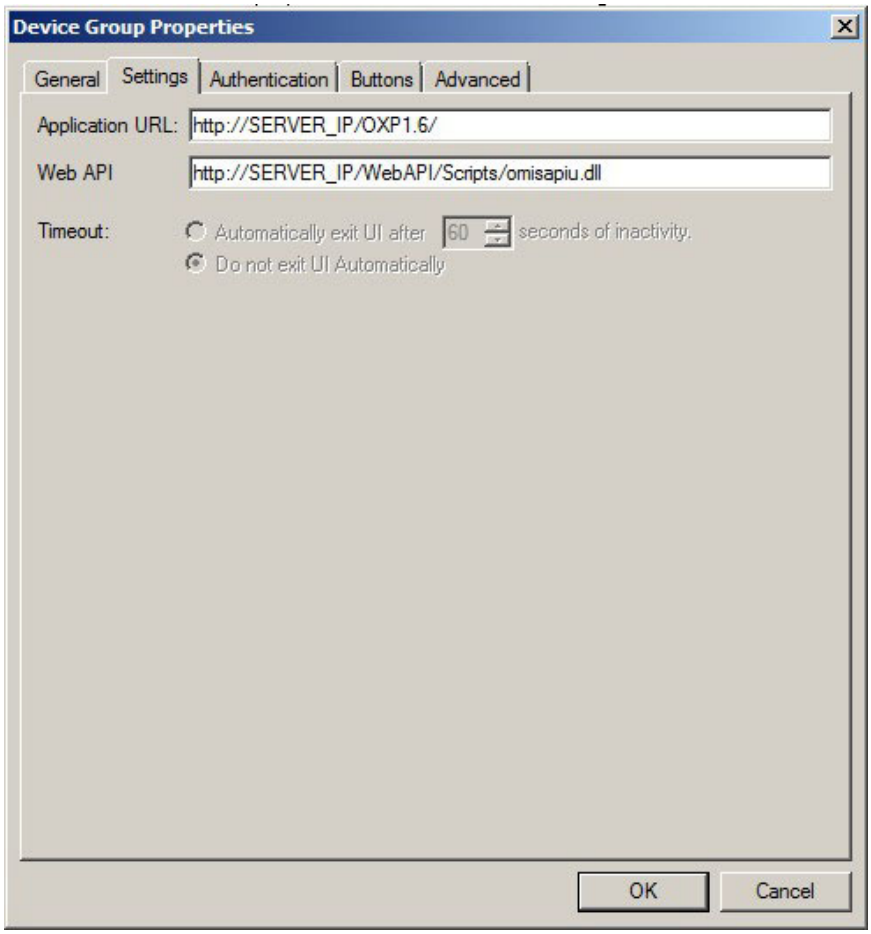


The **New Group** page opens.



5. In the **Name** text box, enter a name for the device.
6. Optionally, in the **Description** text box, enter a device description.

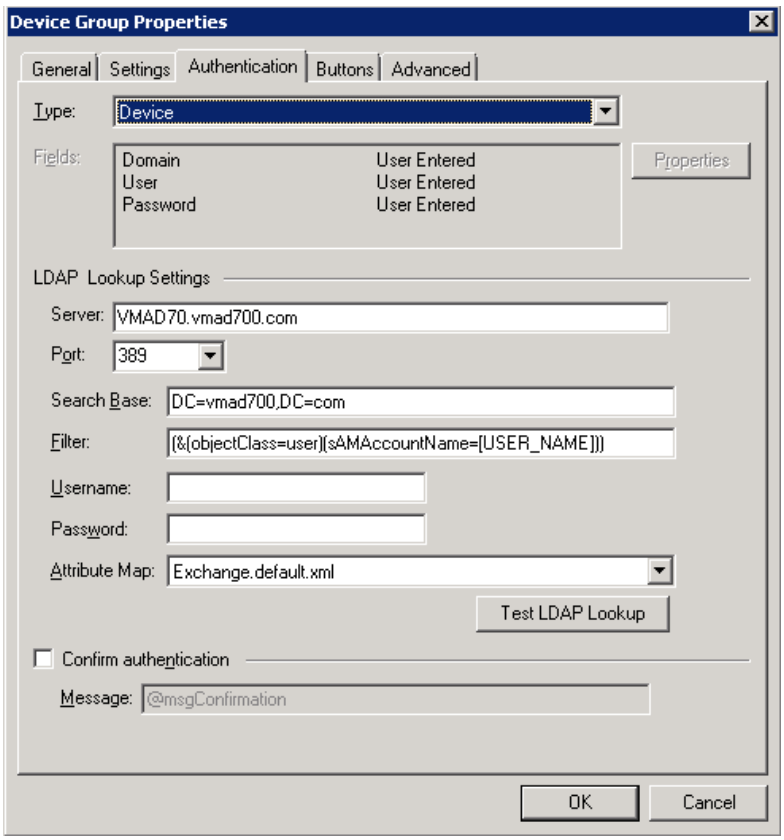
7. Click the **Settings** tab. Change settings only if the IIS/Web server is remote or if you are configuring HTTPS.



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

NOTE: If you are installing as HTTPS, change the URL path from HTTP to HTTPS. For example:
Application URL: `https://FQDN/OXP1.6/`
Web API: `https://FQDN/WebAPI/Scripts/omisapiu.dll`

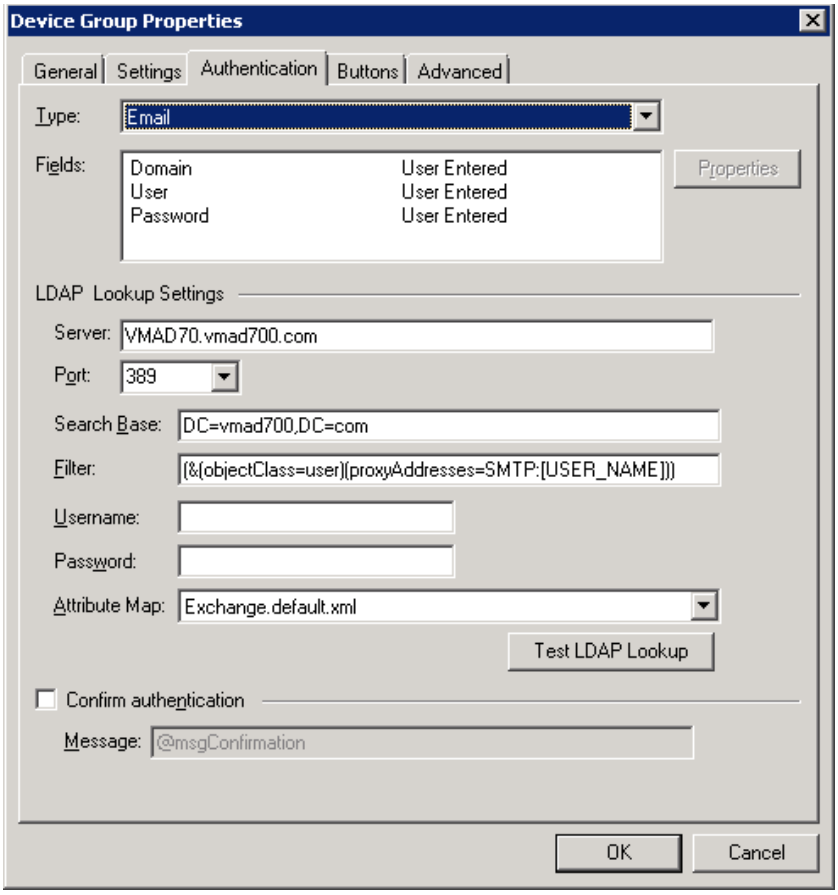
8. Click the **Authentication** tab to specify the type of user authentication required for the group of devices.



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

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

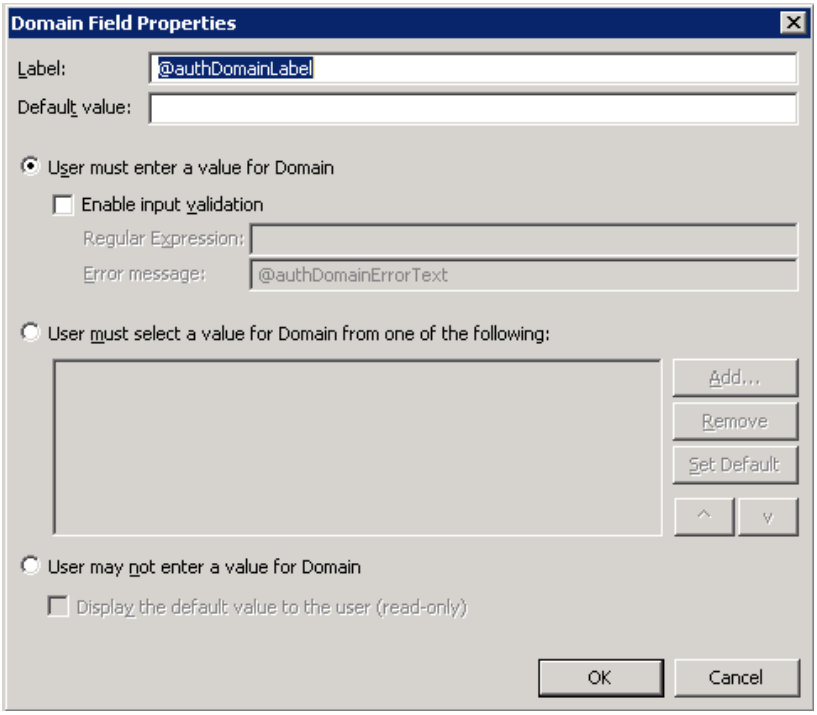
If you select **Email**, **Login**, or **PIN** as the authentication type, you can define the properties for the **Domain**, **User**, and **Password**. For example, if you select **Email**, notice that the **Fields** section is active:



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:



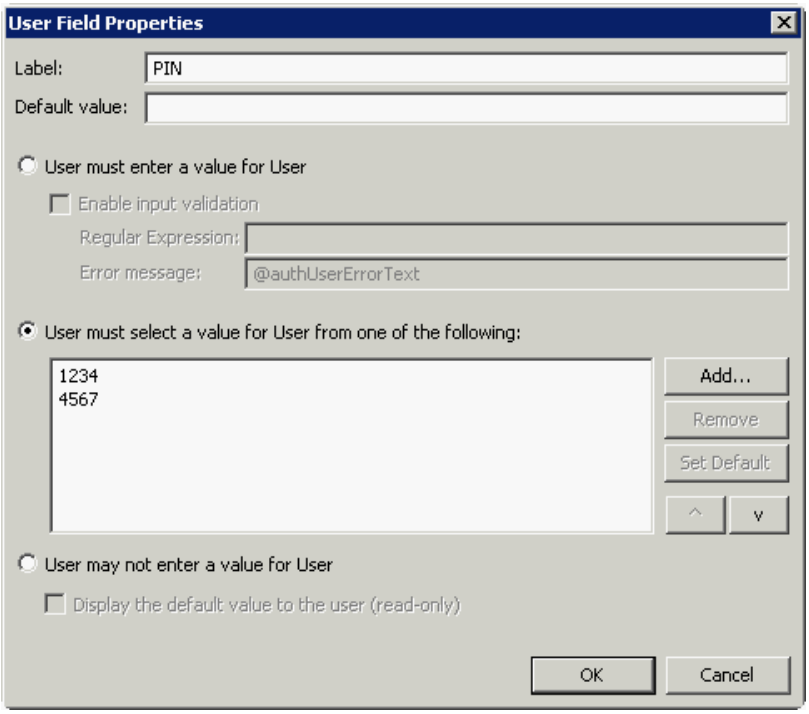
When you define a domain, you can specify a **Default value** (domain) that will be displayed at the device. In addition, you can specify one of the following:

- **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:



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:

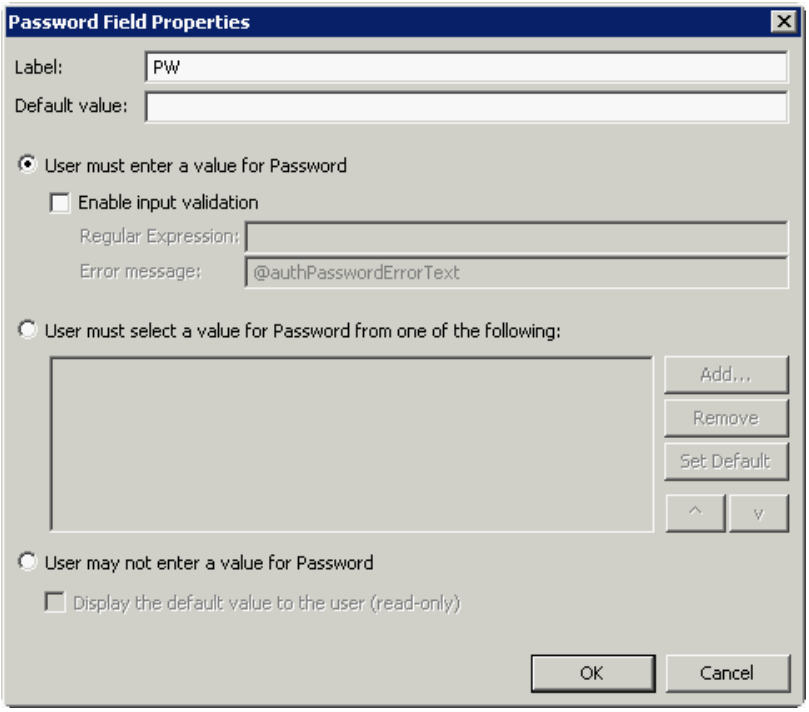
- **User must enter a value for User** - The device user will need to enter a user for authentication during login at the device.
- **User must select a value for User from one of the following** - If there are multiple users in the environment, use this option to create a list from which the user can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



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

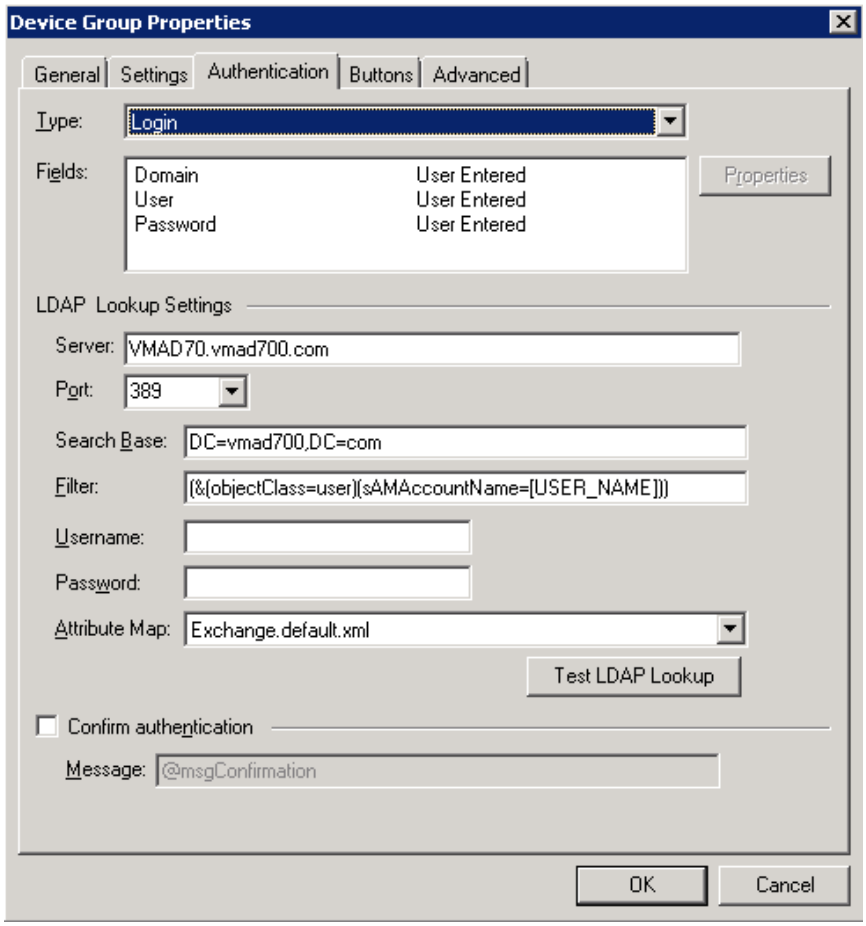
- **User must enter a value for Password** - The device user will need to enter a password for authentication during login at the device.
- **User must select a value for Password from one of the following** - If there are multiple passwords available in the environment, use this option to create a list from which the user can select.
- **User may not enter a value for Password** - This option prohibits the user from entering a password. Use this option only when PIN authentication is used without a password. Do not select this option if you are using Email, Login, or PIN (with password) authentication.

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

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

---

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

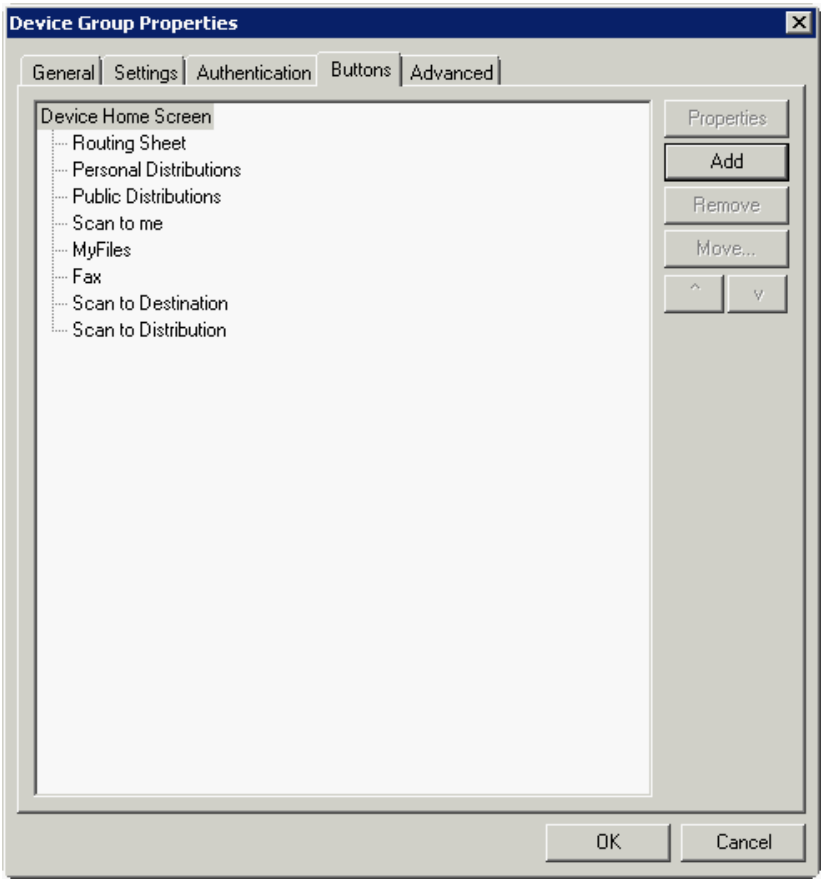


11. In the **Username** text box, enter the name of a Windows user who has permissions to query the active directory.

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

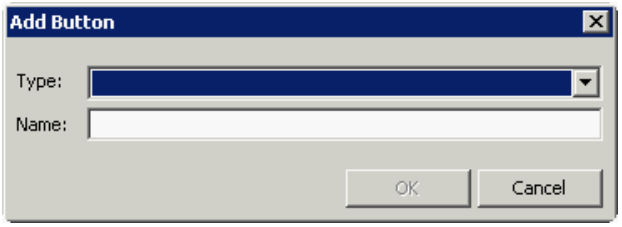
13. Select the **Confirm authentication** option if you want to display a prompt on the device to verify the user's information when authenticating.

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



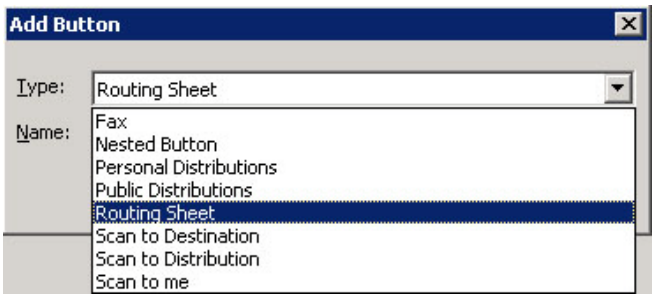
NOTE: It is best to add or remove buttons before installing to the device. Otherwise, if buttons are added or removed, or if button text is modified, it will be necessary to uninstall and run the installation again.

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

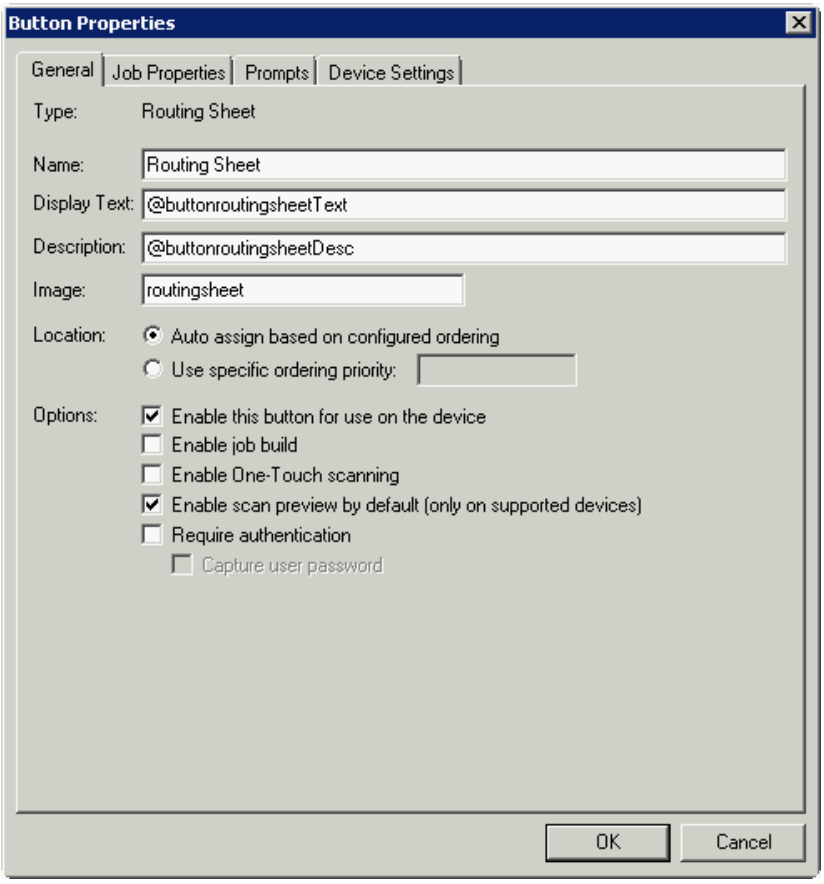


NOTE: If the **Add** button is not active, click on **Device Home Screen**.

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



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



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

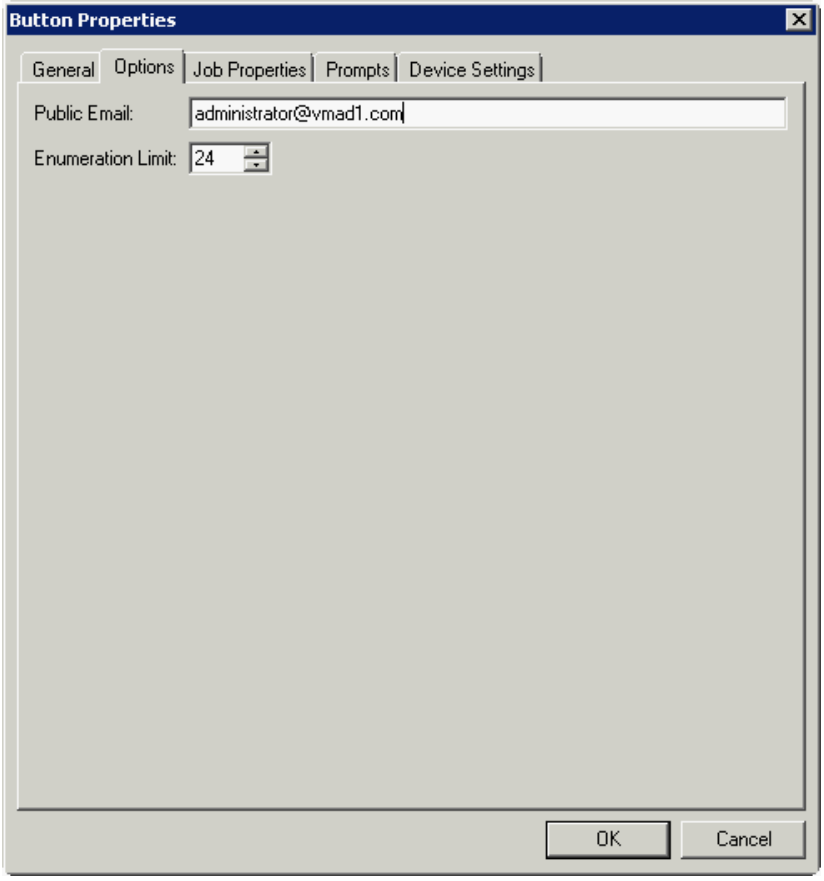
NOTE: Do not change Image from the default value.

19. Specify a location for the button. Select either of these options:
    - **Auto assign based on configured ordering** - The button is positioned based on a predefined order.
    - **Use specific ordering priority** - You can enter a value to indicate the button placement. Position 1 is in the upper left location and position 2 is in the upper right location, in a Z-order layout. The pattern is as follows:

      1 2
      3 4
      5 6
      etc.
20. Select addition options for the button:
    - **Enable this button for use on the device** - Self-explanatory.
    - **Enable job build** - This option enables the Scan More feature.
    - **Enable One-Touch scanning** - This allows the user to select a button with the documents already loaded in the Automatic Document Feeder for one-touch scanning. Typically, this is used with a Distribution that has all scan settings saved.

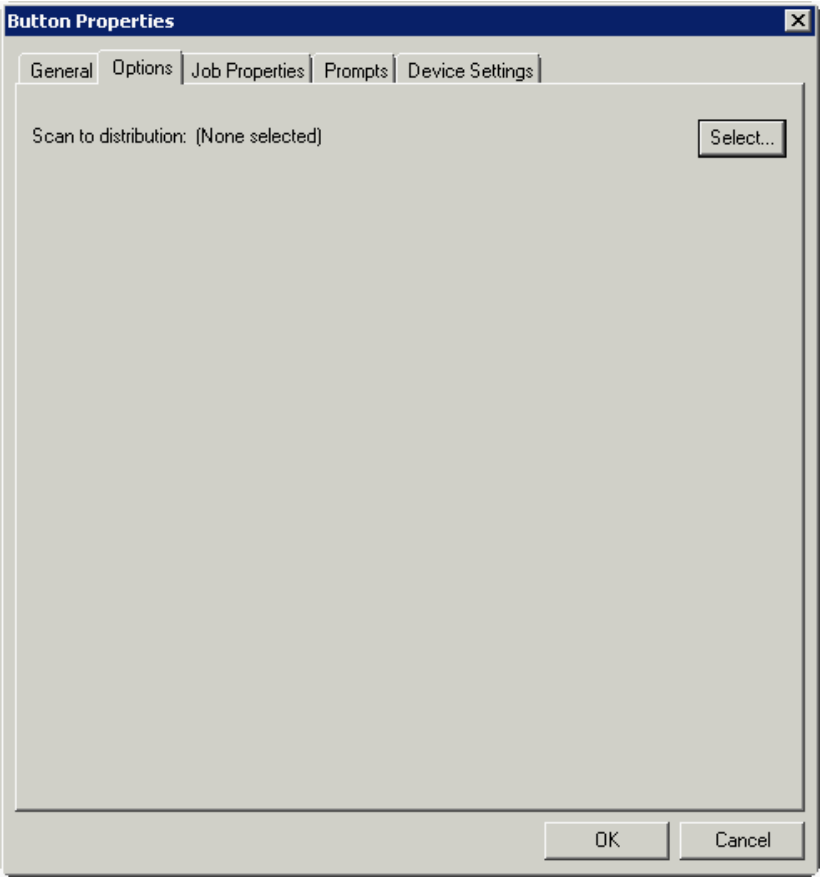
- **Enable scan preview by default (only on supported devices)** - This applies to **Futuresmart** devices only.
- **Require authentication** - If you select this option, you can then indicate that the button should capture the user's password. Note that although the Routing Sheet feature typically does not require authentication, you can configure this requirement here.

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

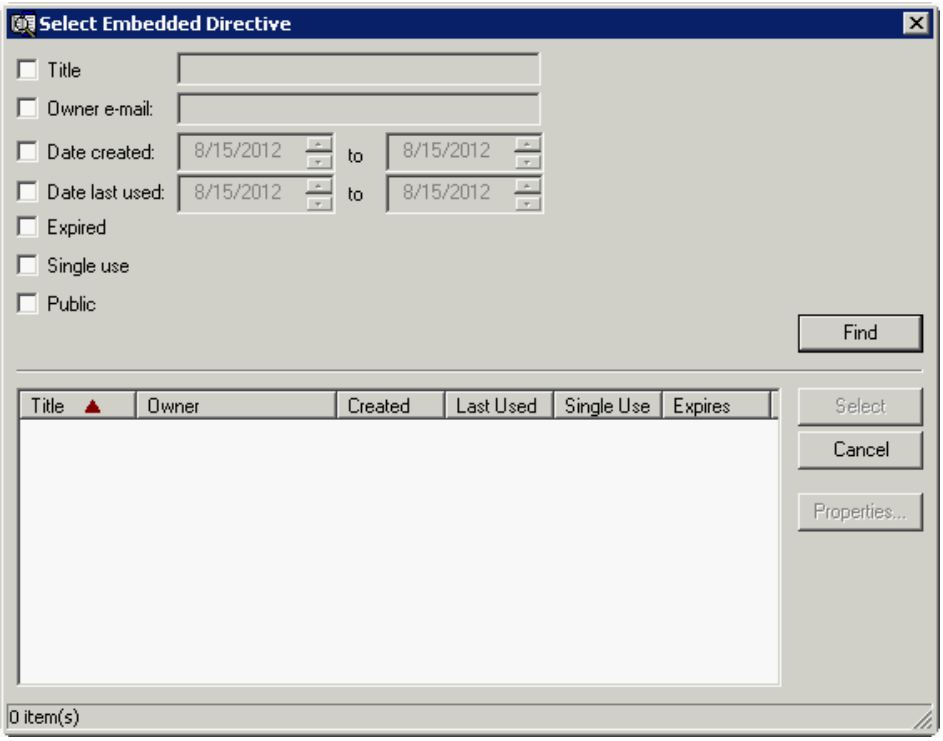


Enter a **Public Email** address (if applicable) and set the **Enumeration Limit** for distributions (the maximum number of distributions allowable).

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



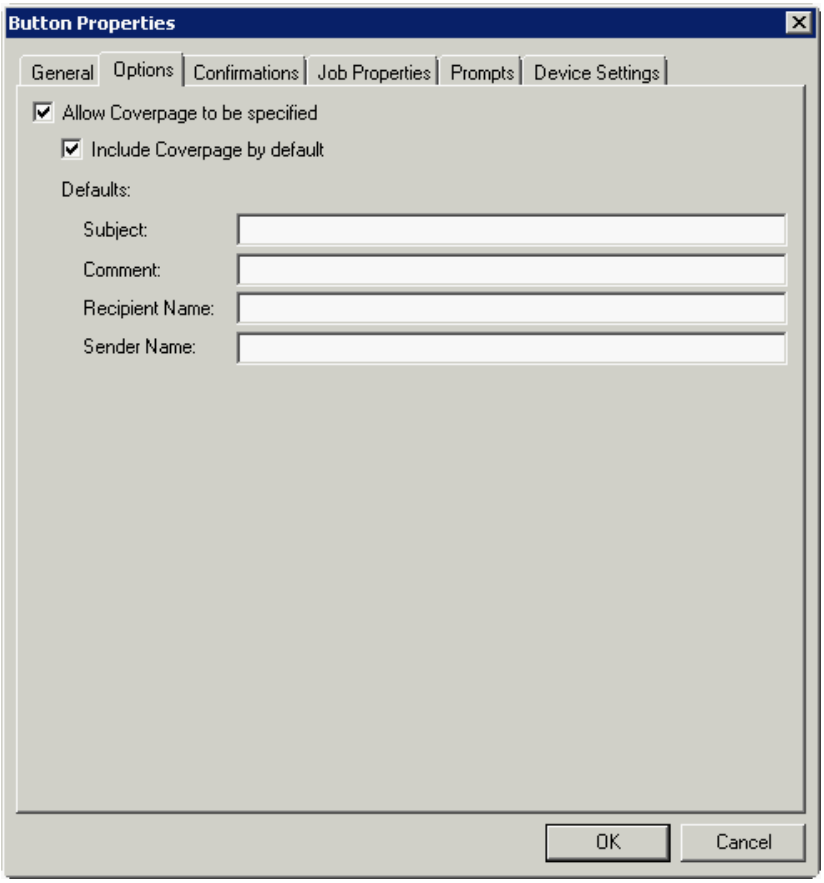
Click **Select** and the **Select Embedded Directive** dialog is displayed.



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

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

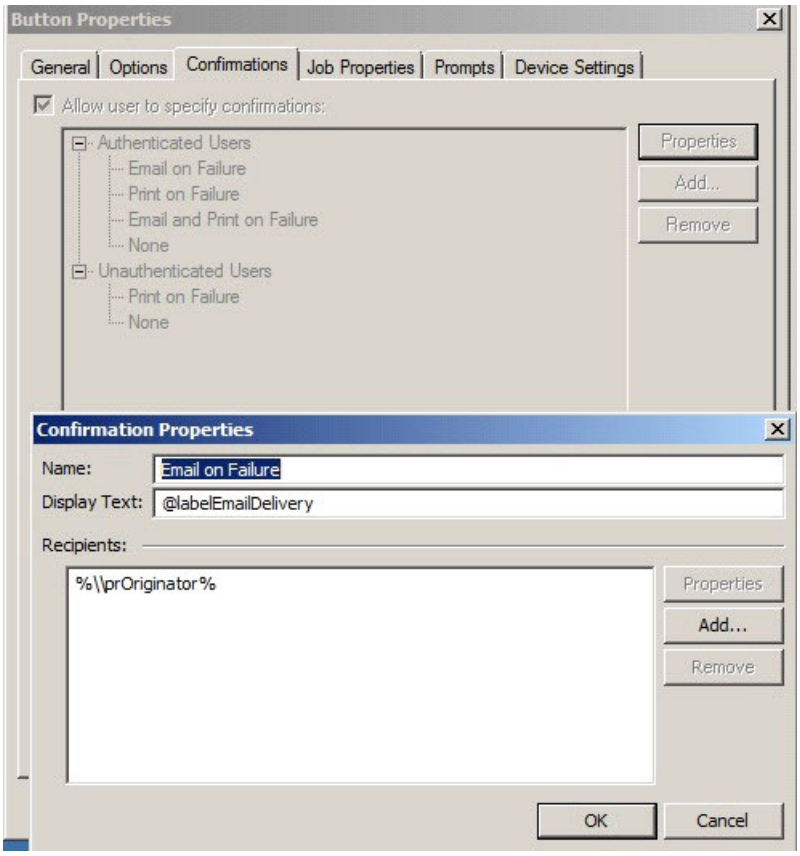
23. If you are adding a **Fax** button, click the **Options** tab to configure fax cover pages. Select options to allow a cover page to be specified and include the cover page by default. In addition, you can indicate the information (subject, etc.) that will appear on the cover page.



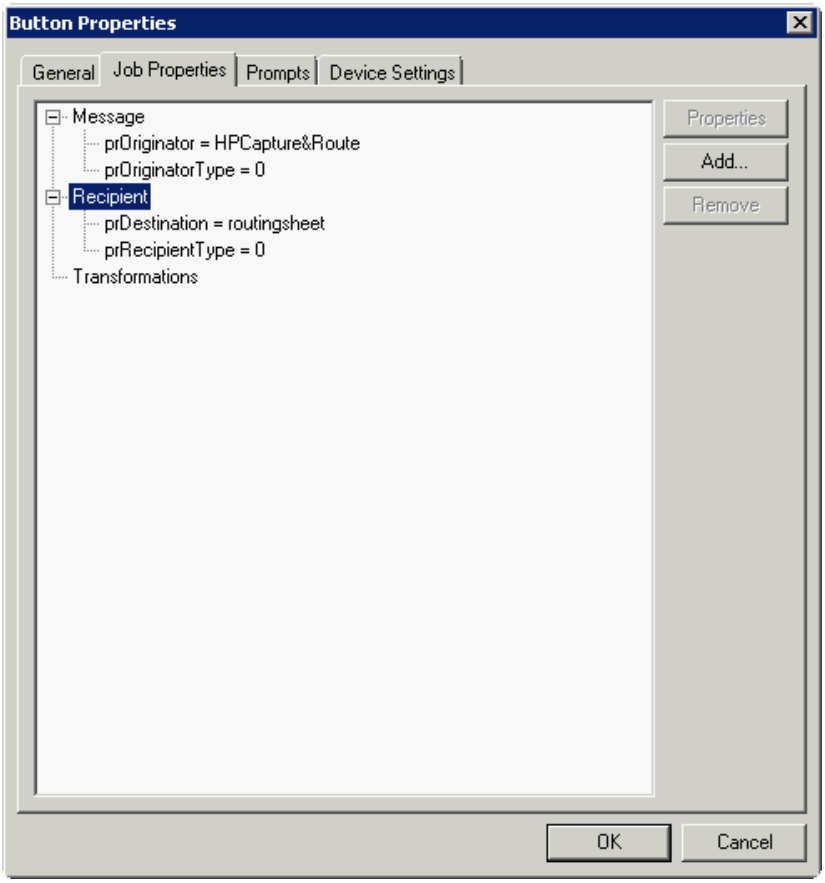
24. If you are adding a **Fax** button, click the **Confirmations** tab to:

- Allow authenticated and non-authenticated users to select the button.
- Define the type of fax confirmations (select a field and click **Properties**).
- Add recipients for confirmations (click the **Add** button).

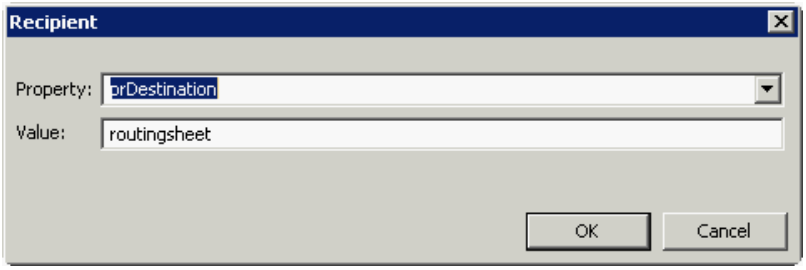
For example, you can edit the fields for the Originator for faxed faxes:



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



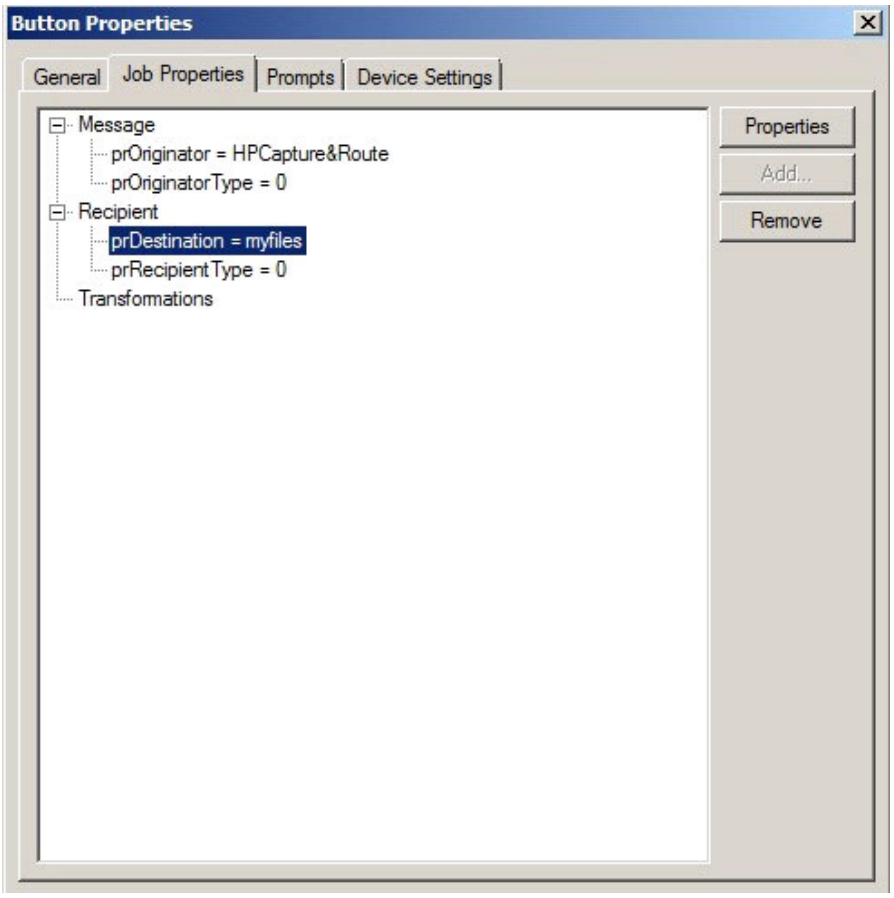
You can add, remove, or change a property. This example shows the property of a **Destination**.



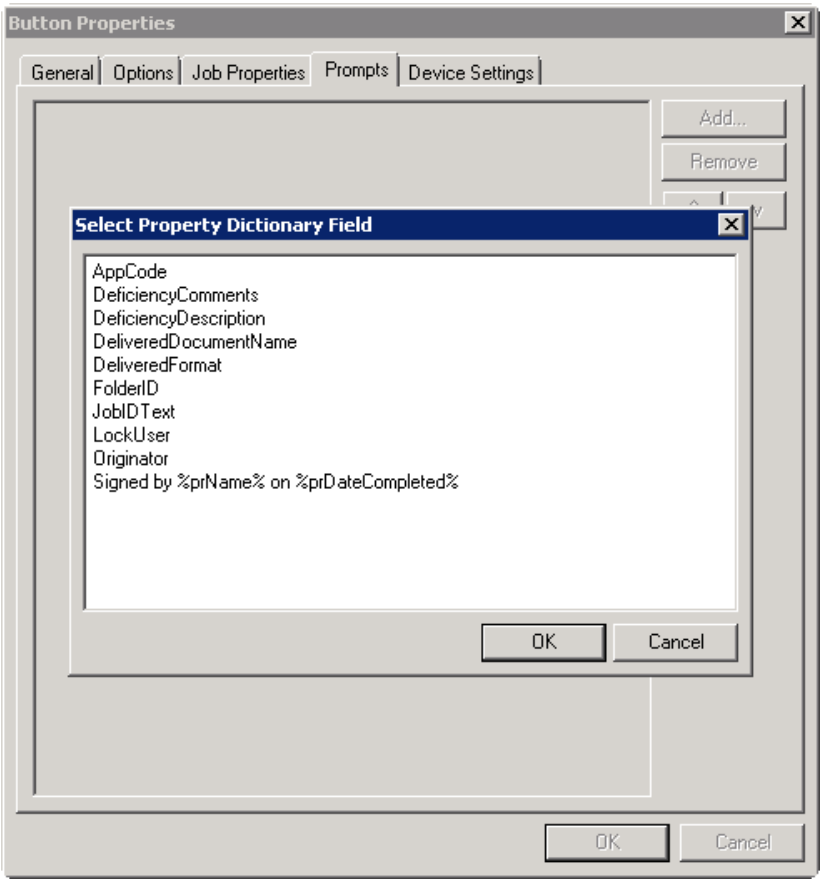
You can change an **Originator**, **Destination**, or **Recipient**. You also can add a **Transformation** (replacing a data value (a message property, recipient property, Embedded Directive property, or template variable) with another value.).

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

- The default 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.

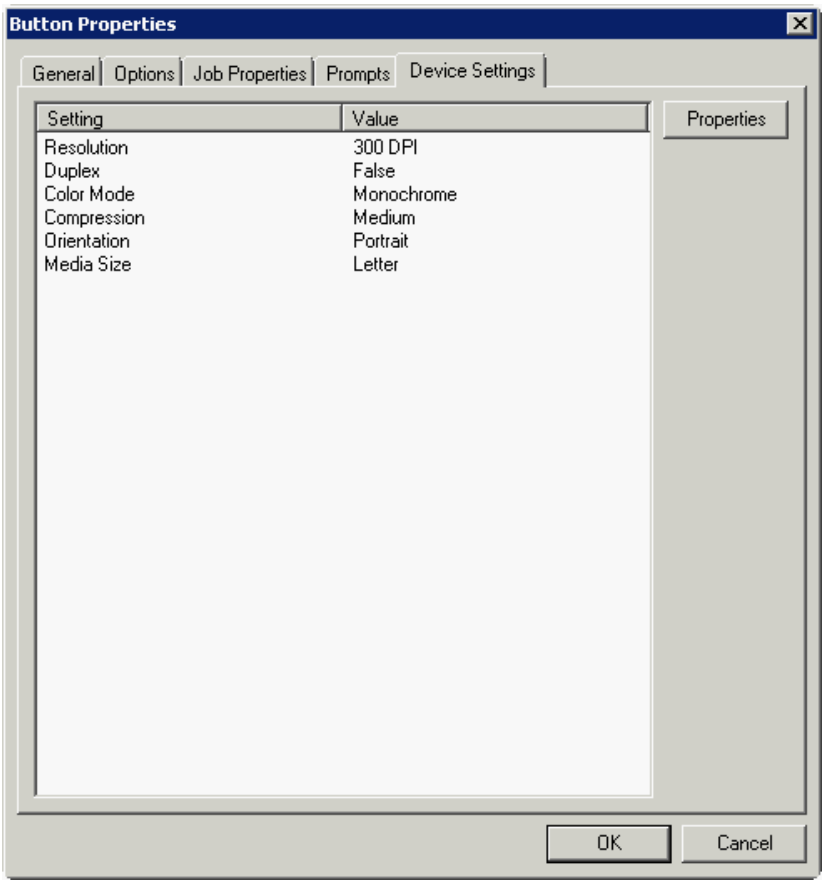


26. Click the **Prompts** tab. Click **Add** to select a prompt configured on the HP CR server. The **Select Property Dictionary Field** is displayed.

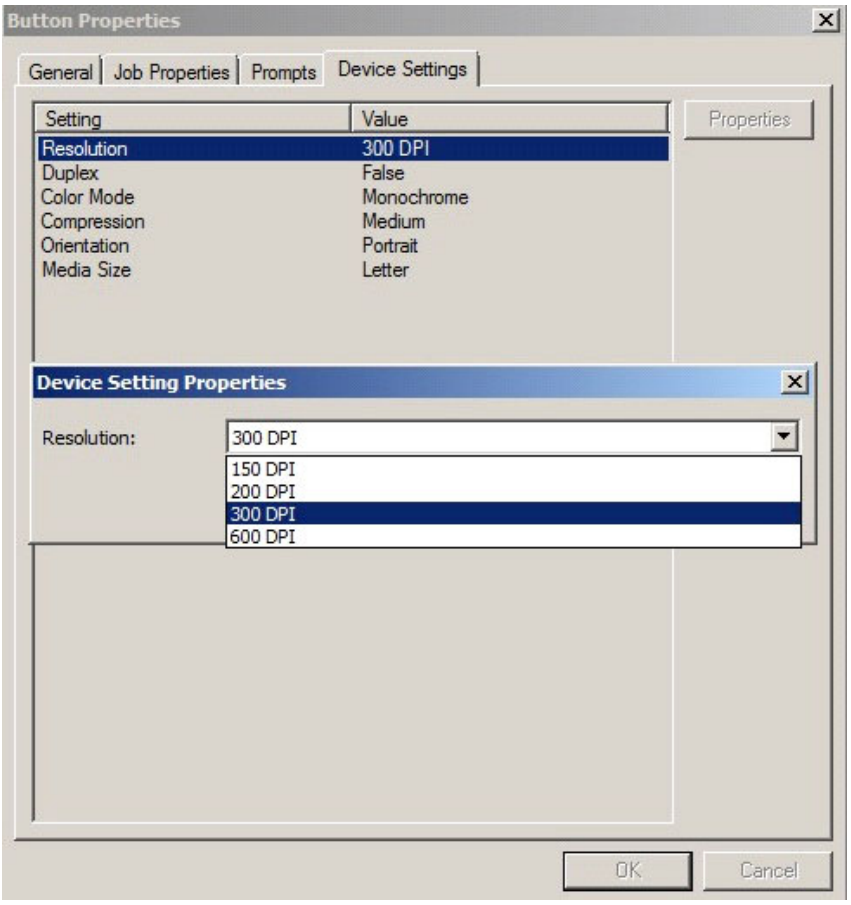


Select a prompt and click **OK**.

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



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



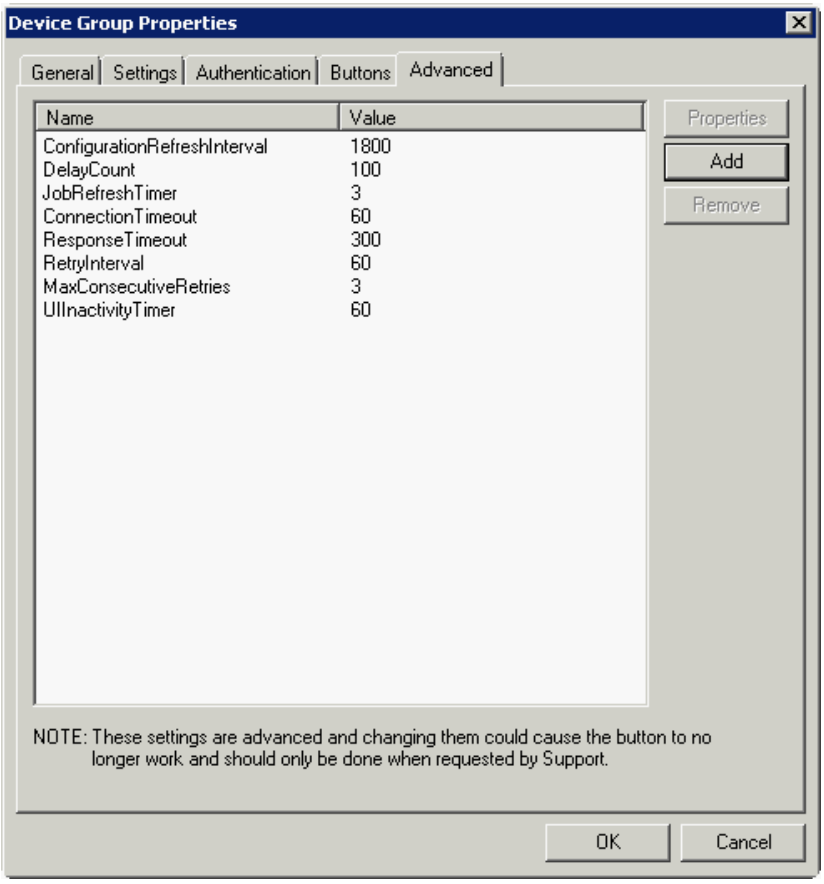
28. Click **OK** to return to the **Device Group Properties**.

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

---

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

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



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

31. Once a button configuration is complete, the xml files can be exported for importing into HP's WebJet Admin server for button deployment.

    Go to the **Devices** node and right-click on the group name. Then, select the **Export to Web Jet Admin** option. See Installing OXPd v1.6 buttons (60).

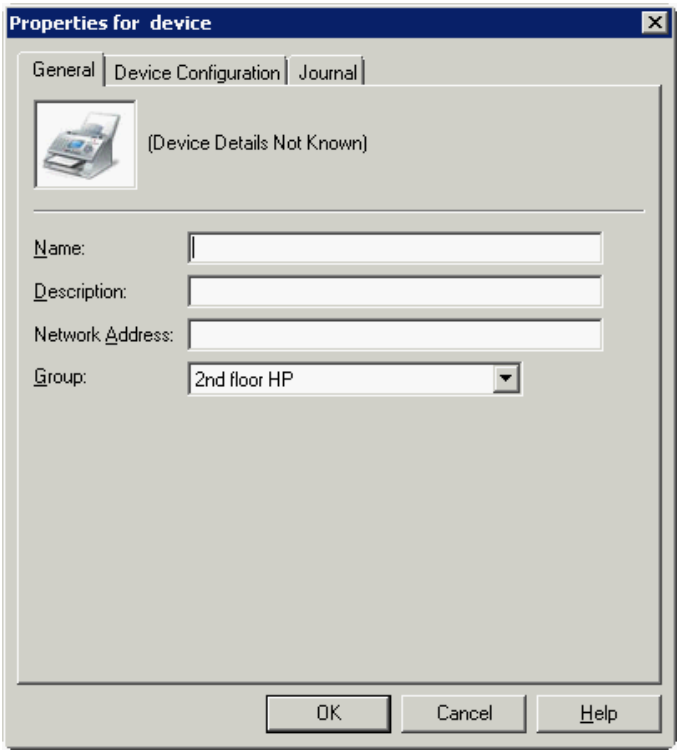
4-1-2 Updating the Deviceloader.xml to support new devices

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

4-1-3 Adding a new device

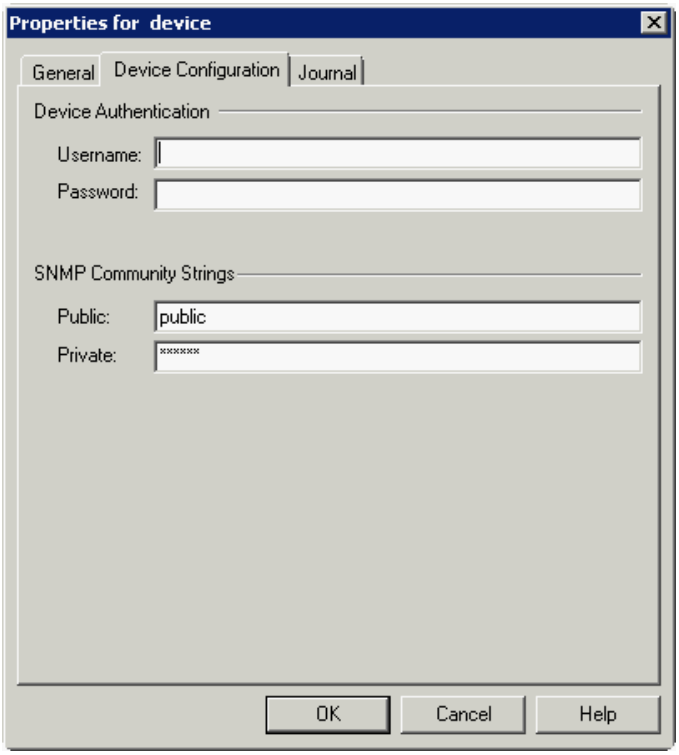
1. In the console tree, expand the HP CR server and go to the **Devices** node.
2. Right-click and select the group name. Then, select **New > Device**.

   The **Properties for device** page opens.

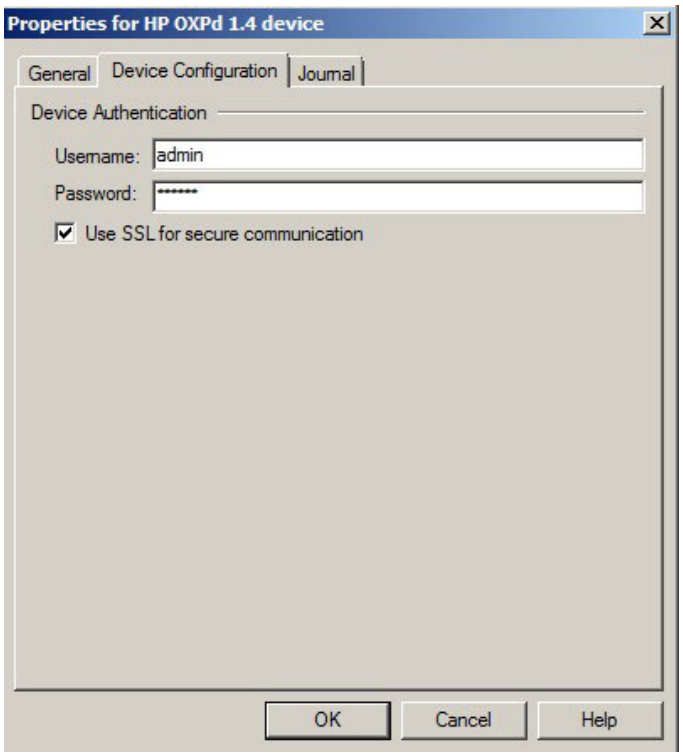


3. In the **Name** text box, enter a name for the device.
4. Optionally, in the **Description** text box, enter a device description.
5. In the **Network Address** text box, enter the HP device IP address.

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



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



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

9. If you are using HP OXPd v1.6, configure the **SNMP Community Strings** section (this section will not appear for HP OXPd v1.4).
   - In the **Public** text box, enter the v1.6 device public community string.
   - In the **Private** text box, enter the v1.6 device private community string.

   The default value is public in both the **Public** and **Private** fields.
10. Click **OK** to add the device.
11. Test by selecting the newly added device. Right-click on the device name and select **Query** from the drop-down options. Verify that the device is successfully queried from the server.
12. After a successful query, right-click and select **Install**.
13. Verify that the buttons appear on the device.

4-2 Choosing an authentication method

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

You can configure:

- LDAP authentication
- HP authentication at the device

4-2-1 Configuring LDAP authentication

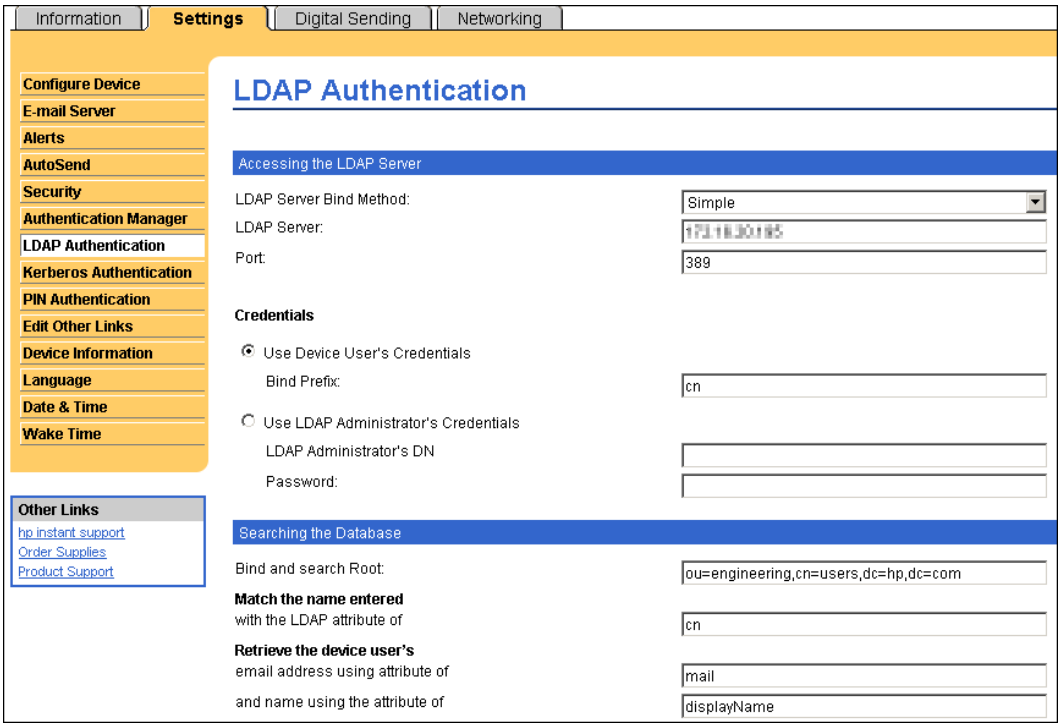
When you choose LDAP Authentication, the user is prompted to enter an email username and password. The HP Authentication Manager uses the login credentials to initiate a lookup. The lookup validates the user and returns the user's email address. Then the Embedded Device Client for HP OXPd uses the email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

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

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

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

LDAP Authentication binds to the LDAP server with the device user's common name (CN). The search is conducted within the root ou=engineering,cn=users,dc=hp,dc=com using the device user's common name (CN). The return value is the user's email address (mail) and name (displayName).

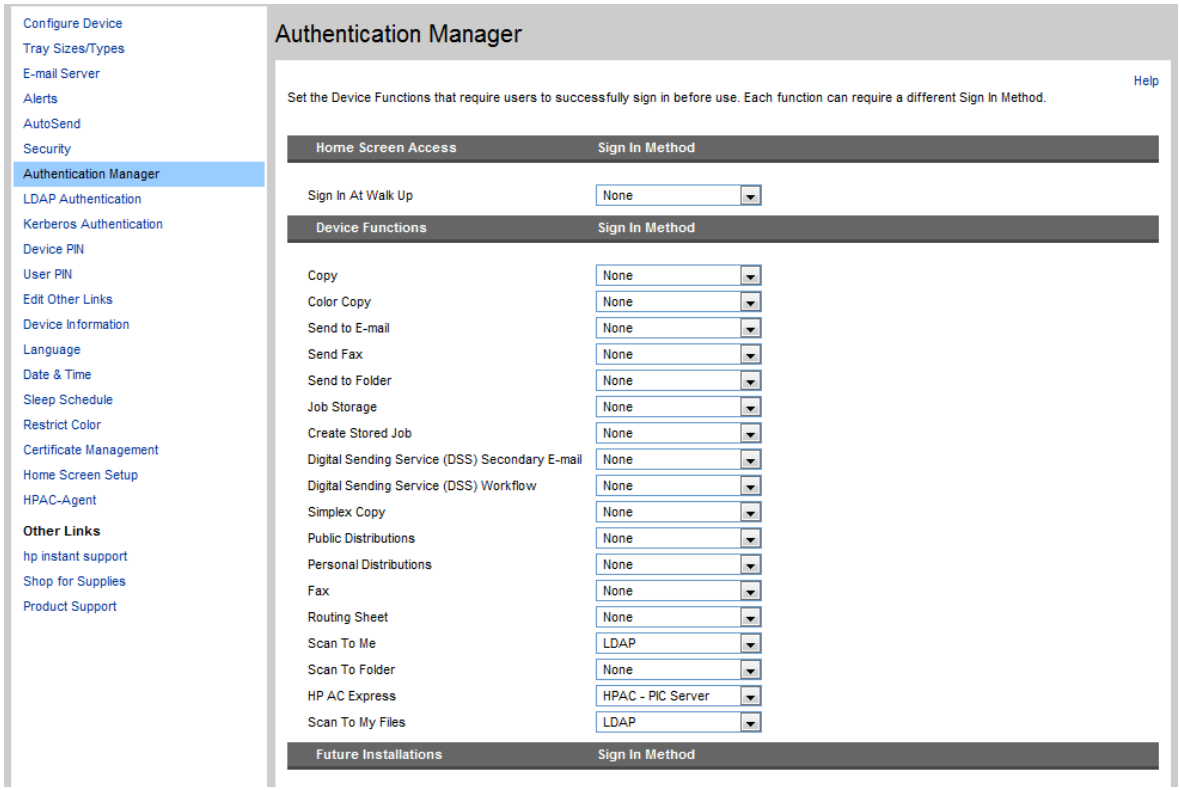


4-2-2 Configuring HP authentication on the device

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

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

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



7. Click **Apply**.

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

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

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

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

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

1. Navigate to: `C:\Program Files\HP\HPCR\HPOXP\Configuration`
2. Open `configuration.xml` for editing.
3. Search for the `<Search UseABService` node.
4. Verify the value is set as:
   `<Search UseABService="true" ABServiceAddress="HPCR_IP_Address">`

   For example:
   `<Search UseABService="true" ABServiceAddress="111.222.333.444">`
5. Save your changes to the configuration file.

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

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

4-3 Configuring the server

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

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

When rules have been created for all HP CR scanning features available on devices in your environment, the HP CR server is fully configured for the Embedded Device Client for HP OXPd. Now you are ready to test the HP CR scanning features. Continue with the information in Section 6: Testing (71).

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

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

5-1 Supported devices

The following devices are supported:

Table 1 HP Device Series Matrix

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

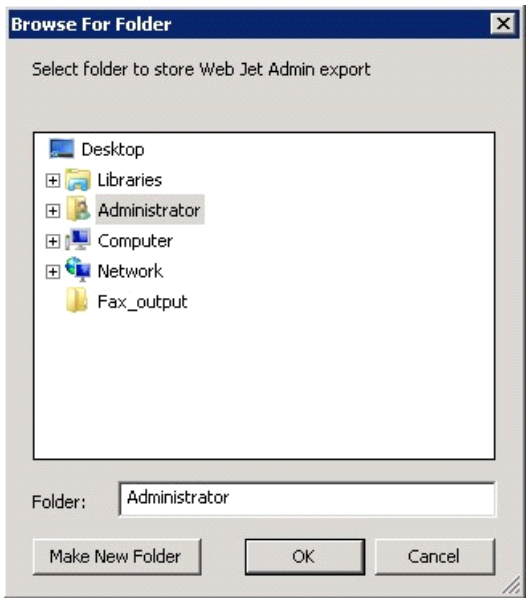
Device	Operating System
Color LaserJet CM 3530 MFP	Oz
Color LaserJet CM 4540 MFP	FutureSmart
ScanJet 7000n	FutureSmart
ScanJet 8500	FutureSmart
LaserJet Flow M525 MXP	FutureSmart
LaserJet Flow M575 MXP	FutureSmart
LaserJet M775 MFP	FutureSmart
LaserJet M4555 MFP	FutureSmart

5-2 Exporting the XML files

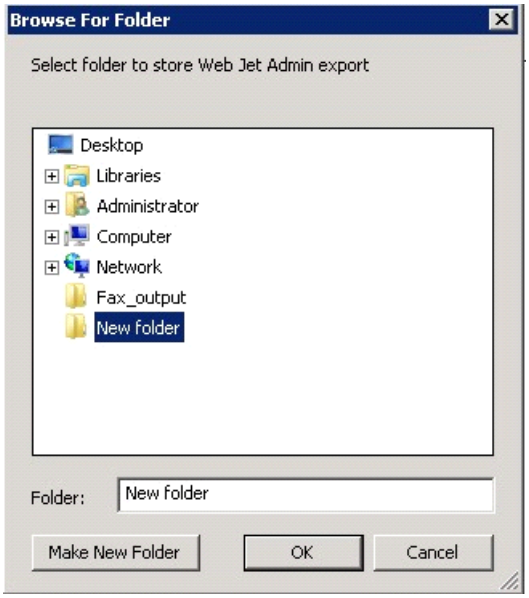
Complete the following procedure for HP CR to configure the HP OXPs device client with the desired settings.

1. Once the configuration is complete (as described in Section 2: Embedded Device Client for HP OXPd installation and Section 4: Required configuration), right-lick the **Devices** group to which you intend to deploy buttons. Select **Export to Web Jet Admin**.
2. You can now store the XML files by browsing to a network folder or creating a new folder destination.

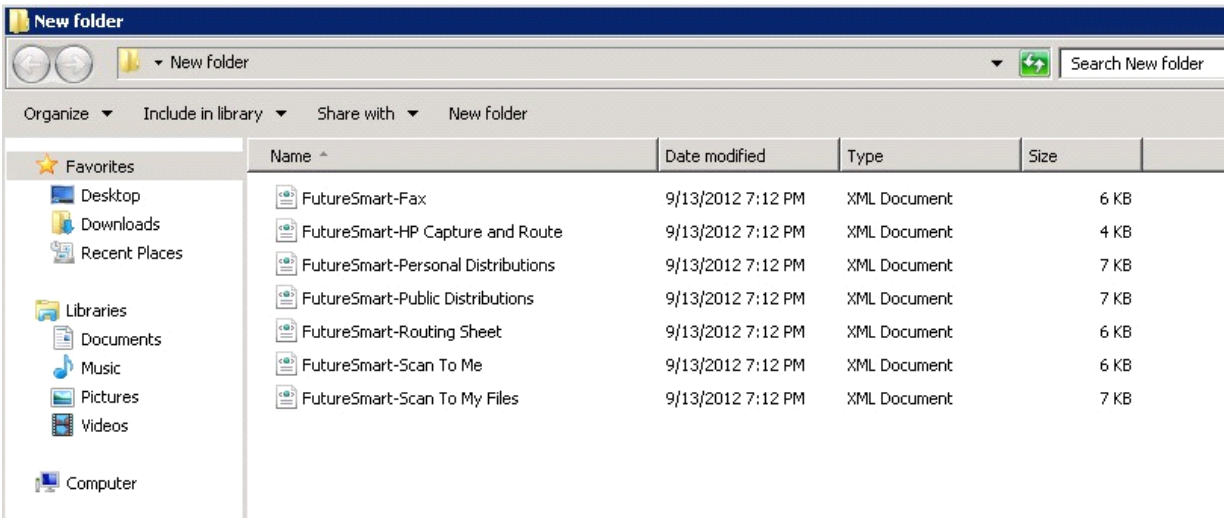
   Browse:



Make New Folder:



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



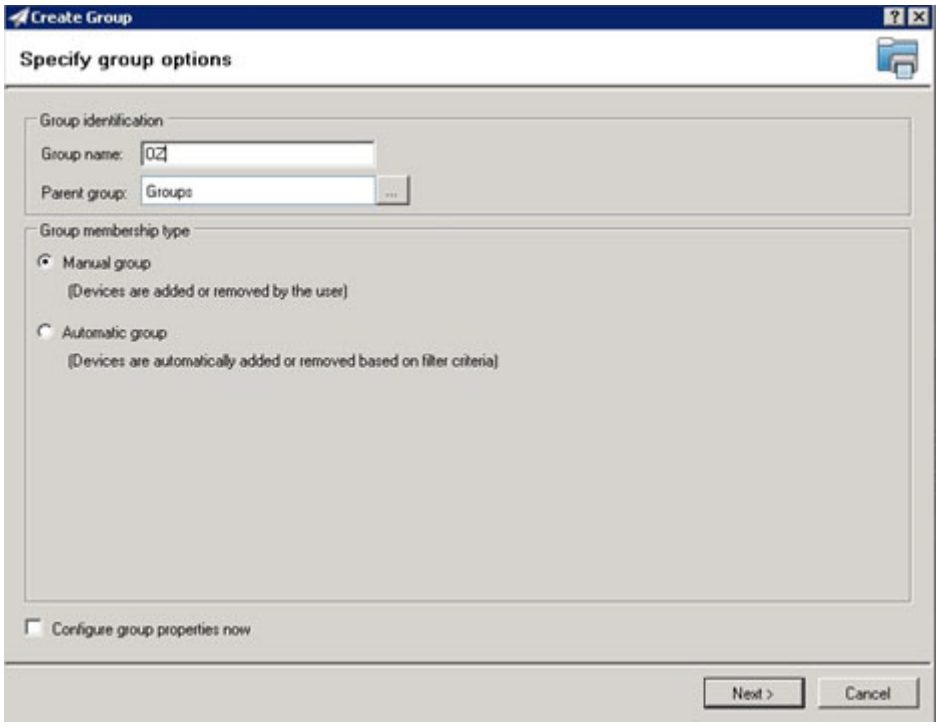
5-3 Installing OXPd v1.6 buttons

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

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

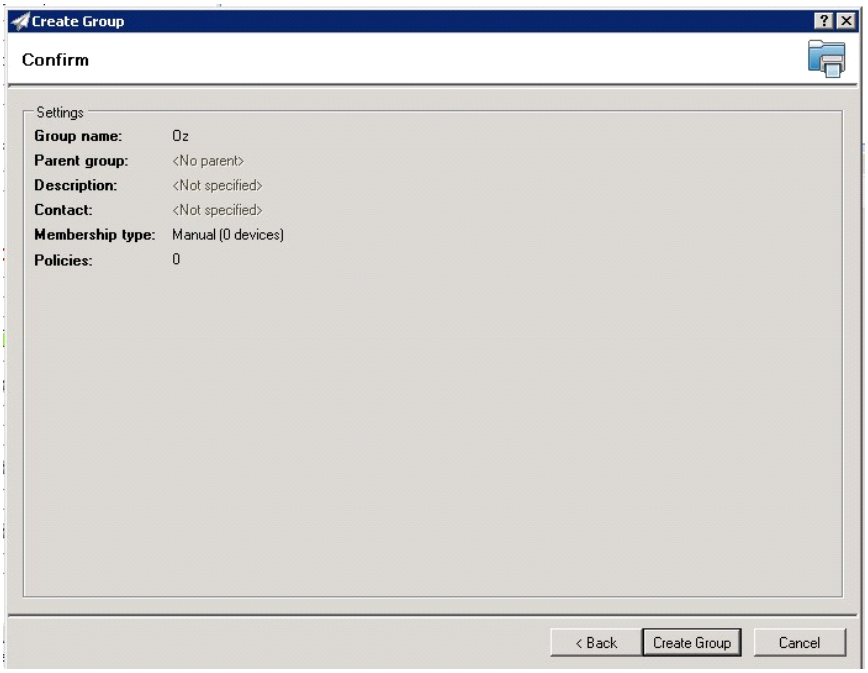
1. Right-click the **Group** node and select **New group**.

   The **Specify group options** page is displayed.

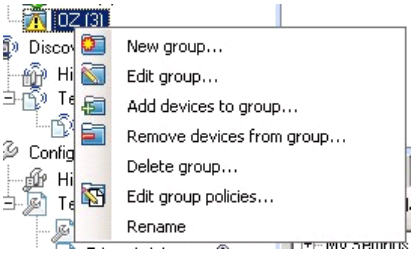


2. Enter the name of the new group that you will use to group similar devices for HP OXPd button installation. (Preferably, this is a device group name that will allow the administrator to easily configure similar firmware or button functionality installations such as Jedi, Oz, etc.)

3. Click **Next** and verify the group name is correct. The **Confirm** page is displayed, showing the settings for the group.

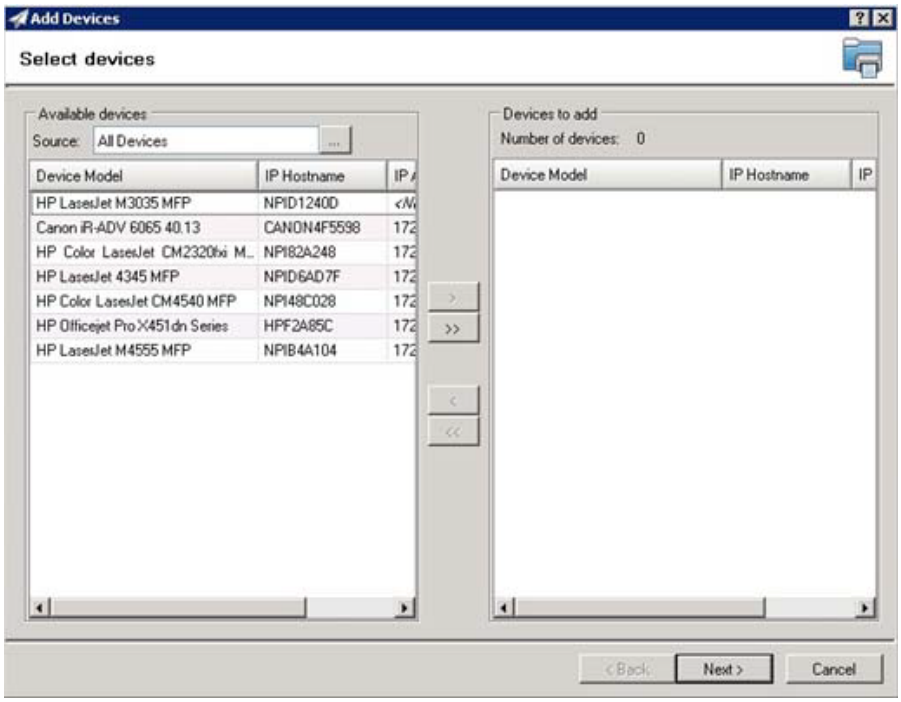


4. Click **Create Group** and then **Done**.
5. Right-click the newly created group and select **Add devices to group**.

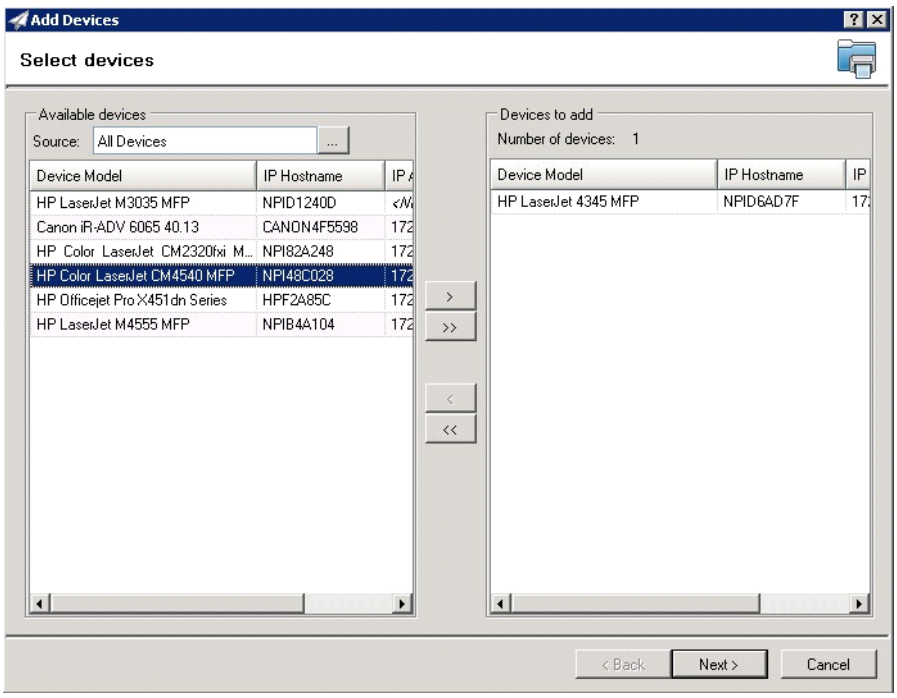


NOTE: For more options in using the Web Jetadmin device filters to find or add devices, consult HP's Web Jetadmin team for a complete Web Jetadmin installation guide.

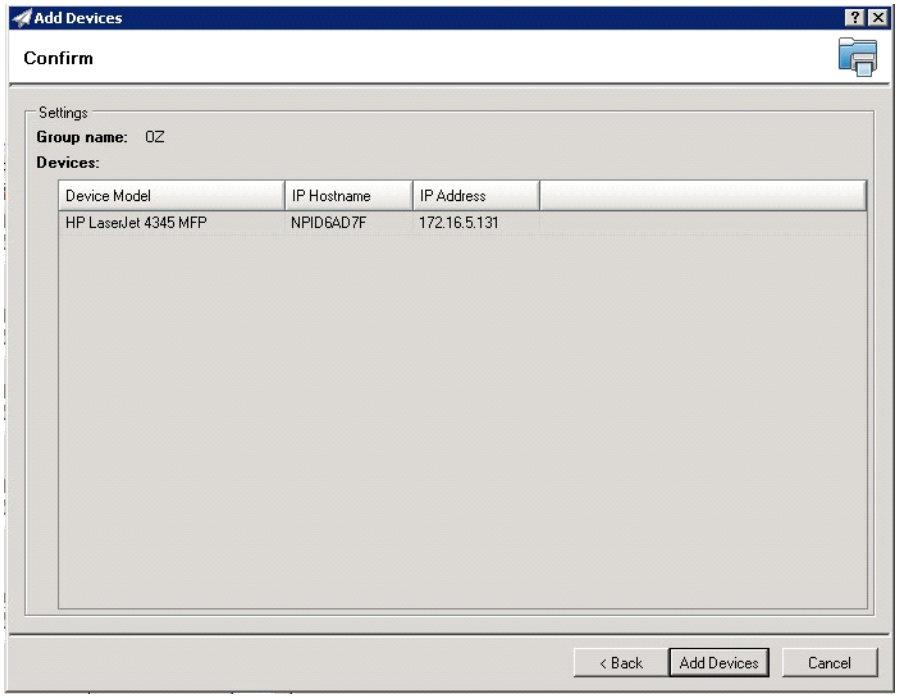
The **Select Devices** page is displayed.



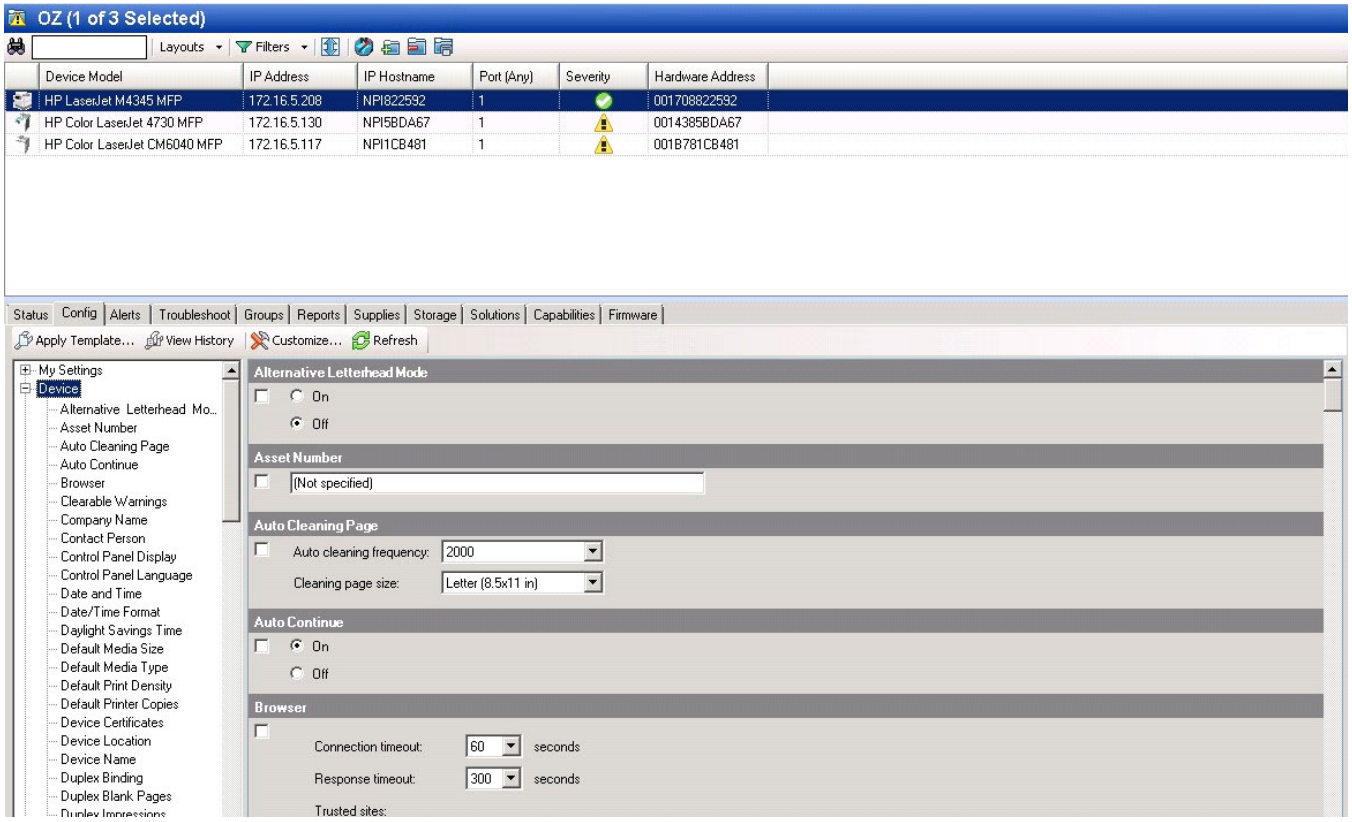
6. In the **Available devices** list (on the left), highlight the device(s) to be added to the group. Then click the **>** (add) button. The selected device(s) will be added to the **Devices to add** list (on the right).



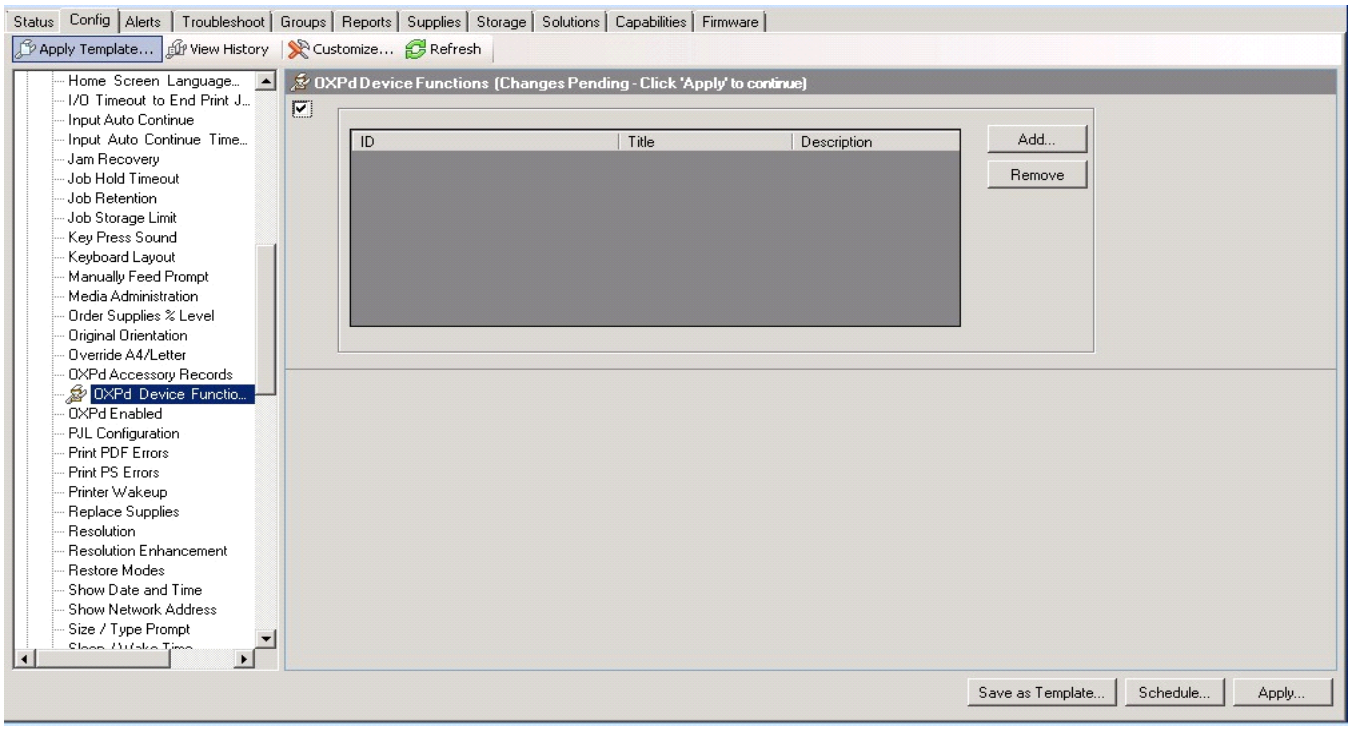
7. Click **Next**. The **Confirm** page is displayed.



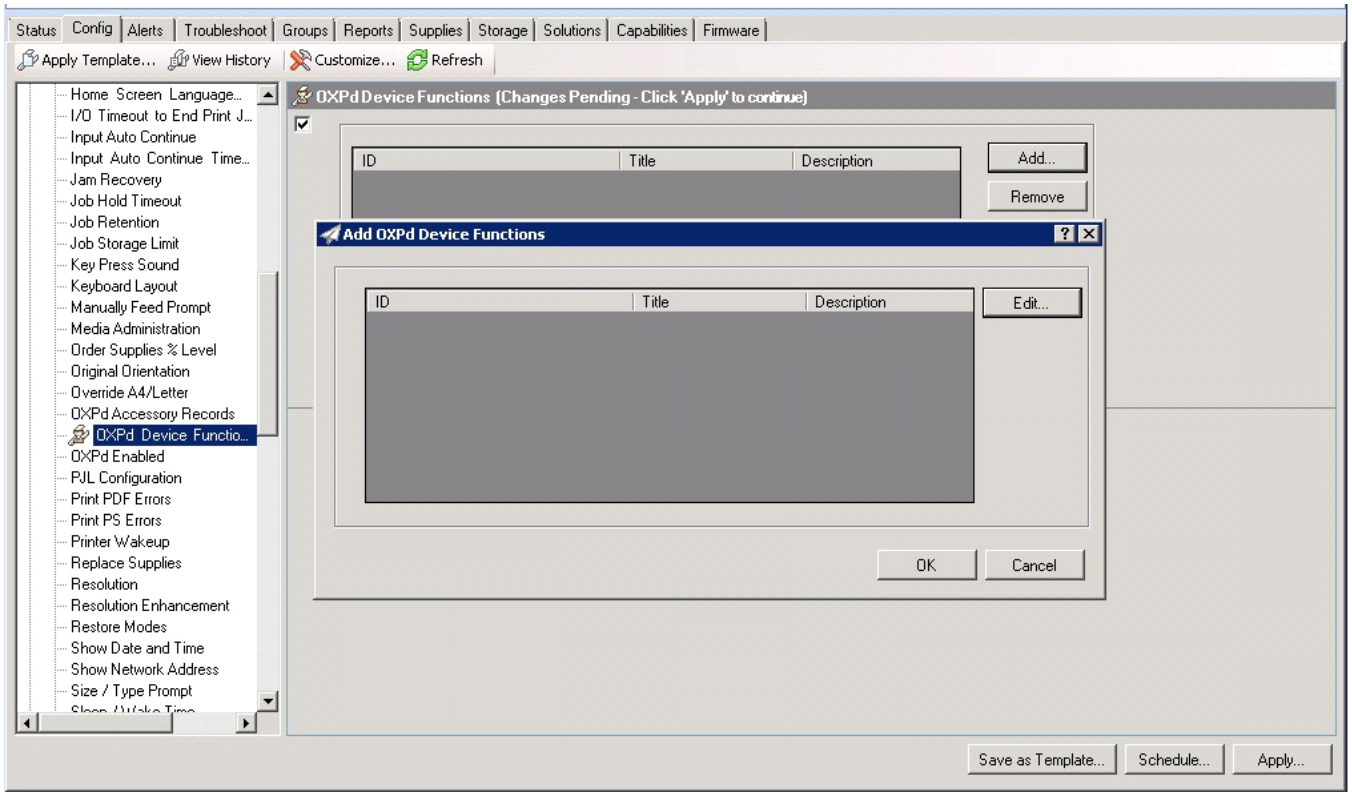
8. Click the **Add Devices** button. You should see the devices added to your new group in the **Group** window.
9. Highlight the device(s) to which you want to install buttons.



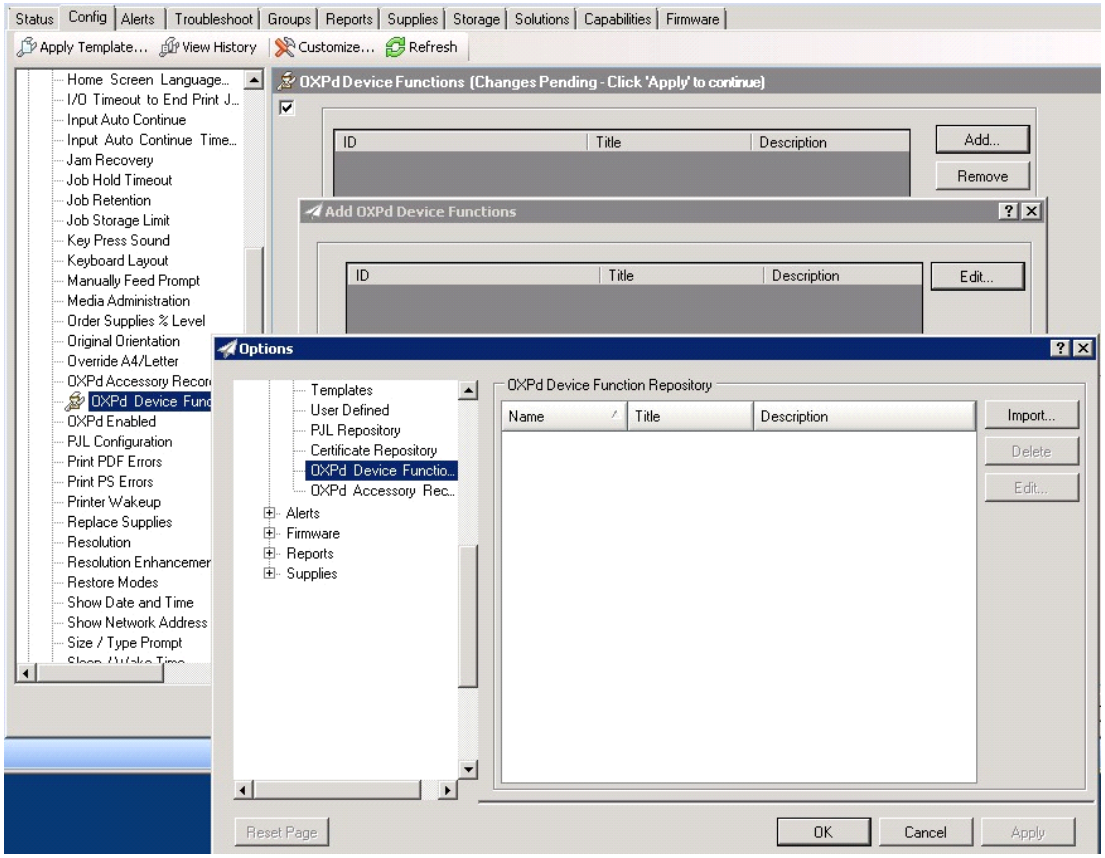
10. Click the **Config** tab and scroll to the **OXPd Device Functions** subset (as shown below). Check the box in the upper left corner of the center window. The title bar of that area will display: *OXPd Device Functions (Changes Pending - Click 'Apply' to continue)*.



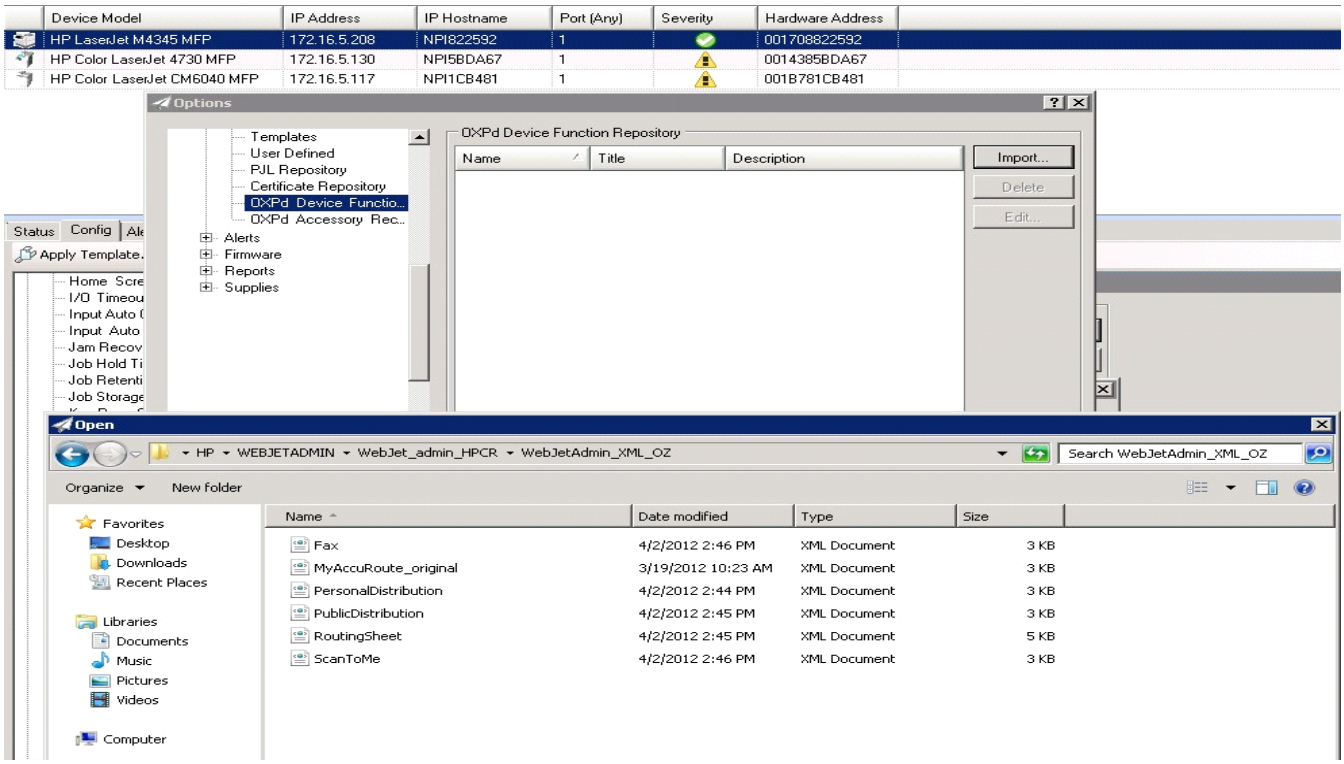
11. Click the **Add** button. The **Add OXPd Device Functions** windows is displayed.



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

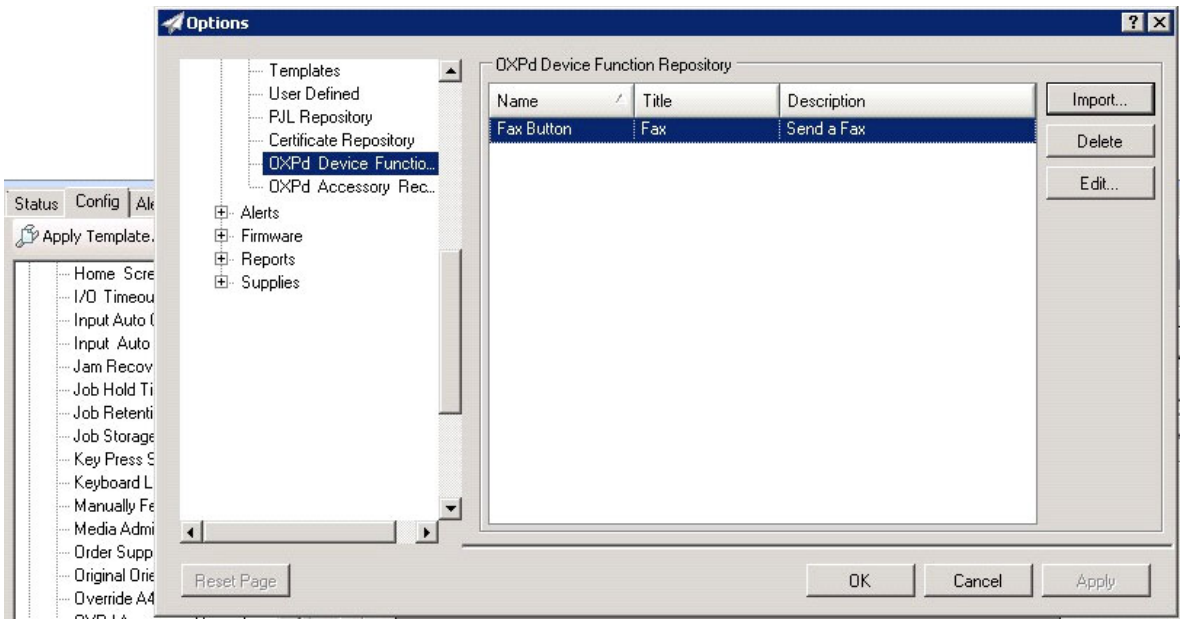


13. Click **Import**. In the **Open** window, search for your XML files.

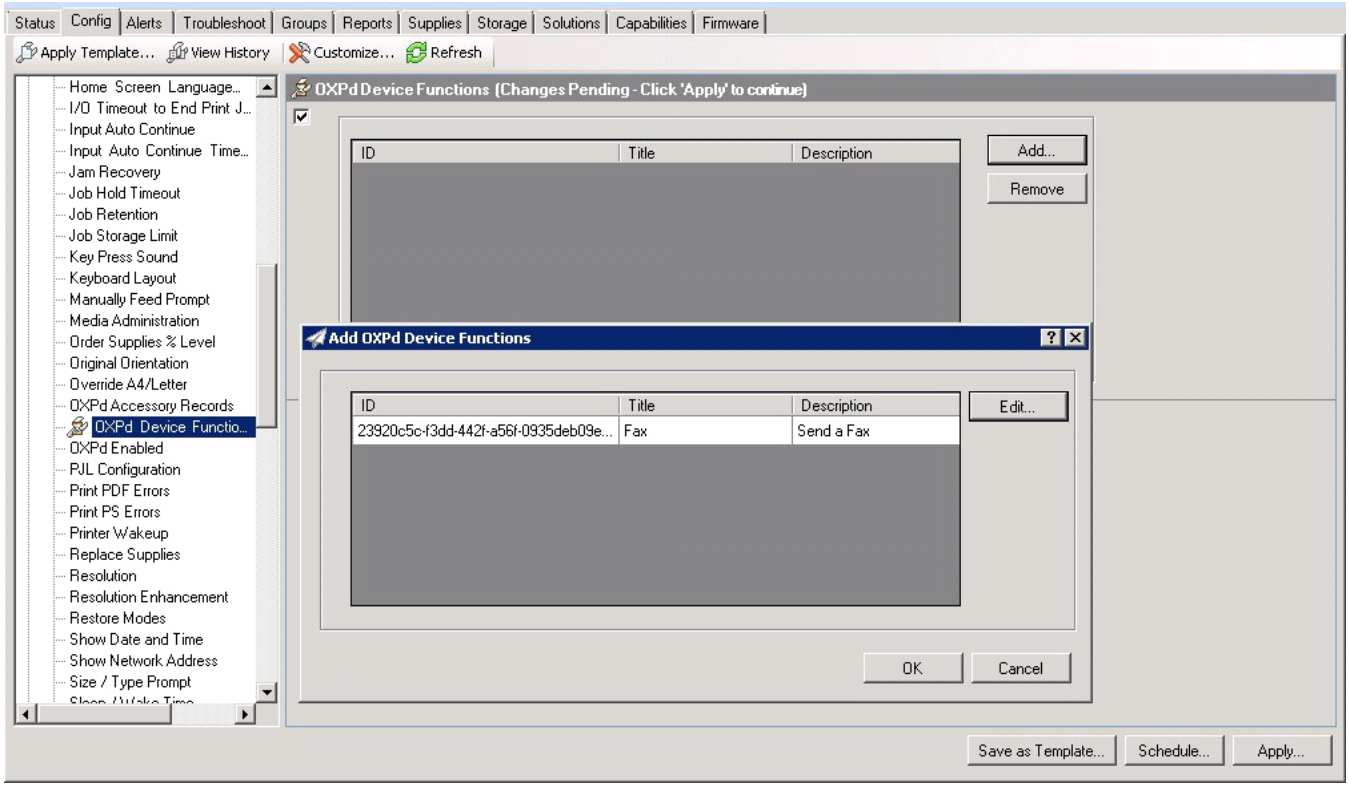


14. Select to highlight the file and then click **Open** to add the file. (You can import only one file at a time in the **Open** window.)

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

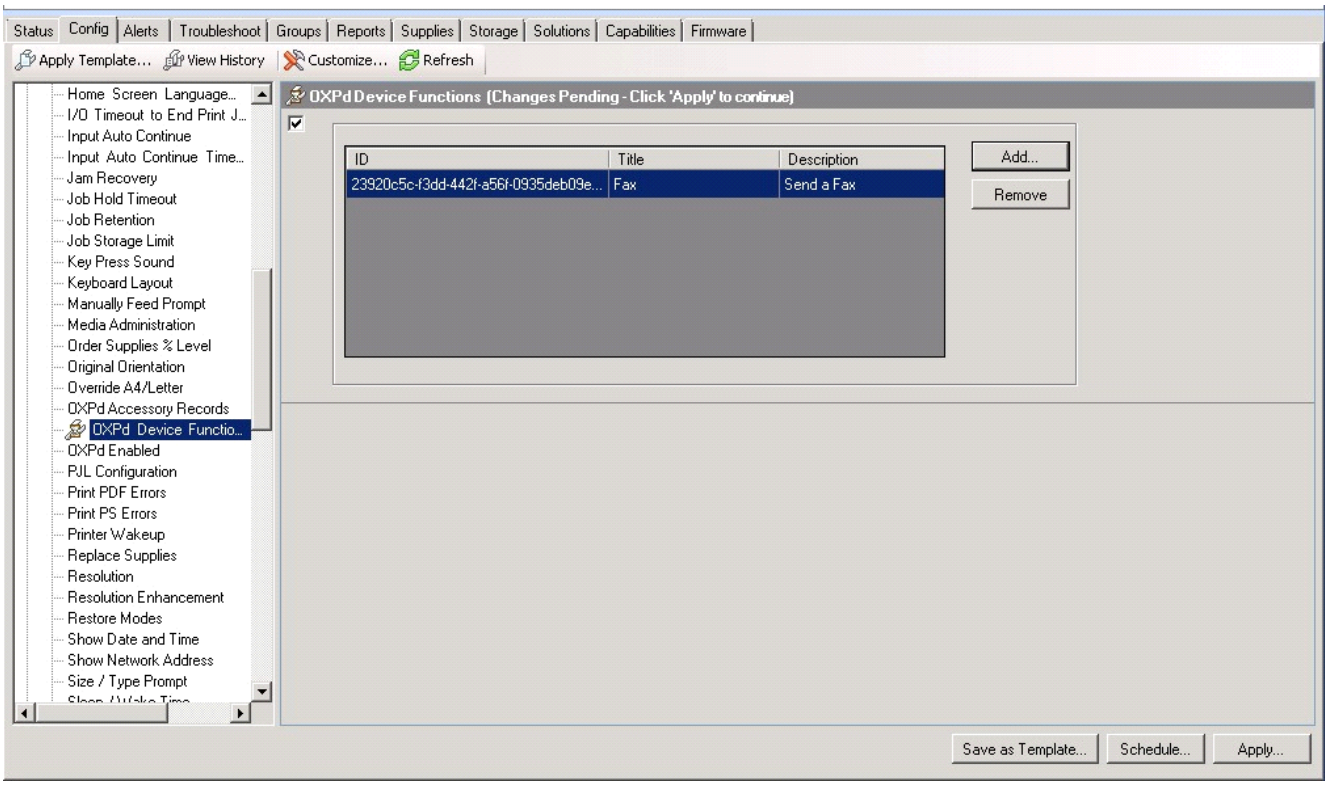


16. Click **OK**. The **Add OXPd Device Functions** window is displayed.

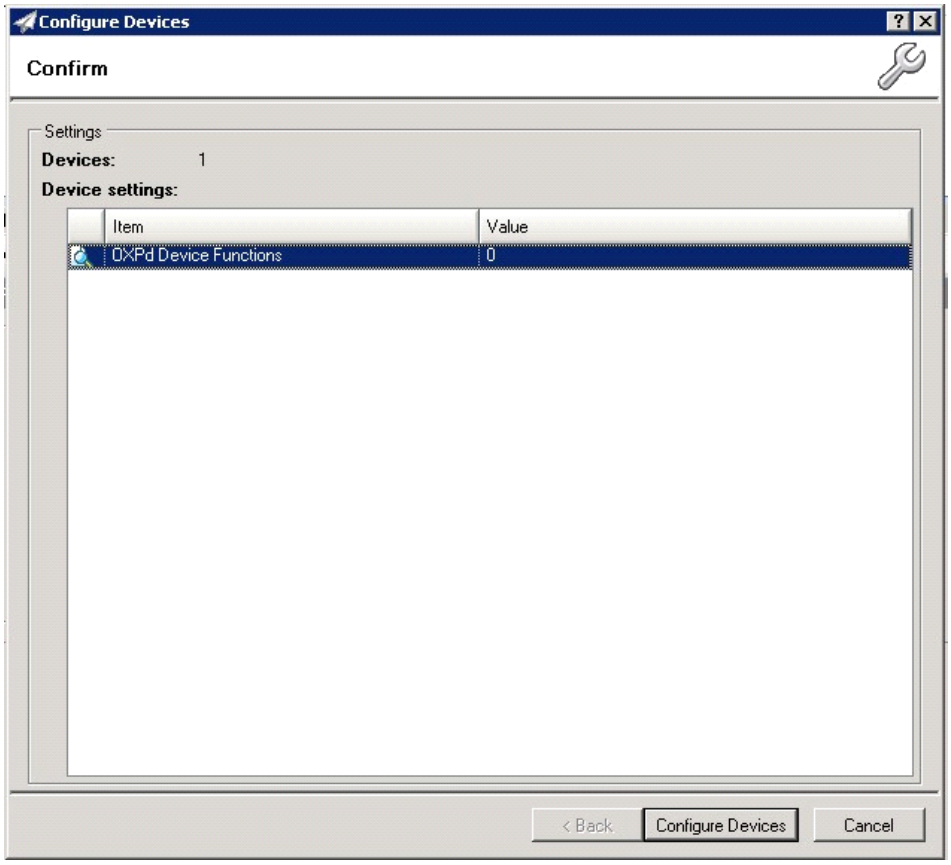


17. You should see the file referring to the feature(s) or button(s) you are about to install onto the device. Click **OK** to close the **Add OXPd Device Functions** window and return to the **OXPd Device Functions** window.

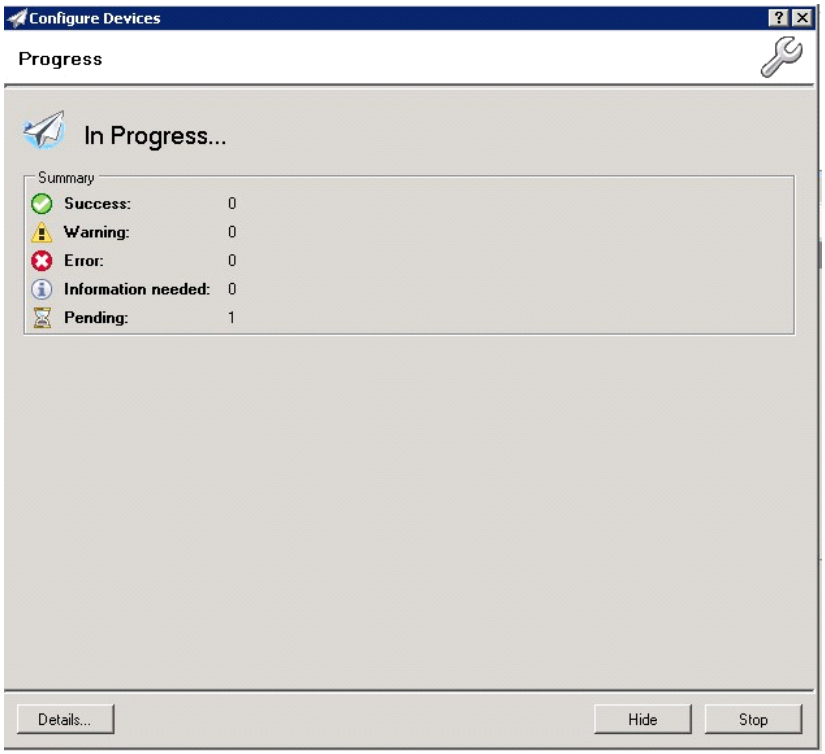
At this point, you can continue to add another feature or button (repeating Steps 11 through 16).



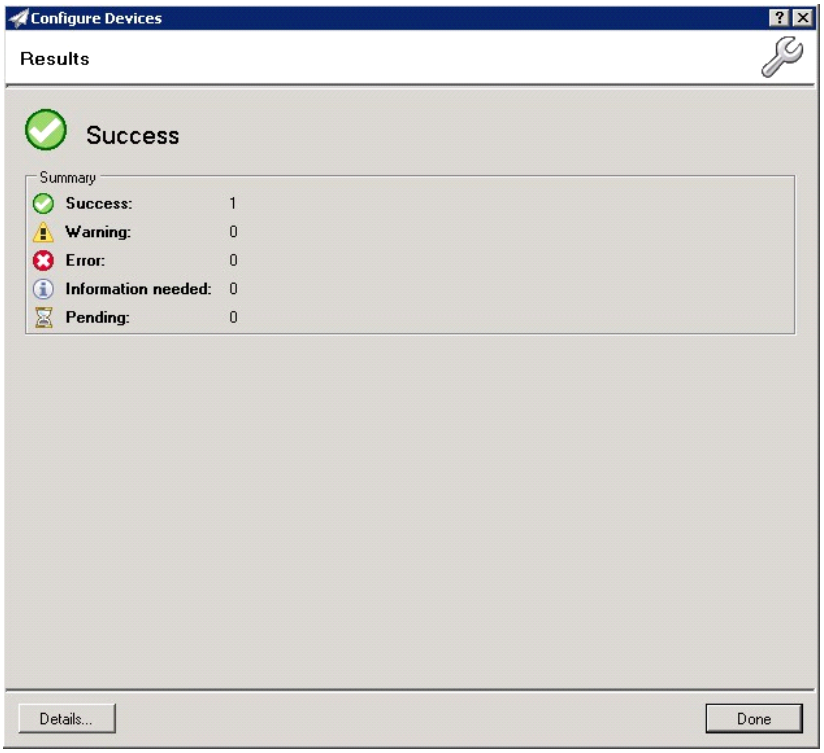
18. After you have added and confirmed all of the desired features/buttons, click **Apply**. The **Confirm** page is displayed.



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

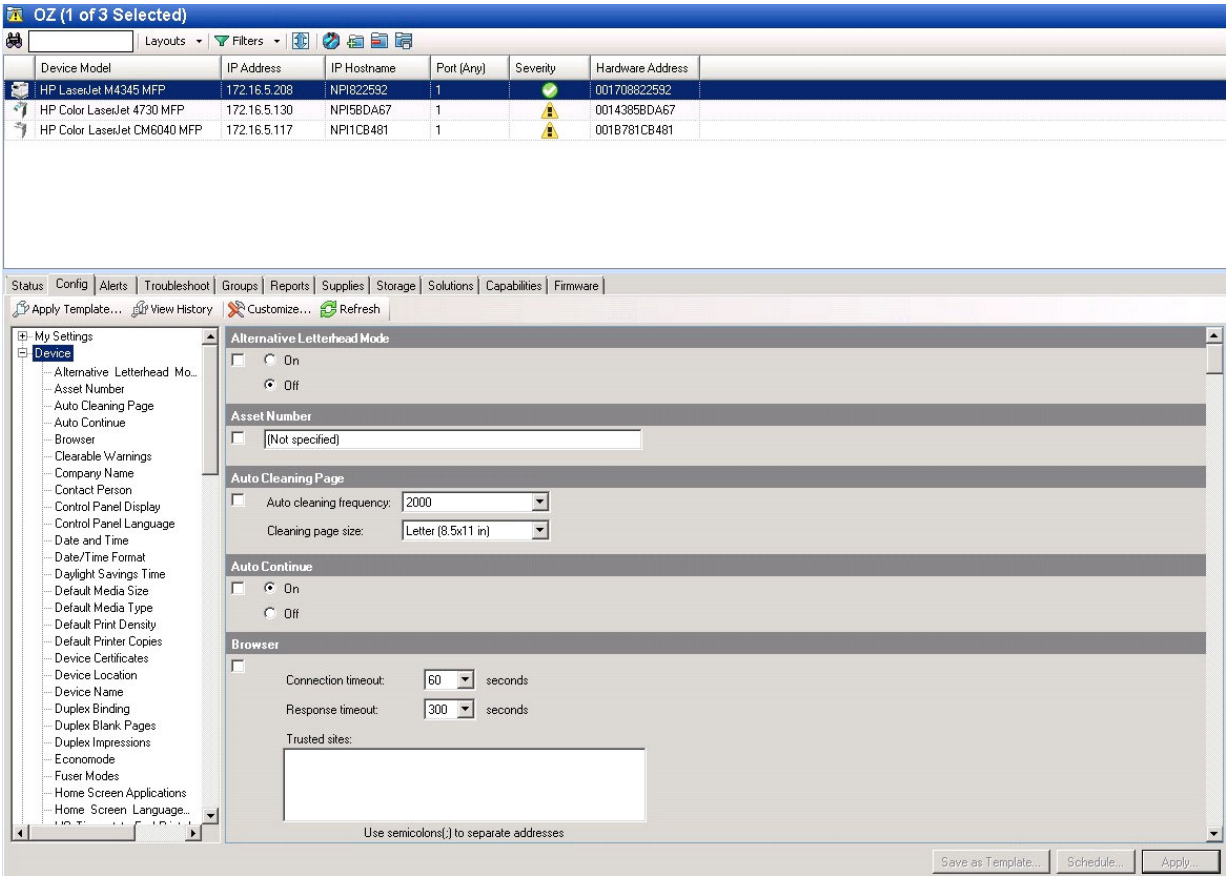


The **Results** screen will then indicate if the installation was successful or if an error was received.

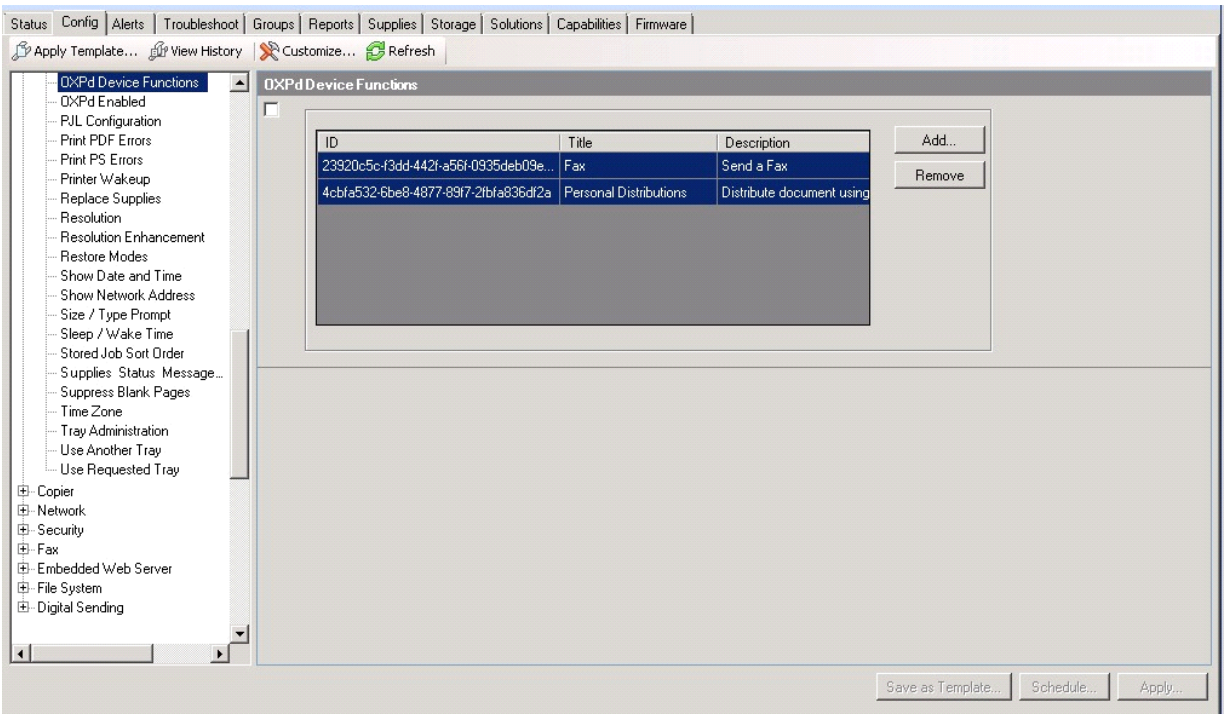


NOTE: You can click the **Details** button to show additional notes if an error has occurred.

20. Click **Done** to return to the main **Group** window, which defaults to the **Device** subset node.



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



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

6 Testing

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

6-1 Testing the Routing Sheet feature

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

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.

6-2 Testing the Device Administrator user interface

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

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

- Email
- PIN
- PIN with Password
- Login

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