upland AccuRoute

AccuRoute® Embedded Device Client Installation Guide

upland AccuRoute

Upland AccuRoute
6 Riverside Drive
Andover, MA 01810
Phone: (978) 327-5700
Toll-free US: 1-800 886-7845

Upland Software Headquarters
Frost Bank Tower
401 Congress Avenue, Suite 1850
Austin, TX 78701-3788
Toll Free: (855) 944-7526

Upland AccuRoute Resources

The Upland Community

The Upland Community is the central hub for Upland customer information, in the community you can:

- · Track tickets

- · Search and Download Knowledge

- · Interact in Upland Forums

- · Stay up to date on AccuRoute and/or Upland News

Access the Community by logging in with your company email at:

https://community.uplandsoftware.com/hc/en-us

Customer Service and Technical Support Contact Information

- · Phone: (978) 327 6800 or (1-888) 303 8098

- · E-mail: omtool-support@uplandsoftware.com

- · Community: https://community.uplandsoftware.com/hc/en-us

NOTE: Technical support requires an active support contract. For more information go to:

https://uplandsoftware.com/accuroute/customer-success/support-overview/

Sales, Consulting Services, Licenses and Training

- · Phone: (978) 327 5700 or (1-800) 886 7845

- · Email: ARmarketing@uplandsoftware.com

Contents

Section 6: Configuring HP MFP Devices

Section 7: Configuring Samsung Devices

Section 8: Configuring Xerox Devices

Section 9: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

Section 10: Testing

Section 11: Troubleshooting

Section 1: Introduction

AccuRoute features are accessible where the users need them most—on the web, office machines, multi-function devices, and business systems that are an integral part of the communication workflow.

This guide contains instructions for deploying the AccuRoute Embedded Device Client to multi-function devices.

> **Note** This guide is written for system administrators with detailed knowledge of the AccuRoute server and the devices.

This section of the guide includes:

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

Overview of AccuRoute Embedded Device Client

The AccuRoute Embedded Device Client brings the versatile document routing capabilities of AccuRoute to supported devices. These capabilities are founded in Omtool's Distribution Rule technology.

The AccuRoute Embedded Device Client runs on OXP (Open Extensibility Platform), an ASP.NET layer sitting between the device and the AccuRoute server. It communicates between the OXP SDK installed on the device and the AccuRoute server via the Embedded AccuRoute for Intelligent Device Client application.

Figure 1-1: **AccuRoute scanning features on the HP device running AccuRoute Embedded Device Client**

Each feature has a unique function that is detailed in the following table. (To see how each feature works on the device, go to Section 10: Testing, for the complete screen sequence of each feature.)

Table 1-1: **AccuRoute scanning features in AccuRoute Embedded Device Client**

Feature	Description	Login required	Notes
Fax	This option allows the user to perform 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 AccuRoute server via HTTP/HTTPS protocol. The AccuRoute server sends the fax to the intended recipients.	No	
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 Web Client, where they can configure Fax Release Schedule Calendars.
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 AccuRoute 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 AccuRoute Web Client (where the user can create the Distribution Rules and Routing Sheets).
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 AccuRoute 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 AccuRoute Web Client (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 Web Apps User Interface (where the user can create the Distribution Rules and Routing Sheets). |
| Routing Sheet | After the user selects Routing Sheet, the device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server then decodes the Distribution Rule and distributes the document to the intended recipients. | No | The device user must be able to generate Routing Sheets. This requires access to AccuRoute Web Client (where the user can create the Routing Sheets). |
| Scan to Destination

(formerly Scan to Folder, see Notes) | The device scans and delivers the document to the AccuRoute folder via HTTP/HTTPS protocol. The server picks up the scanned document from the network folder, processes it, and delivers it to the intended folder. | No | If you previously used "Scan to Folder" for this button, you must change the display text of the Scan to Destination button. This is described in Configuring button properties (4-12) during the device configuration. |

Table 1-1: AccuRoute scanning features in AccuRoute Embedded Device Client

Feature	Description	Login required	Notes
Scan to Distribution	After the user selects Scan to Distribution, the device scans and delivers the documents to a configured distribution.		
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 AccuRoute server picks up the scanned document from the network folder, processes it and delivers it to the intended folder.	No	
Scan to Me	The user selects Scan to Me and logs in to the device. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server processes the document using the device user's personal Scan to Me directive and distributes the document to the intended recipients. Or, the scanned document is emailed to the sender (the default).	Yes	Scan to Me is an advanced feature of AccuRoute Web Client. It enables the server to process all AccuRoute messages from the same user with the same Distribution Rule. Scan to Me requires access to AccuRoute Web Client (where the user can create the Distribution Rules and Routing Sheets). In addition, Scan to Me must be configured in the AccuRoute Web Client and on the server. For more information on this feature, consult Configuring button properties (4-12).
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 AccuRoute server (via HTTP/HTTPS protocol) where it is processed and distributed to the My Files section of the user Web Client client.	Yes	All jobs scan.
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 the intended recipients.	No	Mobile Reservations are generated by the Mobile Client and require a Mobile Client license.
Nested Buttons	The Nested Buttons feature provides the ability to configure one top-level button that all other AccuRoute buttons will display under, minimizing the front panel home screen real estate. For example, one button can be configured and labeled "AccuRoute." This button would be the only AccuRoute 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.
Device Information	This option allows users to access a screen of detailed information about the multi-function printer (MFP) with which they're working, including the device name, hostname, IP address, serial number, fax number, inbound/outbound fax support, and business unit.	No	Users can print the screen information to the device.

Table 1-1: **AccuRoute scanning features in AccuRoute Embedded Device Client**

Feature	Description	Login required	Notes
Job Queue	You can use the Job Queue option to obtain a list of jobs submitted to the AccuRoute server from a specific MFP or by a specific user. For all users, Job Queue can provide a list of all previously scanned jobs from an MFP or all faxes sent from the device. The system administrator configures the type of items that can be reported. For authenticated users, Job Queue can list any previously faxed items associated with the logged-in user.	Optional	Users can select any job from the list and print the job details to the device.
MyMessages	The MyMessages button offers authenticated users the ability to view and print their messages, including faxes. The system administrator defines the scope of message organization options available for users.	Yes	

Main components of the environment

The AccuRoute Embedded Device Client environment consists of the following components.

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

  > **Note** AccuRoute v6.0 installs the AccuRoute Intelligent Device Client as part of the server installation. No separate installation of this component is required unless the AccuRoute Embedded Device Client is installed on a remote system, and then the AccuRoute Intelligent Device Client would be installed on the remote system as well.

- **AccuRoute Embedded Device Client** - See Section 3: Installation for installation instructions.
- **HP Device** - See Supported devices (2-1) for a list.

Installation components

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

Table 1-2: **Description of installation components with locations and functions**

Component	Location	Function
AccuRoute Embedded Device Client Install	`...\Omtool\Omtool Server\Clients`	The setup contains the `setup.exe` file for the AccuRoute Embedded Device Client. Use this file to install the AccuRoute Embedded Device Client.
AccuRoute Embedded Device Client Configuration Manager	Devices node in the AccuRoute Server Administrator.	The Device Client Configuration node is a management tool installed with the AccuRoute Server Administrator, and is used to manage settings and options that will be available on the device. **Note:** A device license must be installed in order for the Device Client Configuration manager node to be used.

Document workflow

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

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

Workflow for the Fax, Routing Sheet, Scan to Destination, and Scan to Distribution features

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

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

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

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

Figure 1-2: **Workflow for Fax, Routing Sheet, Scan to Destination, and Scan to Distribution**

Workflow for the Fax Release feature

User authenticates at the device and either releases the document to be printed or leaves it in a "hold" state

...HPOXP\Output

AccuRoute Embedded Device Client for HP OXPd

Scanned document is sent to the Embedded AccuRoute for Intelligent devices via HTTP/HTTPs

...WebAPI File Transfer

Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) running on the web server

Database

Omtool server application

Dispatch component

Windows server

Fax arrives on the AccuRoute server, matches to a device listed on the DTT that has either a calendar-based or manual hold set, and remains queued on the server

A - An inbound fax arrives at the AccuRoute server and matches to a device listed in the Destination Translation Table (DTT) that has either a calendar-based or manual hold set. The fax remains queued on the server.

B - At the device, the user authenticates and either releases the document to be printed or leaves it in a "hold" state.

Figure 1-3: **Workflow for Fax Release**

Workflow for the Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files features

When a user begins a scan session with one of these options, the device requests the AccuRoute Embedded Device Client to retrieve Distribution Rules.

Note For Personal Distributions, Scan to Me, and Scan to My Files, the device user must authenticate himself at the device using the configured authentication type. See Configuring authentication (4-6).

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

Server sends requested Distribution Rules via the AccuRoute Embedded Device Client for HP OXPd and the Embedded AccuRoute for Intelligent Sevices

Scanned document is sent from the device to AccuRoute Embedded Device Client for HP OXPd via HTTP/HTTPs

...HPOXP\Output

...WebAPI File Transfer

AccuRoute Embedded Device Client for HP OXPd

Scanned document is sent from the AccuRoute Embedded Device Client for HP OXPd to the Embedded AccuRoute for Intelligent Services via HTTP/HTTPs.

Embedded AccuRoute for Intelligent Sevices (Omtool ISAPI Web Server Extension) running on the web server

Scanned document is sent by the Embedded AccuRoute for Intelligent Services via HTTP/HTTPs to the AccuRoute server where it is processed and routed to the intended recipients.

Database

Omtool server application

Dispatch component

Windows server

A - The user selects the Personal, Public Distribution, Scan to Me, or Scan to My Files feature. (If the user chooses Personal Distribution, he logs into the device.) The device requests the list of Distribution Rules from the server. The AccuRoute server returns the requested data. The user selects a Distribution Rule from the list and scans the document.
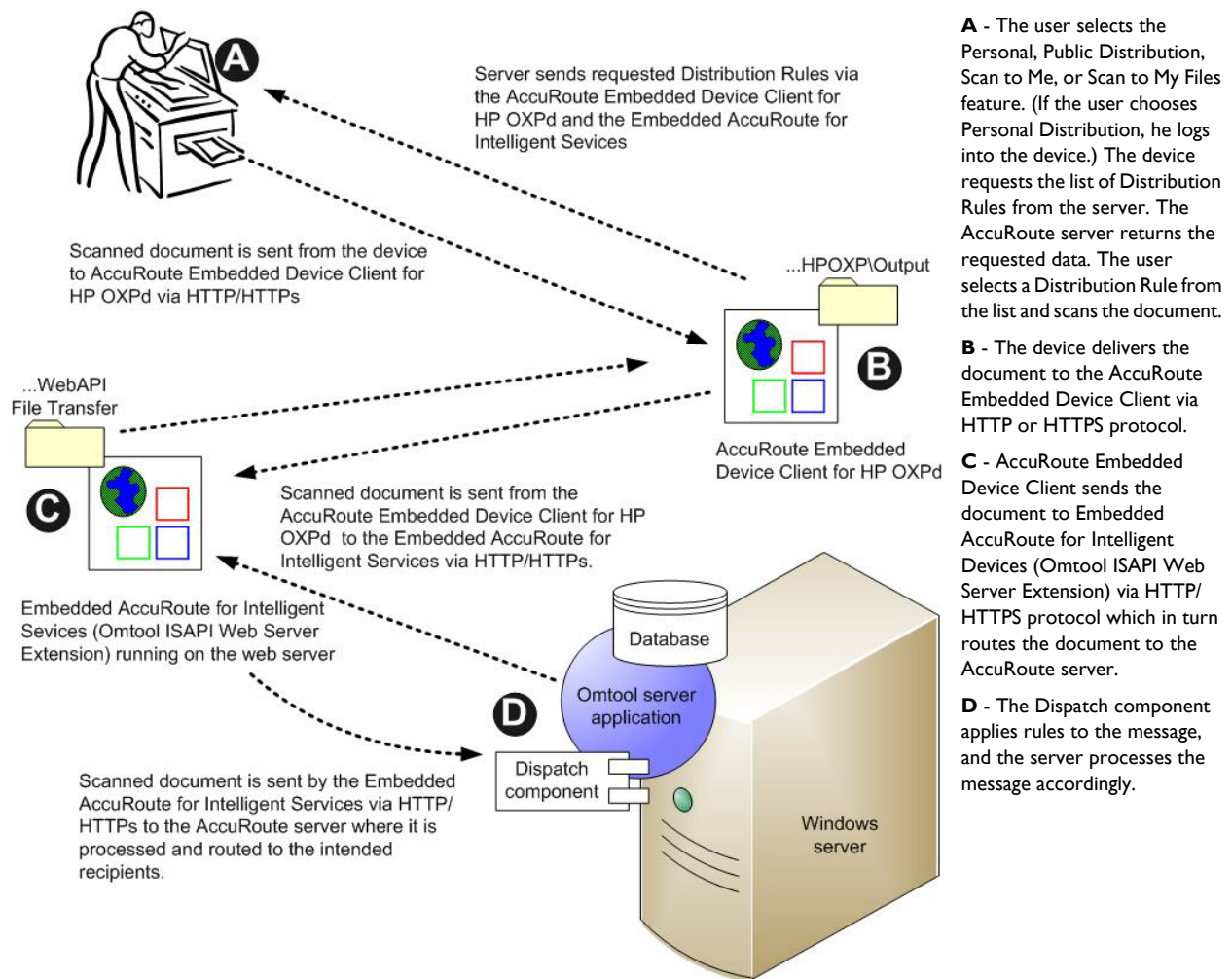
B - The device delivers the document to the AccuRoute Embedded Device Client via HTTP or HTTPS protocol.

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

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

Figure 1-4: **Workflow for Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files**

Deploying AccuRoute Embedded Device Client

1   Complete the installation requirements. ([Section 2: Requirements](#))

Note   If you are planning to use HTTPS protocol, you must create a CA certificate before installing the AccuRoute Embedded Device Client. Refer to the description of setting up a CA certificate using Microsoft Certificate Services and enabling SSL in [Section 3: Setting up a CA Certificate and SSL](#) (3-1).

---

2   Install the AccuRoute Embedded Device Client. ([Section 3: Installation](#))

3   Configure the embedded Web Server of the device. Refer to the description of required configuration in the *AccuRoute® Server Installation and Integration Guide,* which is available through [http://www.omtool.com/documentation/accuroute/6.0/documentation.htm.](#)

4   Configure the AccuRoute server. Refer to the description of configuring the server in the *AccuRoute® Server Installation and Integration Guide,* which is available through [http://www.omtool.com/documentation/accuroute/6.0/documentation.htm](#).

5   Configure optional capabilities. Refer as needed to

    a   ([Section 6: Configuring HP MFP Devices](#))

    b   ([Section 8: Configuring HP FutureSmart, OZ, and Pro Devices to Use the OPS Server Certificate for HTTPS environments](#))

    c   ([Section 7: Configuring Samsung Devices](#))

    d   ([Section 10: Configuring HP S900 Series MFP Devices](#))

    e   ([Appendix: Configuring HP Pro Devices on a Remote OPS Server with HTTPS Support](#))

6   Test the AccuRoute scanning features on the device. ([Section 10: Testing](#))

7   Troubleshoot the setup, if necessary. ([Section 11: Troubleshooting](#))

Related documentation

- AccuRoute v6.0 Server Installation Guide
- Omtool Server Administrator Help
- AccuRoute Embedded Device Client Quick Start Guides

Note   The quick start guides have been designed to be posted near the device, distributed to device users, and published on your organization's intranet.

For all documentation related to AccuRoute v6.0, consult the [AccuRoute v6.0 documentation page](#).

Section 2: Requirements

This section includes:

Supported devices

AccuRoute supports the AccuRoute Embedded Device Client on HP, Samsung, Xerox, and Ricoh devices.

For lists of supported devices, including models and firmware specifications, refer to the device-specific chapters:

- Section 6: Configuring HP MFP Devices (6-1)
- Section 7: Configuring Samsung Devices (7-1)
- Section 8: Configuring Xerox Devices (8-1)

For more information on Ricoh devices, see the *Embedded AcuRoute for Ricoh (ESA) Device Client Installation Guide*.

AccuRoute server requirements

The AccuRoute Embedded Device Client requires:

- ❐ AccuRoute server v6.0
  - ‣ with appropriate device license
  - ‣ fax-enabled to support fax-based features
- ❐ At least one fax-enabled connector to support fax-based features
- ❐ AccuRoute ISAPI Device Client (included with default server install)
- ❐ ASP.NET 3.5.1

Note To allow the installation prerequisite process to install Microsoft .NET 3.5.1, the system must have internet access. Microsoft .NET 3.5.1 is required to install the device client application.

Device authentication requirements

The AccuRoute 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. Refer to the *AccuRoute Server Installation Guide* ([AccuRoute v6.0 documentation page](#)).

The types of authentication are:

- **Device** authentication uses the native 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 user 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 AccuRoute.

Supporting large color documents

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

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

- Increase the **Sleep Schedule** from 10 minutes to the maximum, which is 4 hours.

- Increase the **Inactivity Timeout** in the device Embedded Web Server to 300 seconds.

- Increase the **Maximum allowed content length** value for **Request Filtering** to its maximum of 4294967295.

- Increase the **ASP > Session Properties > Time-out** value in Internet Information Service Manager (IIS).

Sleep Schedule

To increase the **Sleep Schedule**:

1   Log in to the Embedded Web Server on the MFP.

2   Select the **General** tab and locate the **Sleep Schedule** section in the left pane.

3   Increase the **Sleep Delay** value to the maximum allowable time – 120 minutes.

4   Click **Apply**.

Inactivity Timeout

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

1 Log in to the Embedded Web Server on the MFP.

2 Select the **General** tab and locate the **Control Panel Administration** menu.

3 Select **Administration** and click **Display Settings**.

4 Increase the **Inactivity Timeout** value to 300 seconds.

Request Filtering and Content Length

You need to set the **Request Filtering** value to its maximum of 4294967295. The **Content Length** must be modified on the DeviceClient, OXPd 1.6 and WebAPI sites.

To adjust the **Content Length** and **Request Filtering** settings in IIS:

1 Open Internet Information Services (IIS 7) Manager.

2 Select **DeviceClient** or **OXPd 1.6** 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 Click **OK**.

Note   Repeat steps 2-5 for **WebAPI**.

---

7 Reset IIS.

ASP Session Properties

To change the **ASP Session** settings in IIS:

1 Open Internet Information Services (IIS 7) Manager.

2 Select **Sites > DeviceClient**.

3 Double-click **ASP**.

4 Under **Services**, double-click **Session Properties**.

5 Increase the **Time-out** value to 1:20:00. The default is :20:00.

6 Click **Apply**.

7 Restart IIS.

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 AccuRoute 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.

Planning for HTTPS

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

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

- Without HP Pro devices, use a regular generated CA Certificate using Microsoft Certificate Services.

You must create the certificate before installing the AccuRoute 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 AccuRoute 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).

For information on using the OPS Server certificate, see HTTPS support using the OPS-created certificate (6-18).

Device Group Planning

The AccuRoute 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).

Section 3: Installation

This section includes:

Installing the AccuRoute Embedded Device Client

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

2 Navigate to the folder `C:\Program Files (x86)\Omtool\Omtool Server\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 **AccuRoute Embedded Device Client Configuration** page opens.
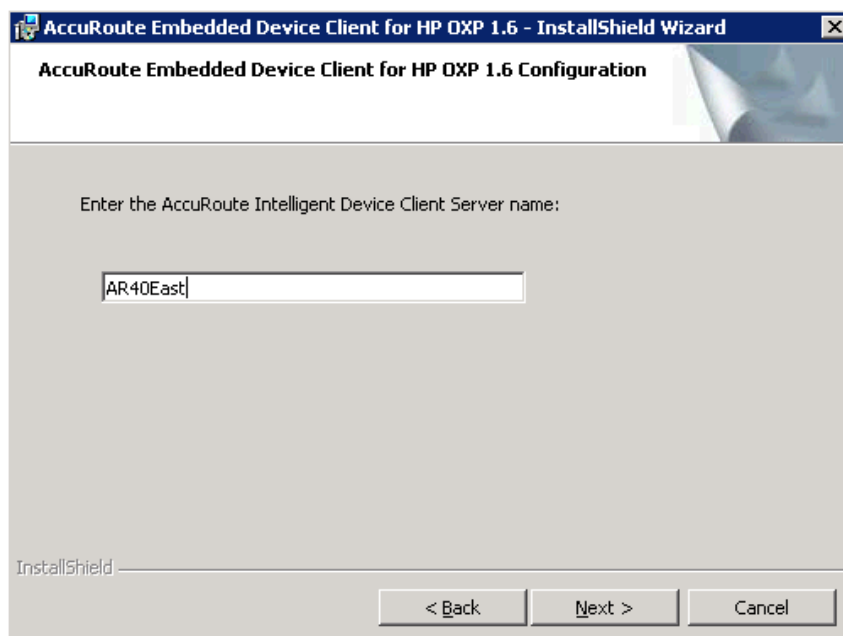
5 In the **AccuRoute Intelligent Device Client Server name** text box, enter the AccuRoute server name or the IP address of the AccuRoute Intelligent Device Client.

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

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

8 Click **Finish**.

Continue to .

Installing the AccuRoute Embedded Device Client on a remote system

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

> **Note** The system must be running Windows 2008 R2 SP-1 x64 or 2012 64-bit and must have Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) and AccuRoute v6.0 installed.

2 Navigate to the `\\Omtool\Omtool Server\Clients\DeviceClient` directory and run `setup.exe`.

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

3 Click **Next**. The **AccuRoute Embedded Device Client Configuration** page opens.

4 In the **AccuRoute Intelligent Device Client Server name** text box, enter the AccuRoute server name or the IP address of the AccuRoute Intelligent Device Client.

5 Click **Next**.

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

7 Click **Finish**.

8 Continue to .

Section 4: Creating Device Groups on the AccuRoute Server Administrator

This section describes:

Refer to Installing Buttons on a New Device (5-1) for steps to install the buttons onto the devices.

See also Section 10: Testing (10-1) and the AccuRoute server administrator on-line help (for additional information including optional configurations, testing, and troubleshooting).

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 the ability to use only the Routing Sheet, Personal Distributions, and Scan to Me features.

The following sections describe

- Creating a group (4-1)
- Configuring authentication (4-6)

Creating a group

1   Click **Start > All Programs > Omtool > AccuRoute Server Administrator**.

2   In the console tree, expand the AccuRoute server.

3   Go to the **Devices** node.

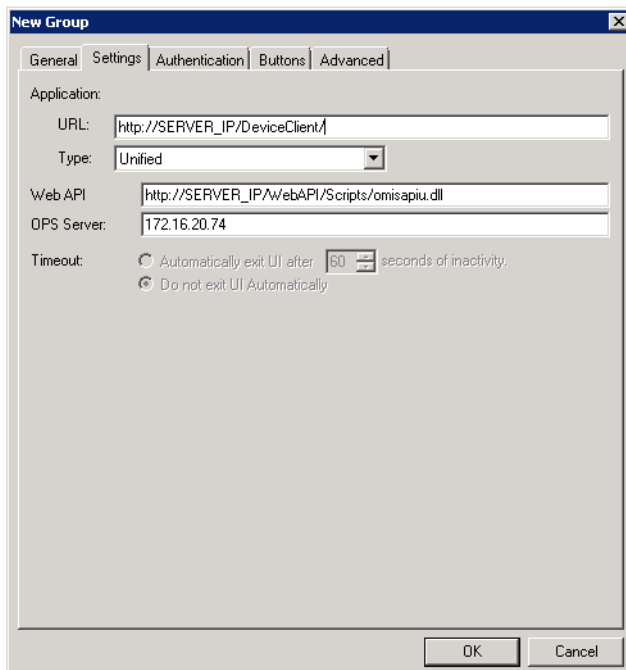4   Right-click and select **New > Embedded Device group**.
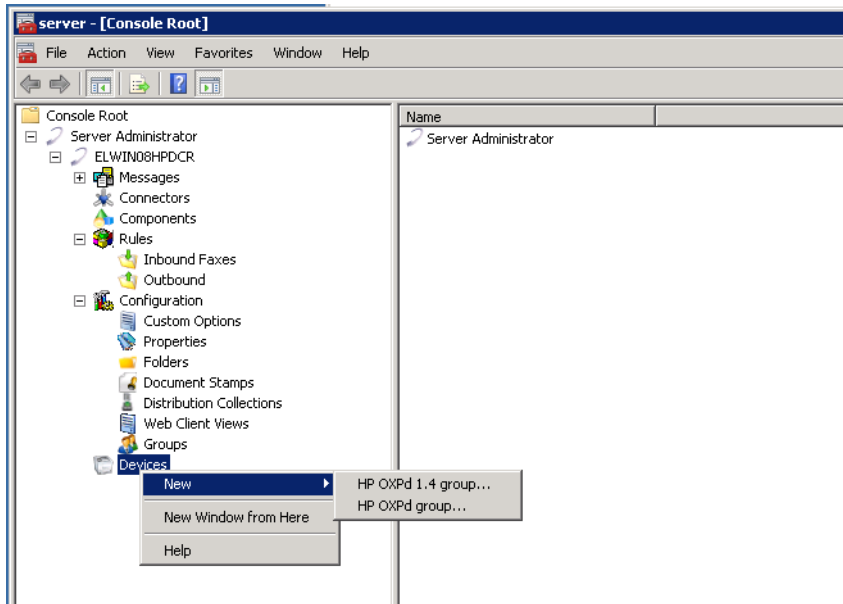
The **New Group** page opens.
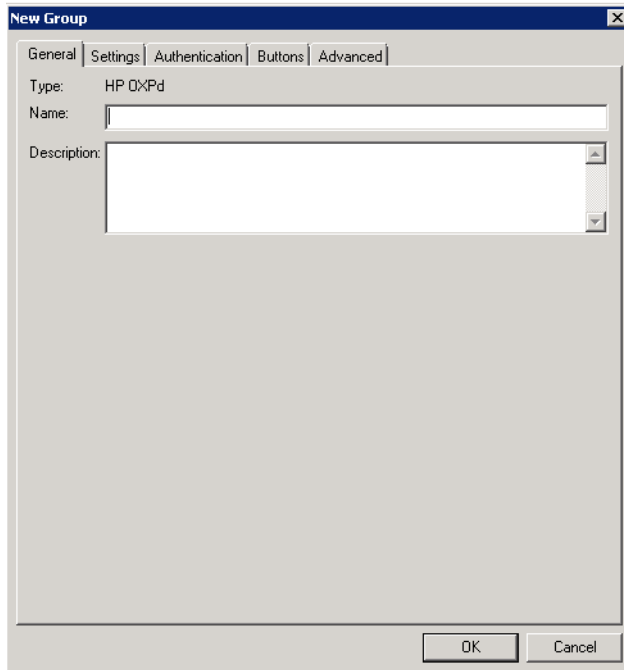
5   In the **Name** text box, enter a name for the device.

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.

- 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 AccuRoute 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 (4-3) through to Editing the OmISAPIU.xml file (4-5).

  Otherwise, continue the procedure below at Configuring authentication (4-6).

  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 **Embedded Device Client**.

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 **Embedded Device Client**.

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 the AccuRoute Embedded Device Client:
`.../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)\Omtool\Omtool Server\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 Configuring authentication below.

Configuring authentication

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

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

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

The following pages describe:

‣ Defining Domain Properties (4-7)

‣ Defining User Properties (4-8)

‣ Defining Password Properties (4-9)

Note HP Pro devices do not support the Device authentication method on their own. They require a stacked solution with another installed authentication service. An example would be HP AC authentication set in the Pro device when Device authentication is set in AccuRoute.

Defining Domain Properties

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

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** in the **Fields** section. The **User Field Properties** dialog appears:

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

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

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

- **User may not enter a value for User** - Do not select this option if you are using Email, Login, or PIN authentication. This option prohibits the user from entering a user value.

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

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

Note   User definition is required for **Login** authentication and optional for all other authentication types.

Defining Password Properties

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

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

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

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

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

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

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

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

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

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.

Continue with Specifying buttons for devices (4-10).

Specifying buttons for devices

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

- Adding new buttons (4-11)
- Configuring button properties (4-12)

Adding new buttons

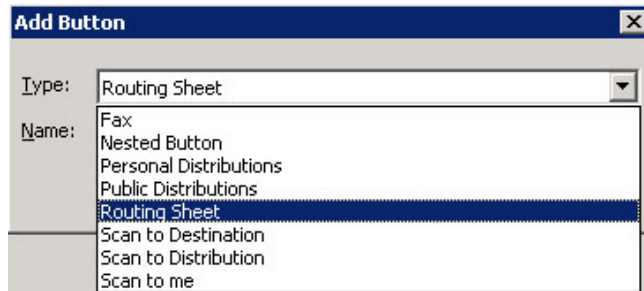**1** In **New Group Properties**, click the **Buttons** tab to add and/or remove buttons that appear on the device.
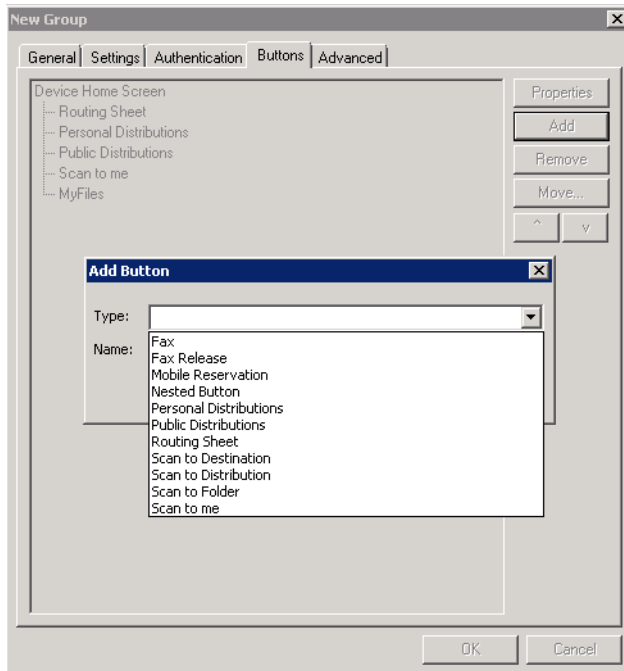
2 To add a button, click **Add**. The **Add Button** dialog is displayed.
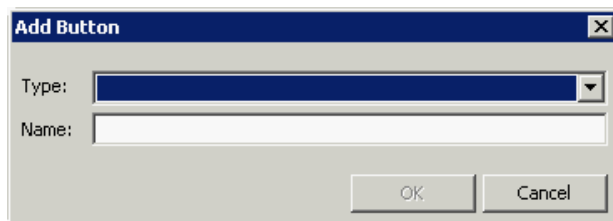
Note If the **Add** button is not active, click on **Device Home Screen**.

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

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

Continue with Configuring button properties.

Configuring button properties

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

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

- Personal and Public Distributions (4-14)

- Scan to Distribution (4-15)

- Fax (4-17)

- Routing Sheet, Scan to Destination, Scan to Distribution, Scan to Me, and Scan to My Files (4-19)

- Fax Release (4-21)

- Job Queue (4-24)

- Device Information (4-25)

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

- Defining Prompts (4-27)

- Defining Device Settings (4-28)

- Defining Advanced Device Settings (4-29)

General Properties

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

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

Note   Do not change **Image** from the default value.

Note   For buttons using **Require Authentication**, select **Capture user password** for the credential pass-through feature and **Always prompt user for password** for use with HPAC authentication.

---

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

- **Auto assign based on configured ordering** - The button is positioned based on a predefined order.

- **Use specific ordering priority** - You can enter a value to indicate the button placement. Position 1 is in the upper left location and position 2 is in the upper right location, in a Z-order layout. The pattern is as follows:

  > 1 2
  > 3 4
  > 5 6
  > etc.

3   Select 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 allows the user to visually preview the documents being scanned from the device. This only applies to **FutureSmart** devices.

▸ **Require authentication** - If you select this option, you can then indicate that the button should capture the user's password. Note that although the Routing Sheet feature typically does not require authentication, you can configure this requirement here.

Personal and Public Distributions

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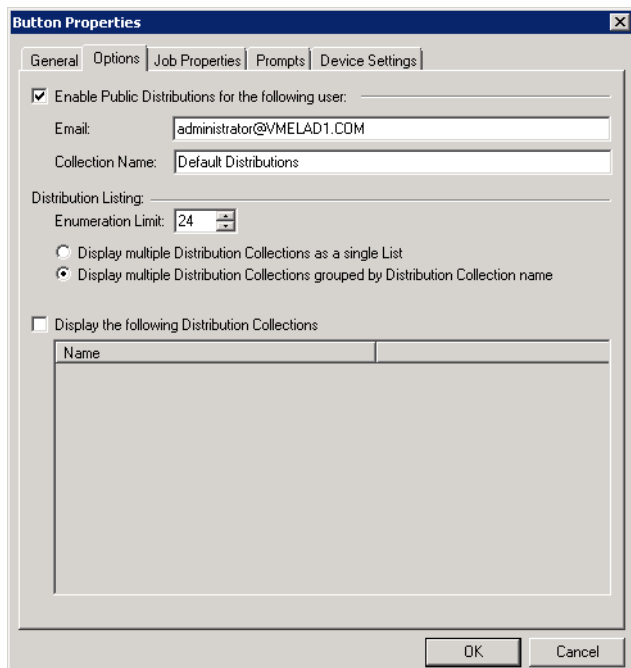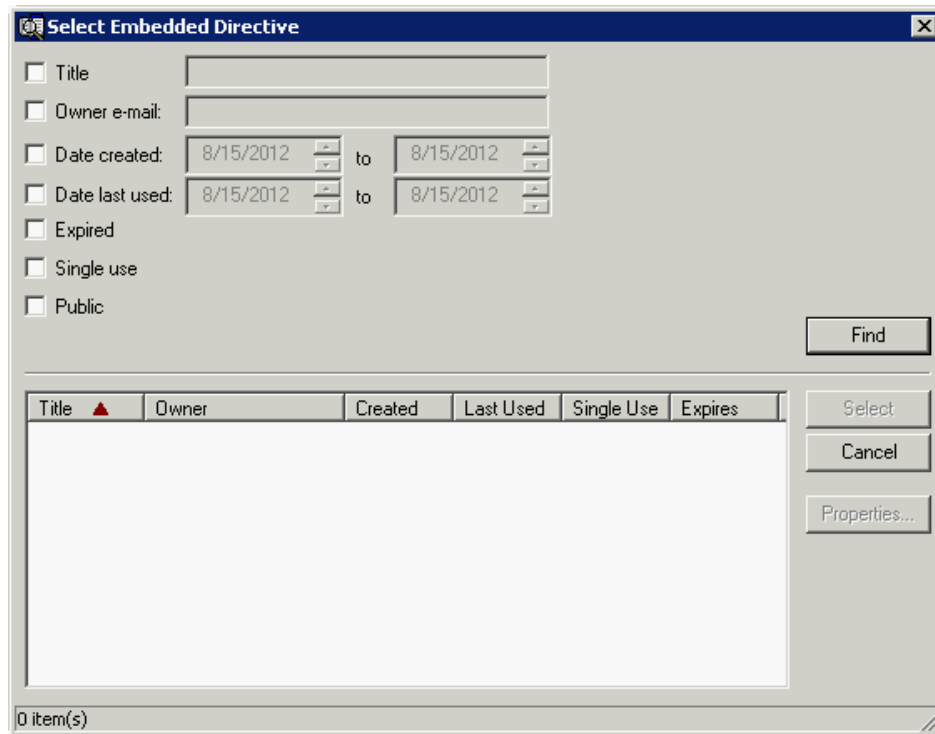

2   Enter a **Public Email** address (if applicable) and set the **Enumeration Limit** for distributions (the maximum number of distributions allowable).

Scan to Distribution

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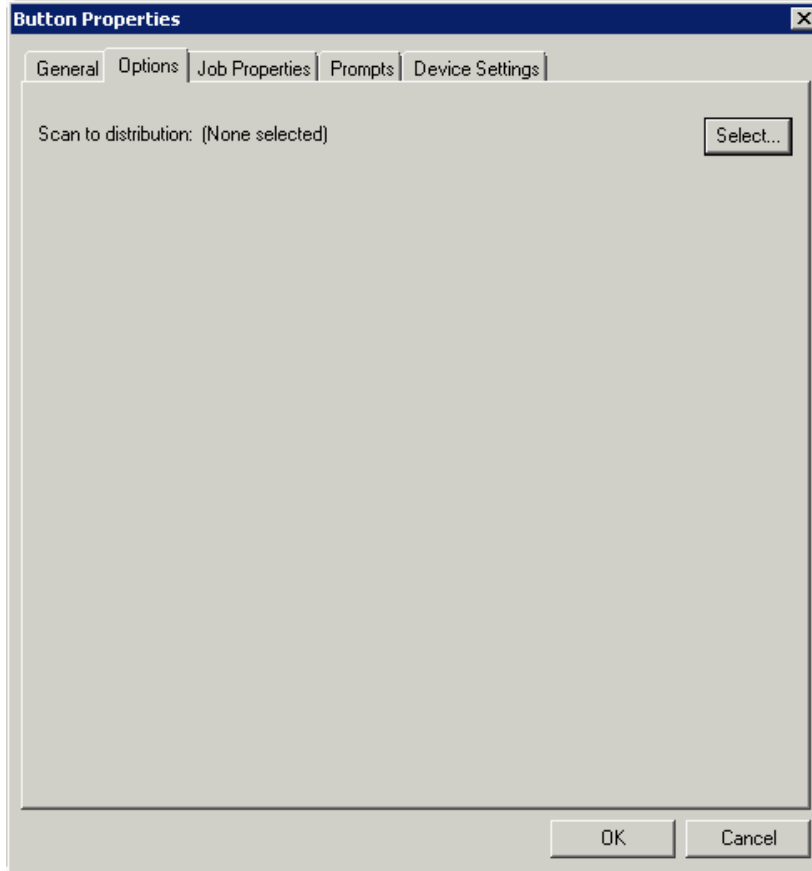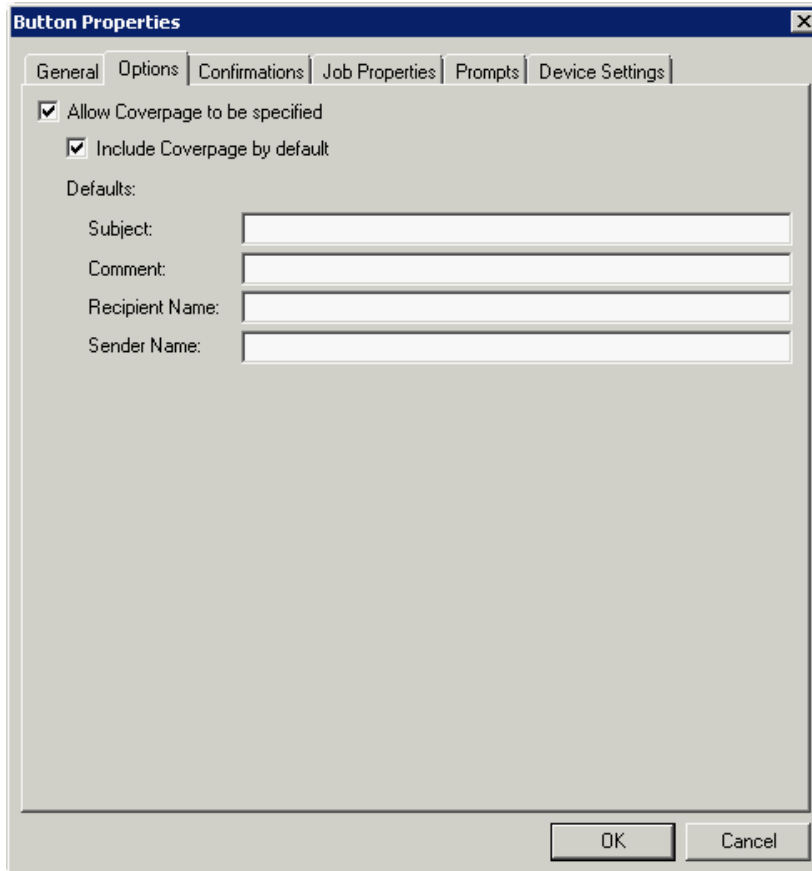
2   Click **Select** and the **Select Embedded Directive** dialog appears.

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

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

Fax

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

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

3   Next, click the **Confirmations** tab to:

▸   Allow authenticated and non-authenticated users to select the button.

▸   Define the type of fax confirmations (select a field and click **Properties**).

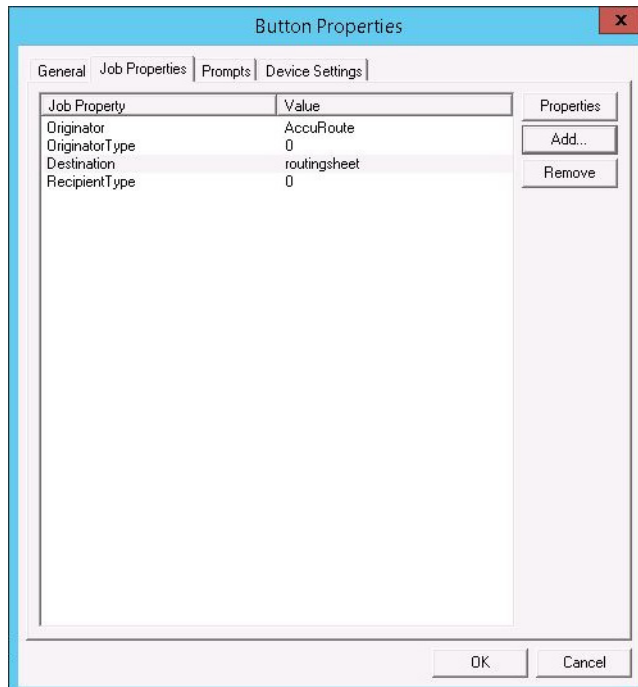▸   Add recipients for confirmations (click the **Add** button).

For example, you can edit the fields for the Originator for faxed faxes:
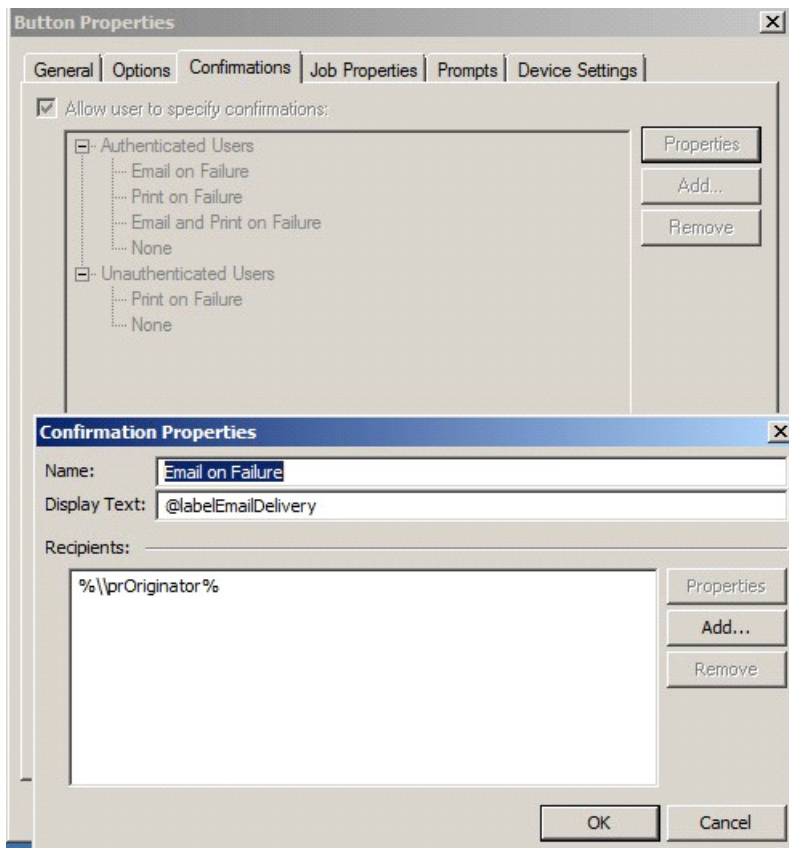
Routing Sheet, Scan to Destination, Scan to Distribution, Scan to Me, and Scan to My Files

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

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

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

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

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

‣ You can also add Transformations here.
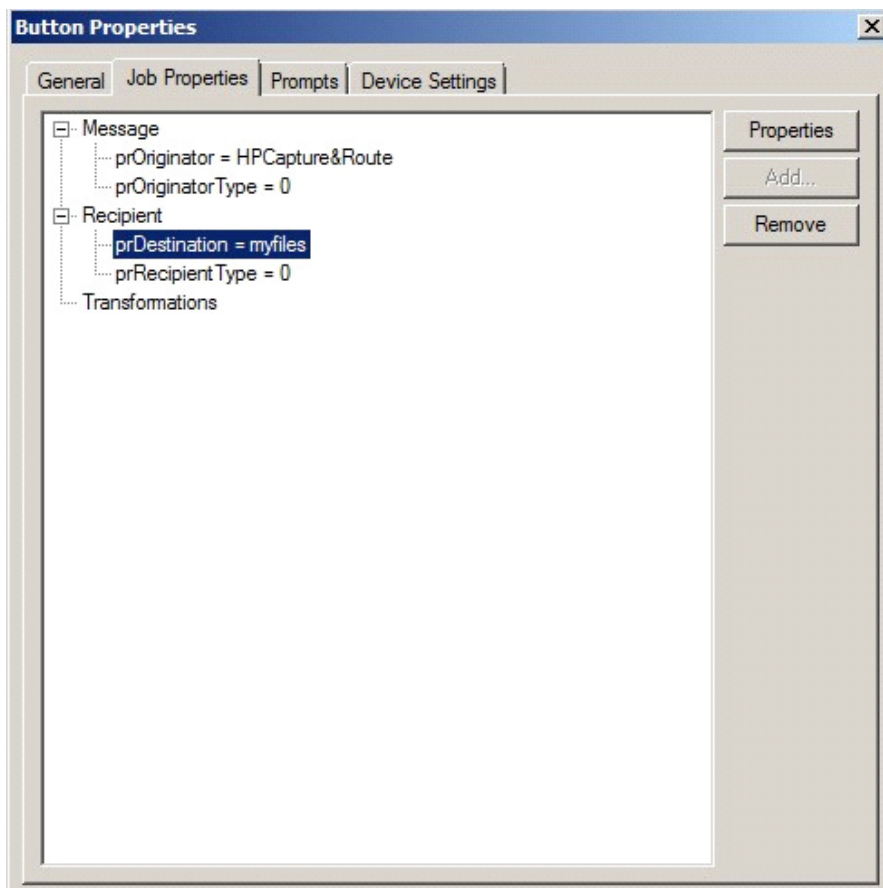
Fax Release

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

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

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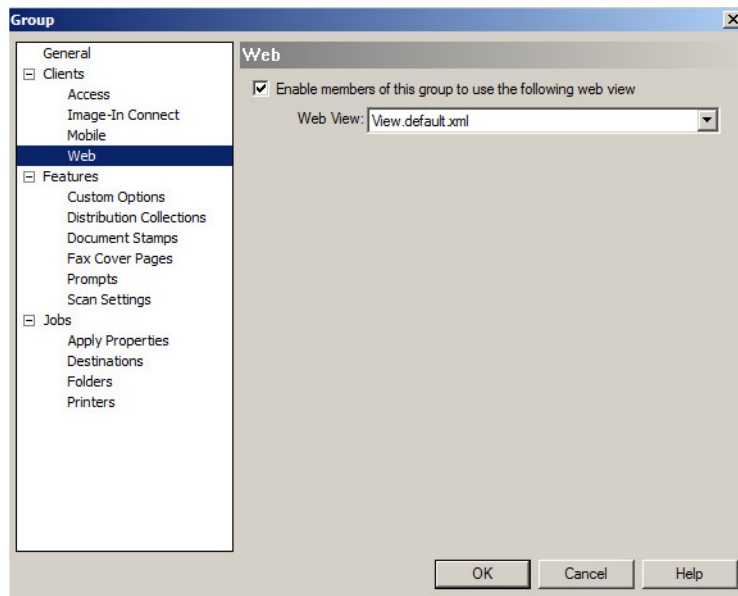

3 From the **Web View** drop-down menu, select the **Web View** for which you will enable Web Client Administration access. Click **OK**.

4 In the Server Administrator, go to **Configuration > Web Client Views** node. Double-click the Web Client View identified in the prior step to open the **Web Client View Properties**.
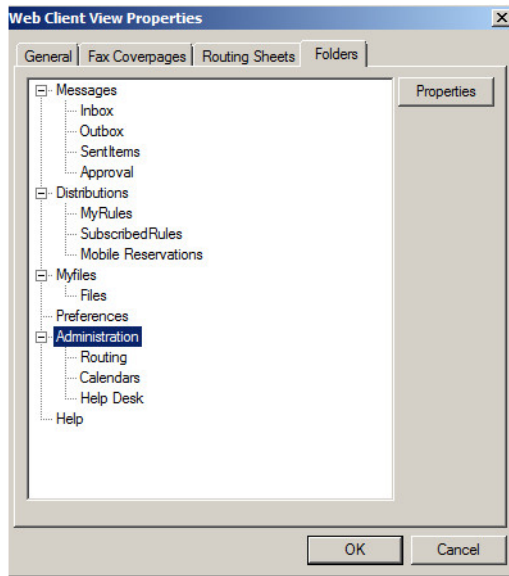
5 On the **Folders** tab, double-click **Administration** and select the **Display this folder** check box. Click **OK** and **OK** again.

6 Open the Web Client and select **Administration > Calendars**. Click **New** to create a new **Fax Release Scheduling Calendar**.
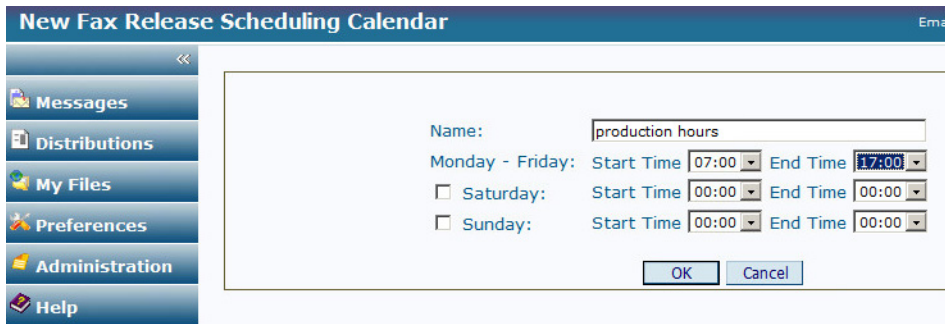
7 In the **Calendar**, define the time periods within which you want to allow authorized users to manually release faxes.Click **OK**.

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

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

10 On this screen you can

▸ Associate a **Device Serial Number** or **Business Unit**.

▸ Enable **Manual Hold** for all faxes from this number.

▸ Enable **Fax Release** and assign a specific **Calendar** (such as the one created in step 7) to guide its use.

▸ Assign a **Manual Override Pin**.

▸ Assign a **Destination** for these faxes, with options such as a specific device, a regulated printer, or another destination, such as email or a Folder.

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

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

11 Click **OK**.

Job Queue

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

To enable the DTT in the Web Client for Administrative users:

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

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

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

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

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

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

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

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

8 Click **OK**.

To add a device as a destination in the DTT:

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

2 In the address bar, enter the URL for the End User Interface. The default value for this is

    http://<ServerName>/WebClient

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

4 Enter the following information on the **New Routing Destination** page:

   a **Fax Number**: Enter the fully normalized fax number. For example: +10005551234

   b **Device Serial Number**: Enter the serial number for the HP device.

   c For the **Manual Hold** option, check the **Hold all jobs** option if all jobs to this device number are to be held indefinitely.

   d If you selected the **Manual Hold** option, go to the **Manual Override Pin** text box and enter the PIN value to be used for enabling or disabling Manual Hold.

   e **Fax Release Calendar**:

      ▲ Check the **Enabled** option.

      ▲ Select the **Calendar** from the drop-down menu.

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

---

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

- For the **Print on Device Printer** option, provide the device IP Address or the UNC path to the device.

  If using a Regulated Printer, select the **Regulated Destination** check box and enter the IP Address or the UNC path to the regulated printer.

  You can select the **Print on specific Media** check box and identify from the drop-down menu the paper size on which incoming faxes will be printed.

  You can also select the **Apply Document Stamp** check box and choose the stamp type of interest from the drop-down menu.

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

- For the **Email/UNC** option, select either **E-mail** or **UNC** and enter the email address or UNC path in the **Destination** text box.

  You can define a specific document format from the **Delivery Format** drop-down menu.

  You can also specify a document name in the **Delivered Document Name** text box.

5   **5.**Click **OK**.

Device Information

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

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

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

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

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

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

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

---

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

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

8   Click **OK**.

To add a device as a destination in the DTT:

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

2 In the address bar, enter the URL for the End User Interface. The default value for this is

`http://<ServerName>/WebClient`

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

4 Enter the following information on the **New Routing Destination** page:

a **Fax Number**: Enter the fully normalized fax number. For example: +10005551234

b **Device Serial Number**: Enter the serial number for the HP device.

c For the **Manual Hold** option, check the **Hold all jobs** option if all jobs to this device number are to be held indefinitely.

d If you selected the **Manual Hold** option, go to the **Manual Override Pin** text box and enter the PIN value to be used for enabling or disabling Manual Hold.

e **Fax Release Calendar**:

- ▲ Check the **Enabled** option.

- ▲ Select the **Calendar** from the drop-down menu.

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

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

For more information about the Administration features of the End User Interface, see the 'Customizing the HP CR End User Interface' section of the [AccuRoute Server Administrator Help](#).

---

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

- ▲ For the **Print on Device Printer** option, provide the device IP Address or the UNC path to the device.

  If using a Regulated Printer, select the **Regulated Destination** check box and enter the IP Address or the UNC path to the regulated printer.

  You can select the **Print on specific Media** check box and identify from the drop-down menu the paper size on which incoming faxes will be printed.

  You can also select the **Apply Document Stamp** check box and choose the stamp type of interest from the drop-down menu.

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

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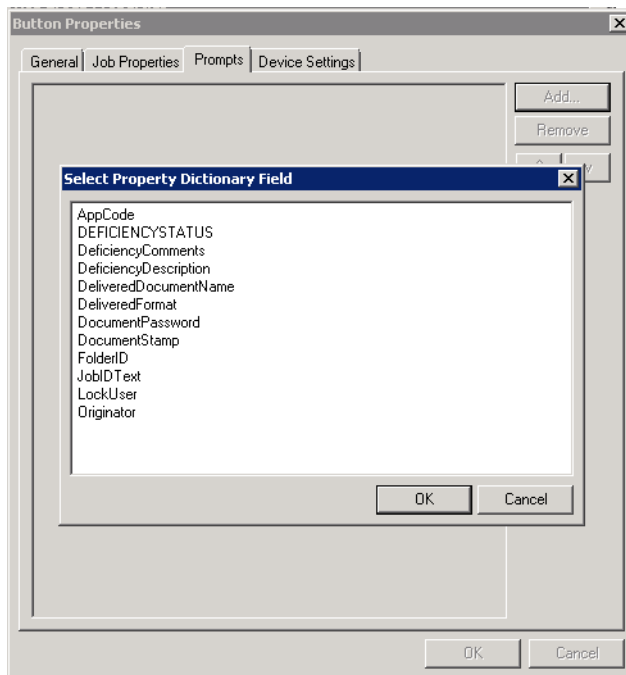
  You can define a specific document format from the **Delivery Format** drop-down menu.

  You can also specify a document name in the **Delivered Document Name** text box.

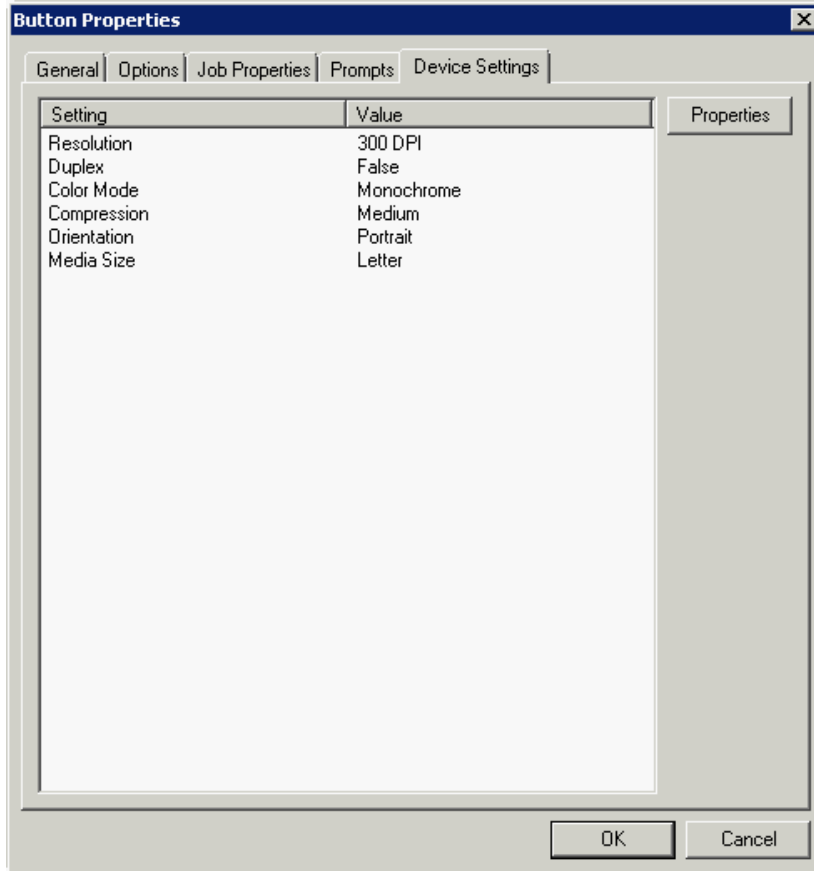**5** Click **OK**.

Defining Prompts

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


Select a prompt and click **OK**.

Defining Device Settings

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

Select a setting and click **Properties** to change the setting value. For example:
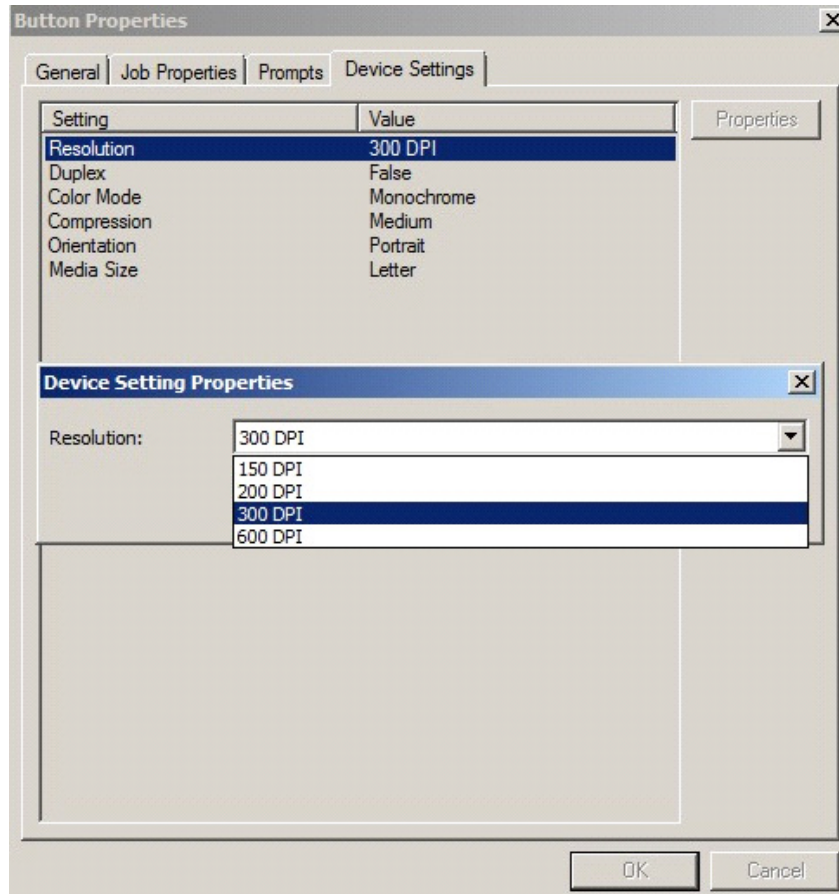
Note   The HP Officejet Pro 276dw does not support 600 x 600 scanning with the AccuRoute Embedded Device
Client.

---

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


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

Defining Advanced Device Settings

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

Note	Advanced features are for adding additional property metadata as part of a message to allow for advanced product capabilities. Please contact Customer Support for assistance with this feature.
	Take note of all defaults before changing any of these settings.
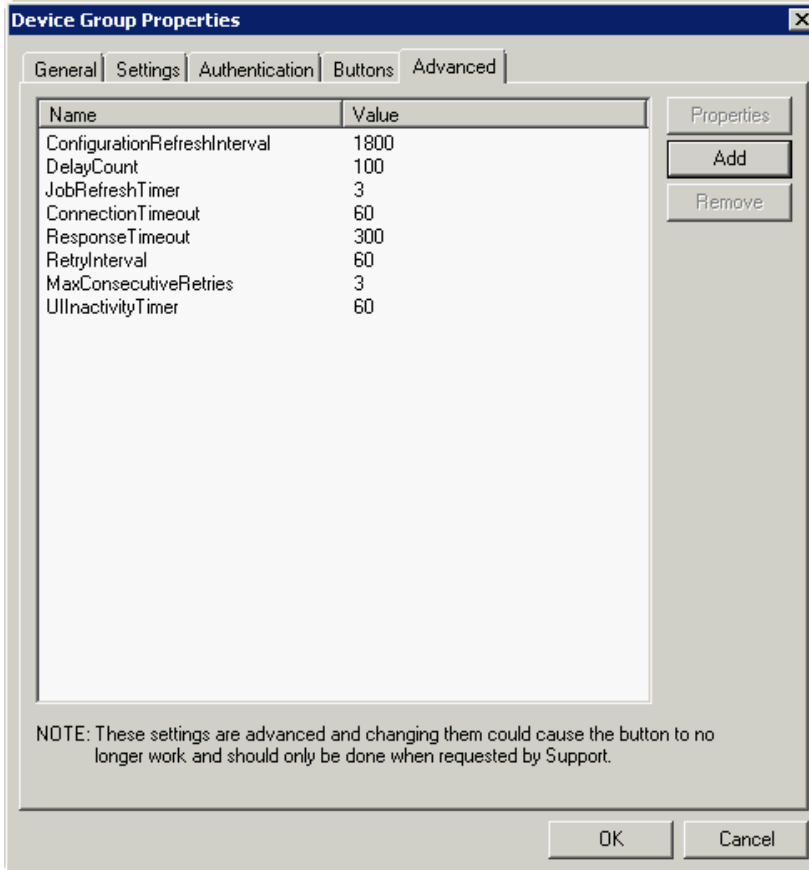
10 Click **OK** to complete the **Device Group Properties**.

11 Once a button configuration is complete, you can install devices using the configured Device Group settings, and the xml files can be exported for importing into AccuRoute'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 AccuRoute Embedded Device Client buttons (9-4).

Updating the Deviceloader.xml to support new devices

If you need to update the `Deviceloader.xml` to include new devices, refer to the AccuRoute server administrator on-line help.

Section 5: Installing Buttons on a New Device

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

See also and the AccuRoute server administrator on-line help (for additional information including optional configurations, testing, and troubleshooting).

Adding a new device and installing buttons

1   In the console tree, expand the AccuRoute server and go to the **Devices** node.

2   Select the group to which you want to add a device. Then, right-click and select the **New > Device**. The **Properties for device** page opens.
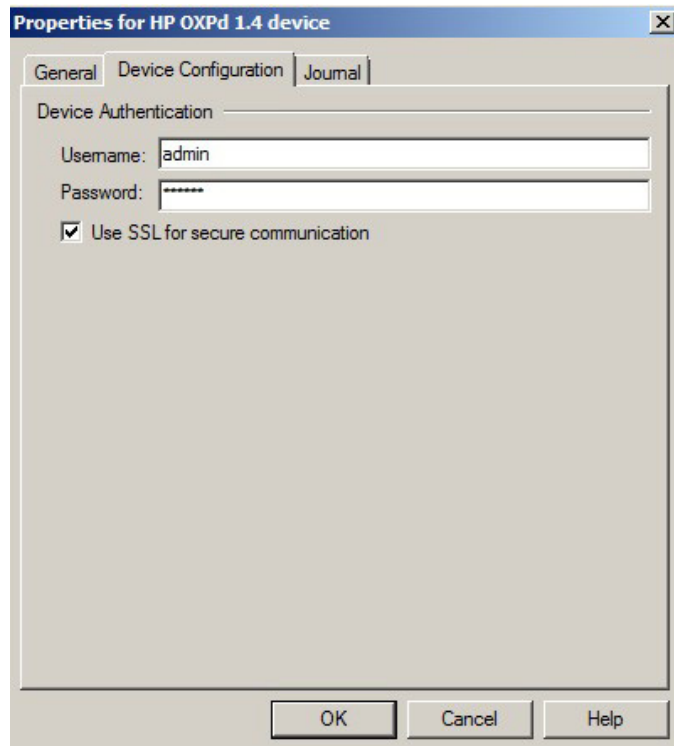
3   In the **Name** text box, enter a name for the device.

4   Optionally, in the **Description** text box, enter a device description.

5   In the **Network Address** text box, enter the device IP address.

6   Click the **Connection** tab. The following example is for HP OXPd v1.6 or OXPd 1.7 devices:
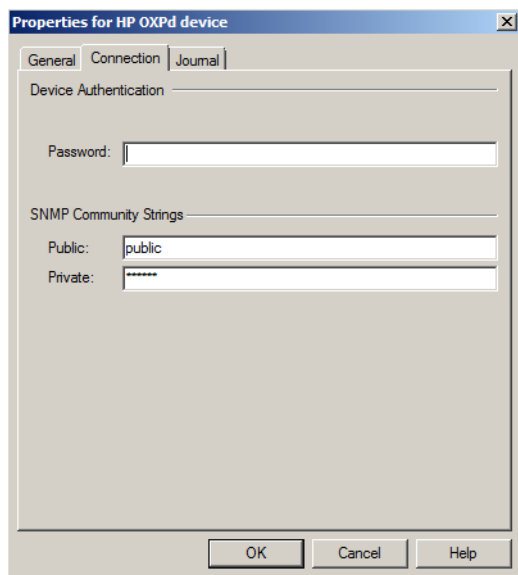
> **Note** When installing to an AccuRoute Embedded Device Client device using HTTPS, you must enter the device Administrator name in the **Username** text box and select the **Use SSL for secure communication** option, as below.

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 the AccuRoute Embedded Device Client, 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** to install buttons on your device.

13   Verify that the buttons appear on the device.

Configuring device authentication

When you select Device Authentication from the Device Group properties, you need to complete the following configuration at the device in order to properly identify the logged-in user (for button options such as **Personal Distributions** or **Scan to My Files**).

Configuration options include:

- Configuring LDAP authentication (5-4)

- Configuring AccuRoute device authentication (5-5)

Note   HP Pro devices do not support LDAP authentication.

Configuring LDAP authentication

When you choose LDAP Authentication, the user is prompted to enter an email username and password. The Authentication Manager uses the login credentials to initiate a lookup. The lookup validates the user and returns the user's email address. Then the AccuRoute Embedded Device Client uses the email address to request information from the AccuRoute server, such as a list of the user's Personal Distributions. When the scan is submitted to the AccuRoute 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 in Defining Password Properties (4-9) for details.

The following figure is an example of an LDAP Authentication configuration for Active Directory. (For information on configuring LDAP Authentication, consult [AccuRoute v6.0 Documentation](#).)

Figure 5-1: **Example of an LDAP authentication configuration for Active Directory (2 screens)**

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

Configuring AccuRoute device authentication

1   Open a Web browser and enter the device IP address.

2   Log in to the Embedded Web Server. All options become available.

3   Go the **Settings** tab and click **Authentication Manager**.

4   Locate the following AccuRoute functions:

‣ Scan to My Files

‣ Personal Distributions

‣ Scan to Me

The list shows the options that are installed with the AccuRoute Embedded Device Client, so it can contain all, some, or none of these functions.

5   For each of the features listed above, click the drop-down menu.

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

7   Click **Apply**.

Configuring the server

When a message arrives on the AccuRoute 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 AccuRoute scanning features.

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

When rules have been created for all AccuRoute scanning features available on devices in your environment, the AccuRoute server is fully configured for the AccuRoute Embedded Device Client. Now you are ready to test the AccuRoute scanning features. Continue with the information in Section 10: Testing (10-1).

Section 5: Installing Buttons on a New Device

Section 6: Configuring HP MFP Devices

This section describes the configuration steps for several types of HP MFP devices, including the HP S900, HP Pro, FutureSmart, and OZ devices. The configurations vary in types of certificates and how to set up HTTPS for SSL.

Select from the following sections as appropriate to your system environment:

- Supported HP devices

- Configuring HP S900 Series MFP Devices

- Configuring FutureSmart and OZ devices

- Configuring HP Pro Devices (only)

- Configuring HP Pro Devices on a remote OPS Server with HTTPS support

- Configuring HP FutureSmart, OZ, and PRO devices to use the OPS Server Certificate for HTTPS environments

Supported HP devices

Omtool supports the AccuRoute Embedded Device Client on all the devices listed in this section..

Table 6-1: **List of devices supported with the AccuRoute Embedded Device Client**

Device	Group	Supported firmware	OXPd Version
LaserJet M3035 MFP	20	48.301.7	1.6.3.2
LaserJet M4345 MFP	20	48.301.7	1.6.3.2
LaserJet M4349 MFP	20	48.301.7	1.6.3.2
LaserJet M5035 MFP	20	48.301.7	1.6.3.2
LaserJet M5039 MFP	20	48.301.7	1.6.3.2
LaserJet M9040 MFP	20	51.252.1	1.6.3.2
LaserJet M9050 MFP	20	51.252.1	1.6.3.2
LaserJet M9059 MFP	20	51.252.1	1.6.3.2
Color LaserJet CM 4730 MFP	20	50.282.0	1.6.3.2
Color LaserJet CM 6030 MFP	40	52.252.2	1.6.3.2
Color LaserJet CM 6040 MFP	40	52.252.2	1.6.3.2
Color LaserJet CM 6049 MFP	40	52.252.2	1.6.3.2
Color LaserJet CM 3530 MFP	50	53.231.6	1.6.3.2, 1.7
Color LaserJet CM 4540 MFP	XX	2302908_435001	1.6.3.2, 1.7

Table 6-1: **List of devices supported with the AccuRoute Embedded Device Client**

Device	Group	Supported firmware	OXPd Version
ScanJet 7000n	XX	2201075_229185	1.6.3.2
ScanJet 8500n	XX	2302829_434645	1.6.3.2, 1.7
LaserJet Flow M525 MXP	XX	2302908_435018	1.6.3.2a, 1.7
LaserJet Flow M575 MXP	XX	2302908_435018	1.6.3.2, 1.7
LaserJet M775 MFP	XX	2302908_435017	1.6.3.2, 1.7
LaserJet M4555 MFP	XX	2302908_435006	1.6.3.2, 1.7
HP Color LaserJet flow MFP M527	XX	2306273_536016	1.7.1
HP Color LaserJet flow MFP M577	XX	2306272_536017	1.7.1
HP Color LaserJet flow MFP M830	XX	2302908_435011	1.6.3.2, 1.7
HP Color LaserJet flow MFP M880	XX	2302908_435005	1.6.3.2, 1.7
HP LaserJet MFP M725	XX	2302908_435014	1.6.3.2, 1.7
HP Officejet Pro 276dw MFP	XX	1416B	1.7, 1.7 Pro
HP Officejet Pro x476dn MFP	XX	1409A	1.7, 1.7 Pro
HP Color MFP S962dn	XX	H1.03.S1.00	
HP Color MFP S970dn	XX	H1.03.S1.00	
HP Color MFP S951dn	XX	H1.03.R2.00	
HP MFP S956dn	XX	H1.02.o1.00	
HP X585 MFP group	XX	2302908_435002	1.6.3, 1.7
HP M680 MFP group	XX	230290_435008	1.6.3, 1.7
HP M630 MFP group	XX	2303714_233000041	1.7
HP PageWide Color MFP 586	XX	2308216-001092	1.7.X
HP PageWide Color MFP E58650	XX	2308216-001092	1.7.X
HP PageWide Color Flow MFP 586	XX	2308216-001092	1.7.X
HP PageWide Color Flow E58650	XX	2308216-001092	1.7.X
HP PageWide Managed MFP P57750dw	XX	2308216-1708d	1.7.X
A3 LaserJet (FutureSmart 4):			
HP LaserJet Managed MFP E72525/ E72530/E72535 Series	XX	2403321-000077	1.7.X
HP LaserJet Managed MFP E82540/ E82550/E82560 Series	XX	2403321-000078	1.7.X
HP Color LaserJet Managed MFP E77822/ E77825/E77830 Series	XX	2403325-000092	1.7.X
HP Color LaserJet Managed MFP E87640/ E87650/E87660 Series	XX	2403325-000091	1.7.X

Table 6-1: **List of devices supported with the AccuRoute Embedded Device Client**

Device	Group	Supported firmware	OXPd Version
A4 LaserJet (FutureSmart 4):			
HP Color LaserJet Enterprise MFP M681/ M682 Series	XX	2403322-000090	1.7.X
HP LaserJet Enterprise MFP M631/M632/ M633 Series	XX	2403322-000088	1.7.X
HP PageWide Color MFP 780, Flow 785, E77650, and E77660 Series	XX	2403782_000143	1.7.3
HP Digital Sender Flow 8500 fn2 Document Capture Workstation	XX	2403732_013004	1.7.3
HP ScanJet Flow N9120 fn2 Document Scanner	XX	2403732_013003	1.7.3

> **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 the AccuRoute 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.

Configuring HP S900 Series MFP Devices

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

This appendix describes the processes for

- Enabling HTTPS for SSL on HP S900 Series devices (6-4)
- Adding buttons to HP S900 Series MFP devices (6-4)
- Device authentication (6-5)

> **Note**   Verify that Section 3: Installation has been completed and that the Device Client is installed.

Enabling HTTPS for SSL on HP S900 Series devices

Apply the following steps to the HP S900 Series device after completing the HTTPS configuration outlined in Section 3: Setting up a CA Certificate and SSL.

1 In a browser, open the **Embedded Web Server** for the HP S900 Series device by entering the **IP address** of the device, and log in.

2 Select **Security Settings > SSL settings**.

3 In the **Setting of SSL** section, select **Enable** for **Client Port: HTTPS**.

4 Save the configuration.

Adding buttons to HP S900 Series MFP devices

> **Note** It is recommended that you install the buttons as Nested buttons. For more information, see Using Nested buttons (6-5).

1 In the AccuRoute Administrator, acquire an **XML Group Dump** from the Device Group. Highlight the **Devices** node, right-click on it while holding the CTRL key and select **Dump XML**. By default, this .xml opens in Internet Explorer.
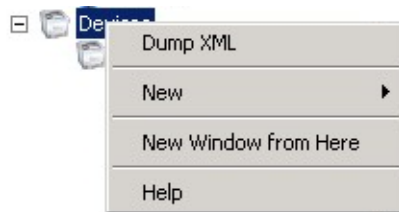
2 In a browser, open the **Embedded Web Server** for the HP S900 Series device by entering the IP address of the device, and log in.

3 From the left menu, select **Application Settings/External Application Settings**.

4 Select **Add(Y)**.

5 In the **Standard Application Registration** page, add an **Application Name** for the feature button.

6 In **Address for Application UI,** use the following generic URL string:

http://DeviceClientServerIP/Device Client/
device.aspx?Group=<GroupName>&FeatureID=<FeatureID>&ClearHistory=1

7 Replace the following fields with the appropriate values:

▸ **Device Client Server IP**

▸ **Group name**

▸ **Feature ID**

You can find the **Group name** under **Devices** in the Server Administrator.

Copy the **Feature ID** value from the **Dump XML** `<Feature id= >`.This corresponds with the Feature Button created in the HP CR Administrator.

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

---

8   The following XML Group dump example shows a Nested button `feature id` within the HP S900 Series Device Group:

```xml
        </Choices>
      </UI>
      <Additional/>
    </Confirmation>
  </DeliveryConfirmations>
  <FeatureSets>
    <shuttle_918177c4574242e0b301c2d269b3b8de>
      <Feature id="Button0" enabled="true" toplevel="true" type="Button">
        <Image/>
        <Text>HP Capture & Route</Text>
        <Description>Scan to HP Capture and Route</Description>
        <AllowJobBuild>false</AllowJobBuild>
        <EnablePreview>false</EnablePreview>
        <AllowUseByNonAuthenticatedUsers>true</AllowUseByNonAuthenticatedUsers>
        <CaptureAuthenticatedPassword>false</CaptureAuthenticatedPassword>
        <CaptureAuthenticatedPasswordAlwaysPrompt>false</CaptureAuthenticatedPasswordAlwaysPrompt>
        <FeatureSpecific>
          <GUID>c9e9e27e-8d07-47c0-8de3-4ddacac029cc</GUID>
          <priority>1</priority>
          <help>@helpfeatures</help>
          <ImageNormal>nested</ImageNormal>
          <PersonalED1/>
          <RoutingSheet2/>
          <GroupED3/>
          <MyAccuRoute4/>
          <ScanToDataProvider5/>
          <Fax6/>
        </FeatureSpecific>
      </Feature>
      <Feature id="PersonalED1" enabled="true" toplevel="false" type="PersonalED">
        <Image/>
        <Text>@buttonpersonalText</Text>
        <Description>@buttonpersonalDesc</Description>
        <AllowJobBuild>false</AllowJobBuild>
        <EnablePreview>false</EnablePreview>
        <AllowUseByNonAuthenticatedUsers>false</AllowUseByNonAuthenticatedUsers>
        <CaptureAuthenticatedPassword>false</CaptureAuthenticatedPassword>
        <CaptureAuthenticatedPasswordAlwaysPrompt>false</CaptureAuthenticatedPasswordAlwaysPrompt>
```

In this example, the specific string created is

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

Using Nested buttons

It is recommended that you use Nested buttons, because:

- The HP S900 Series MFP devices have a display limit of 8 buttons in the main window.

- Nested buttons need only be registered once, as opposed to the individual registrations required if they were not nested.

For more information about Nested buttons, see AccuRoute scanning features in AccuRoute Embedded Device Client (1-2).

Device authentication

1   In a browser, open the **Embedded Web Server** for the device and log in.

2   Select **Network Settings > LDAP settings**.

3   Enter the **Name**, **Search root**, and **LDAP server IP** information.

4   Set **Server Type** to **Custom** (the Search attribute has a default value of `CN`.)

5   Optionally, you can set other **Custom Attributes**, which allow for additional return results.

6   Enter the **Domain\Username** and **Password** for LDAP queries.

7   Change the **Bind Prefix** to CN. This will search based on the user's Common name and can be changed to any Active Directory Attribute.

Note   Other login options are available based on Email address or User number.

---

8   Select **Execute** to verify LDAP search permissions and then select **Submit**.

9   From the left menu, select **User Control > Default Settings**.

10 Select **User Authentication > Enable**.

11 Select **Authentication Method Setting > Authenticate a User by Login name and Password**.

12 Select **Submit** and then **Update**.

Configuring FutureSmart and OZ devices

This section describes the configuration process for FutureSmart and OZ devices only. The configuration involves 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: Creating Device Groups on the AccuRoute Server Administrator (4-1).

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.

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 AccuRoute 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.

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 which you can access it.

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 AccuRoute 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.

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 this 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 appear.

Adding the certificate to the Client certificate directory

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

1   Navigate to the `IIS\LOCAL MACHINE` directory and locate **Server Certificates**.

2   Locate the newly created certificate. Double-click to open the certificate **Properties** page.

3   Click on the **Details** tab.

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)\Omtool\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**.

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 **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:
    `.../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)\Omtool\Omtool Server\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.

Editing the Bootstrap.xml file

1   Navigate to the following path.

`C:\Program Files (x86)\Omtool\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.

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.

> **Note**   The CA Certificate steps, described in <u>Section 3: Setting up a CA Certificate and SSL</u> (3-1), are not supported for HP Pro devices.

The OPS Server installation process includes the following steps:

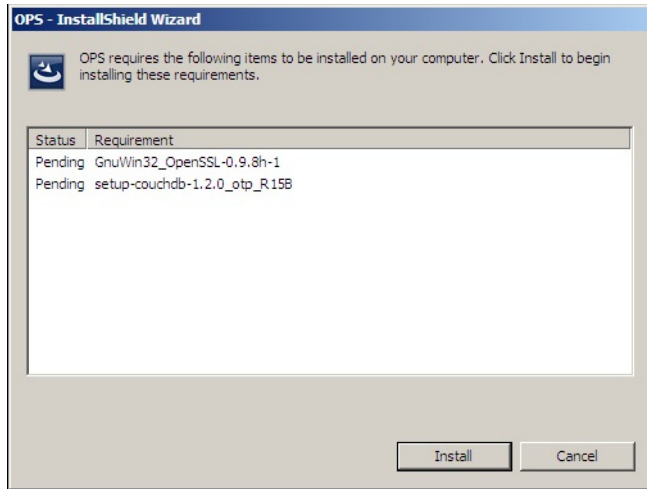> **Note**   Scanning in landscape orientation is currently unavailable for HP Pro devices.

Installing the AccuRoute Embedded Device Client on the server

On the system running the AccuRoute server, install the AccuRoute Embedded Device Client. See <u>Installing the AccuRoute Embedded Device Client</u> (3-1) for more information.

Installing the OPS kit on the server

1   On the server, navigate to `C:\Program Files (x86)\Omtool\Omtool Server\Tools`.

2   Right-click and select **Run as Administrator**.

3   Run `setup.exe` for OPS.

4   The OPS InstallShield wizard appears and requests that you install the following two items:

   ‣ `GnuWin32_OpenSSL-0.9.8h-1`

   ‣ `setup-couchdb-1.2.0_otp_R15B`

5   Click **Install**.

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

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

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

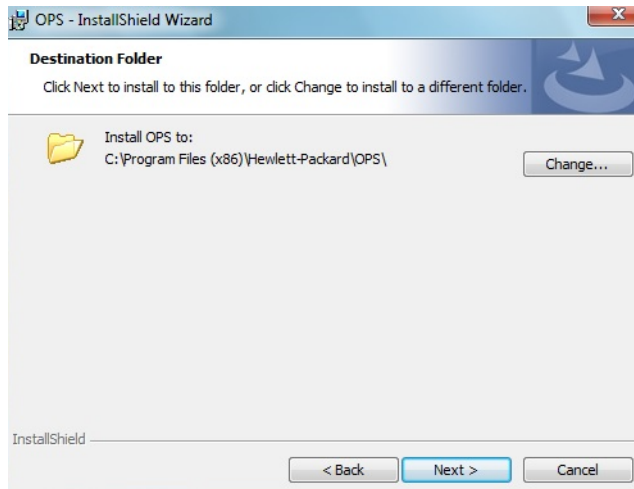Otherwise, the OPS InstallShield wizard **Welcome** screen immediately appears.
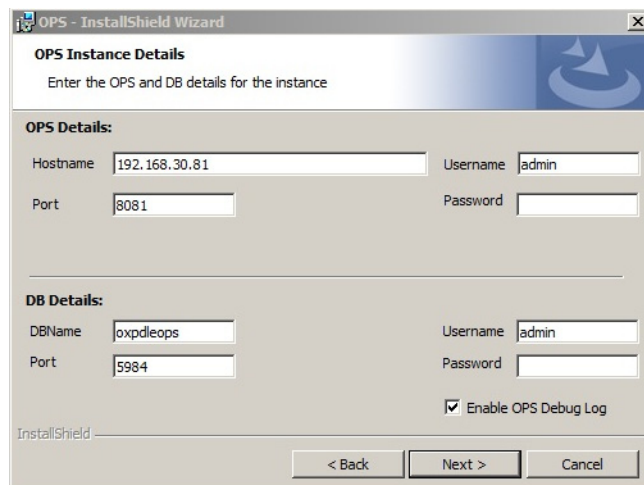

7 Click **Next**. The **License Agreement** screen appears.

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

The **Destination Folder** screen appears.

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

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.

13 Click **Install**.

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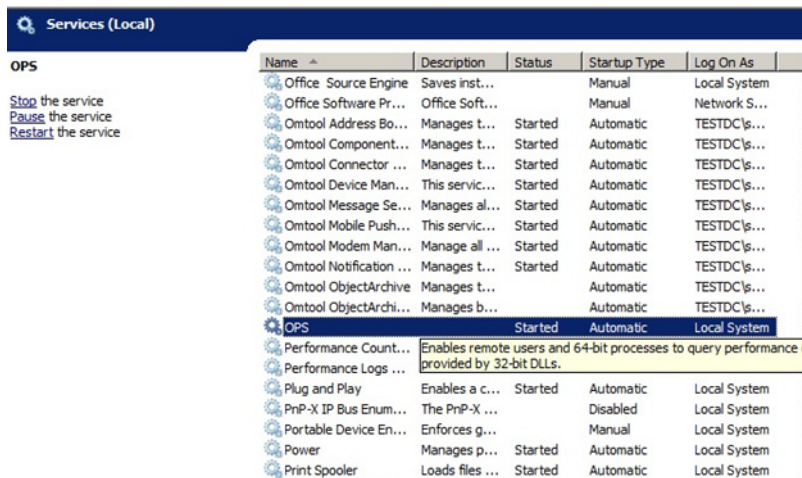

Select both the **Launch OPS** and **Show the readme file** check boxes (**Show the readme file** is optional) and then click **Finish**.

A pop-up message appears to inform you that the OPS server is listening at the IP address and port listed in step 9.
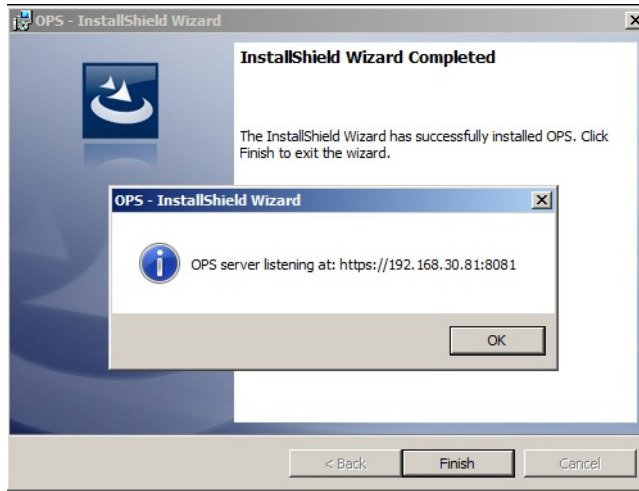
Click **OK**. OPS now appears as a Windows service.

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**.

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**.

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 (6-11).

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 (6-11).

---

7 The following message appears:

`OPS Registered successfully`

Your local OPS server is now installed. See Creating a group of devices (4-1) for more information on creating device groups.

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:
       .../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)\Omtool\Omtool Server\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 <u>Installing the OPS kit on the server</u>.

Note   XML files can be edited using Microsoft Notepad.

---

3   Save the file.

Editing the Bootstrap.xml file

1   Navigate to the following path:
       C:\Program Files (x86)\Omtool\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 <u>Installing the OPS kit on the server</u>.

3 Save the file and reset IIS.

Configuring HP Pro Devices on a remote OPS Server with HTTPS support

This section 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 AccuRoute 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.

Installing the AccuRoute Embedded Device Client on the local server

On the local system (*System A*) running the AccuRoute server, install the AccuRoute Embedded Device Client. See <u>Installation</u> (3-1) 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.

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*.

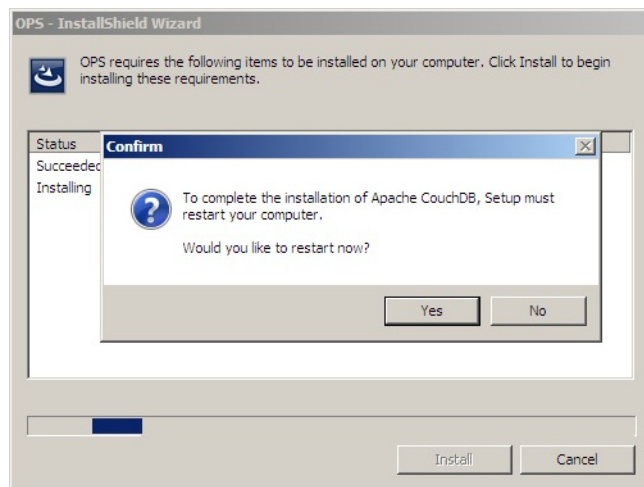**4** The OPS InstallShield wizard appears and requests that you install the following two items:

▸ GnuWin32_OpenSSL-0.9.8h-1

▸ setup-couchdb-1.2.0_otp_R15B

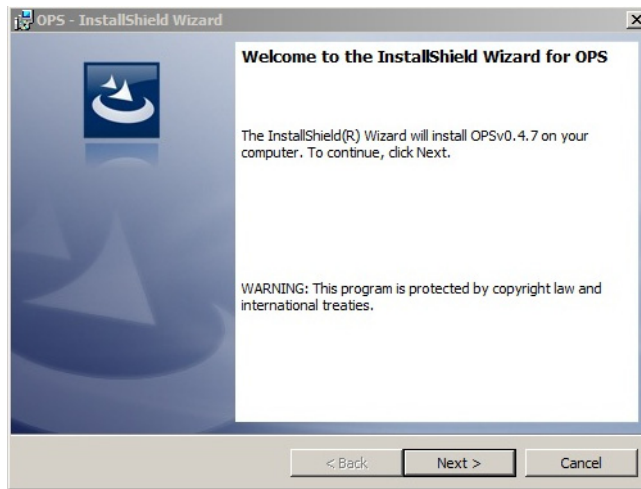**5** Click **Install**.

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

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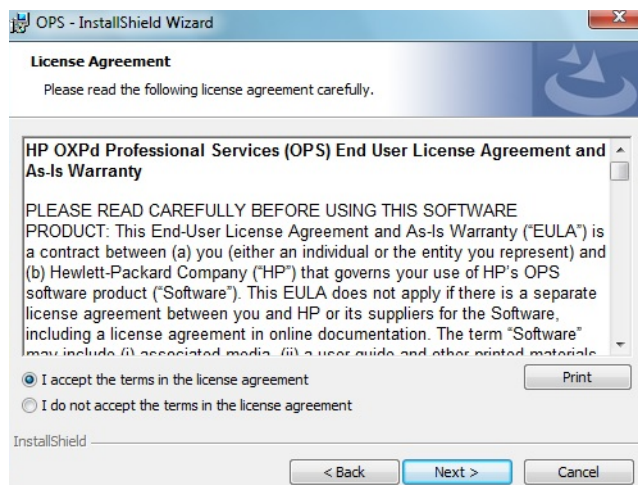

If this message appears, click **Yes** to restart. The OPS InstallShield wizard reappears upon restarting the system.

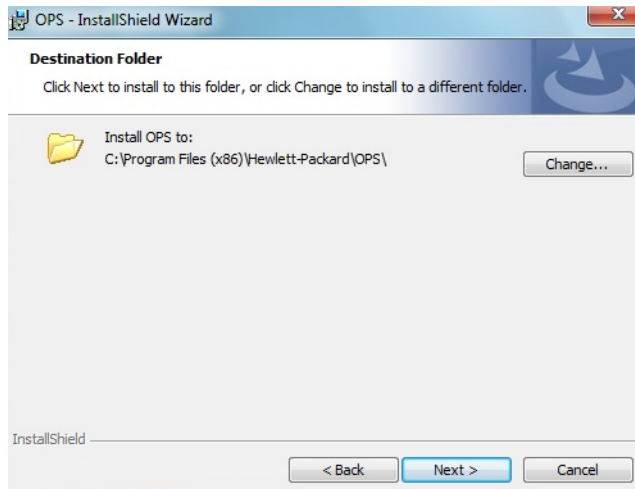Otherwise, the OPS InstallShield wizard **Welcome** screen immediately appears.

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

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

The **Destination Folder** screen appears.

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

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.

13 Click **Install**.

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

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.
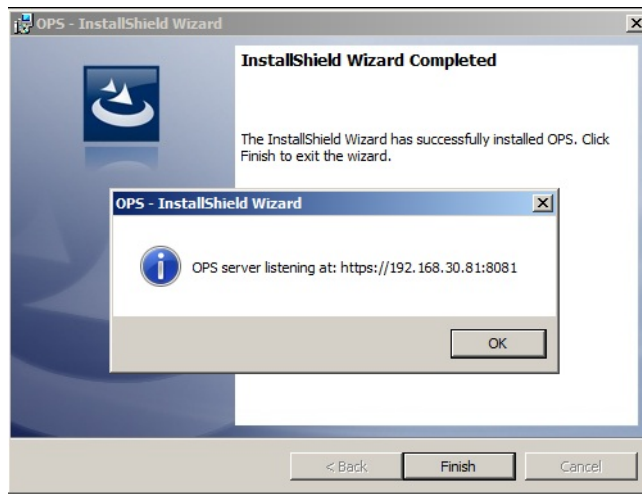
Click **OK**. **OPS** now appears as a Windows service.
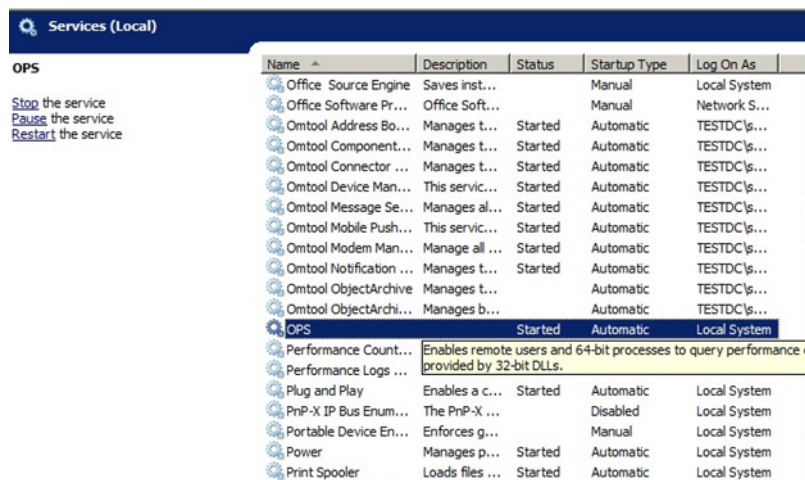
Exporting the OPS server certificate

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)\Omtool\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)\Omtool\DeviceClient\OPS`.

10 Select **Next** and then click **Finish**.

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**.

OPS registration

1 At a command prompt enter

`C:\Program Files (x86)\Omtool\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 (6-20).

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 (6-20). 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 (4-1) for more information
on creating device groups.

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:

    .../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)\Omtool\OmtoolServer\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 <u>Installing the OPS kit on the remote server</u> (6-20).

> **Note**   XML files can be edited using Microsoft Notepad.

4   Save the file.

Editing the Bootstrap.xml file

1   Navigate to the following path.

    C:\Program Files (x86)\Omtool\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 <u>Installing the OPS kit on the remote server</u> (6-20).

Configuring HP FutureSmart, OZ, and PRO devices to use the OPS Server Certificate for HTTPS environments

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

Before continuing, verify that the OPS Server is installed and working as described in Chapter 7: <u>Configuring HP MFP Devices</u> (6-1).

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

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

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

1   Navigate to `C:\Program Files (x86)\Hewlett-Packard\OPS` and copy the certificate saved from previous steps.

2   Navigate to and then paste the certificate into `C:\Program Files (x86)\Omtool\DeviceClient\Certificate\OPS`.

All FutureSmart and Oz devices will use this certificate for HTTPS communication.

Section 7: Configuring Samsung Devices

The AccuRoute Embedded Device Client v6.0 supports Samsung™ devices. The AccuRoute Embedded Device Client communicates information between scanning devices and the AccuRoute Server via the Intelligent Device Client application.

> **Note** The AccuRoute Embedded Device Client v6.0 requires an additional download of the Samsung .PAR file in order to support the Samsung devices. Please contact Customer Service for the download instructions.

This section includes:

Supported Samsung devices

Table 1: **Samsung devices supported by the AccuRoute Embedded Device Client**

Device Type	Model	Name	Firmware version
A3 Devices	CLX-9X5X	Cosmos color	V6.S6.15
	SCX-80XX	Cosmos color	V6.N6.30
	CLX-9252/9258	Cosmos-R color	V6.B6.10.EC08.02
	CLX-9352/9358	Cosmos-R color	V6.B6.10.EC08.02
	SCX-8230/8240	Cosmos-R mono	V5.B6.06.EC08.01
	SCX-8238/8248	Cosmos-R mono	V5.B6.06.EC08.01
	SCX-8123/8128	Polaris mono	V5.C6.28
	CLX-9201/9251/9301	Polaris color	V6.M6.05.0301007.02
	CLX-9206/9256/9306	Polaris color	V6.M6.05.0301007.02
A4 Devices	SCX-5835NX/5935	Elbert2 mono (SuperUI)	V2.00.03.07
	SCX-6555NX	Rushmore mono (SuperUI)	V2.00.03.07
	SCX-6545NX	RushmoreM mono (SuperUI)	V2.00.03.05
	CLX-8385NX	RoseR color	V2.00.03.05
	CLX-8640	Evergreen color	V6.C6.24
	CLX-8650	Evergreen color	V6.C6.24

Server Requirements

- AccuRoute Server v6.0

- Samsung .PAR file (saved to a known location)

For AccuRoute Server installation and configuration instructions, consult the AccuRoute Server Installation and Configuration Guide.

Installation

This section includes:

- Installing the Device Client (7-2)

- Creating device groups (7-2)

- Saving the Samsung .PAR file to the Clients directory (7-2)

Installing the Device Client

Start by installing the AccuRoute Embedded Device Client, following the steps in Section 3: Installation (3-1).

Important	To install and use the new Embedded Device Client, you must first uninstall any prior AccuRoute Embedded Device Clients.

Creating device groups

After you have installed the AccuRoute Embedded Device Client, you need to create device groups for your environment, as described in Section 4: Creating Device Groups on the AccuRoute Server Administrator (4-1).

Continue with Saving the Samsung .PAR file to the Clients directory (7-2).

Saving the Samsung .PAR file to the Clients directory

Log in to the Omtool Support Download site and save the `OmtoolXOAApp.par` file in the following location on the server:

```
C:\Program Files (x86)\Omtool\Omtool Server\Clients\Samsung
```

Continue with Configuration, below.

Configuration

This section describes the configuration process for Samsung devices.

Refer to Creating Device Groups on the AccuRoute Server Administrator and Installing Buttons on a New Device to set up device group authentication, add buttons to devices, and depending on the needs of your system environment, configure HTTPS communication.

With those configurations complete, you can now configure the integration between your Samsung devices and the AccuRoute Server Administrator.

Integrating the Samsung device with the AccuRoute Server Administrator

To complete integration between the Samsung device and the AccuRoute Server Administrator, continue the configuration process by:

Installing the Omtool integration product on a Samsung device (7-4)

Installing the certificate on the device (7-7)

Configuring the device XOA to use SSL (7-9)

Configuring the AccuRoute Server Administrator to use SSL (7-9)

Installing the Omtool integration product on a Samsung device

To prepare to integrate your Samsung device with the AccuRoute Administrator, use the following steps to install the `.par` file that was copied to the `\Clients\Samsung` directory.

    1   Open the Embedded Web Server (EWS) on the device of interest by entering the device IP address in any internet browser. The following example shows a device EWS in Internet Explorer.
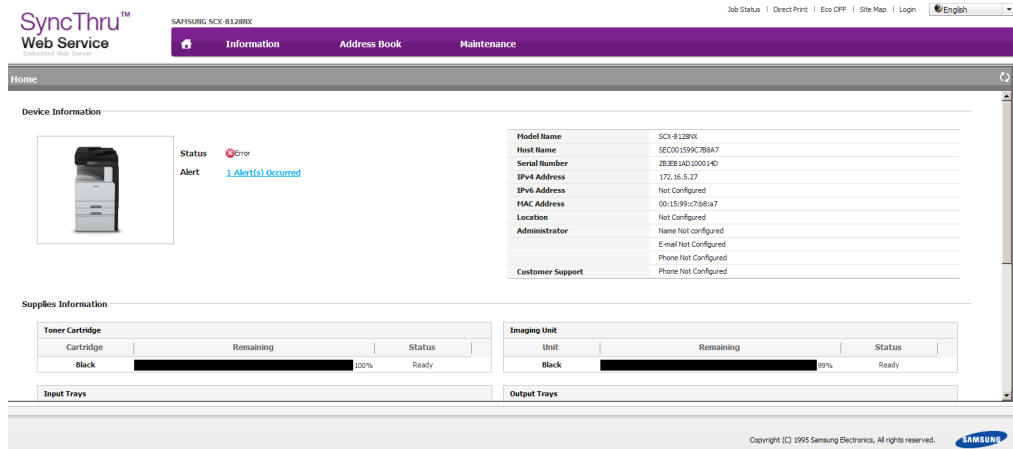
    2   To log in to the device EWS, click **Login** at the top right of the screen. A **Login** screen appears.

    3   Enter the **username** `admin` and the admin **password** and click the **Login** button.

    4   Select the **Maintenance** tab and on the left side of the screen open **Application Management > Application**. The **Application** screen appears.

    5   Click the **Add** button at the top of the **Application** screen.

    6   In the **Installation** screen that appears, select the **Desktop** option and browse to the `.par` file located at

        `C:\Program Files (x86)\Omtool\Omtool`
        `Server\Clients\Samsung\OmtoolXOAApp.par`

7   Click **OK**. The following warning screen appears:
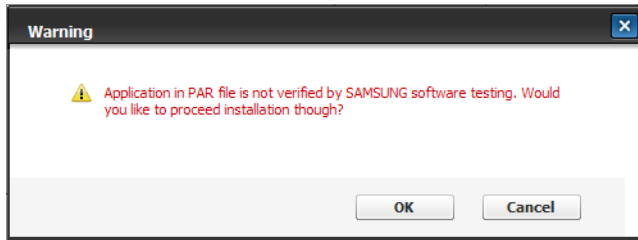
8   Click **OK** and the following **Installation** screen appears:

9   Click **OK** and the following progress screen appears:
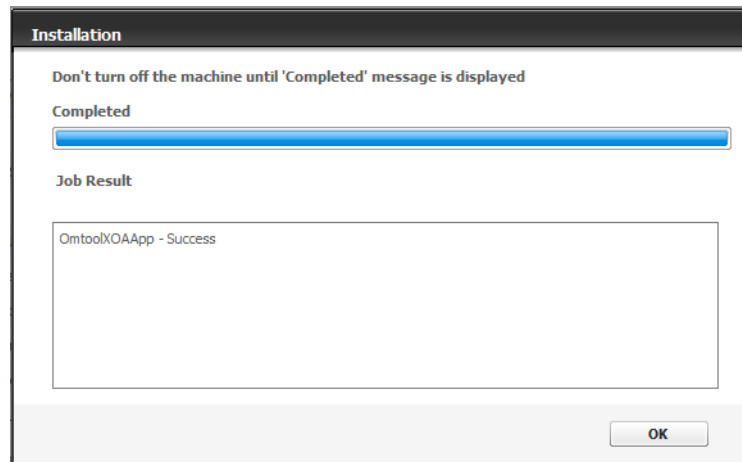
10 Once complete, click **OK** to return to the EWS **Application** screen, where **OmtoolXOAApp** now appears in the application list, as shown below:
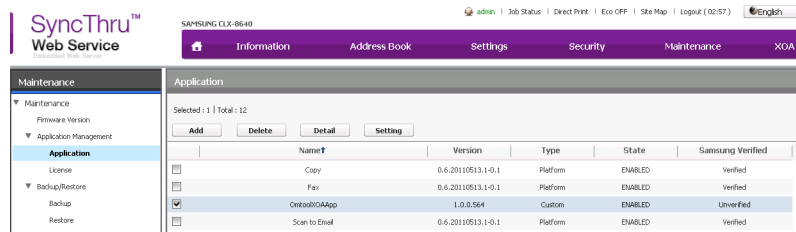
11 Refresh the EWS screen. The **XOA** tab will appear beside the **Maintenance** tab, as shown:
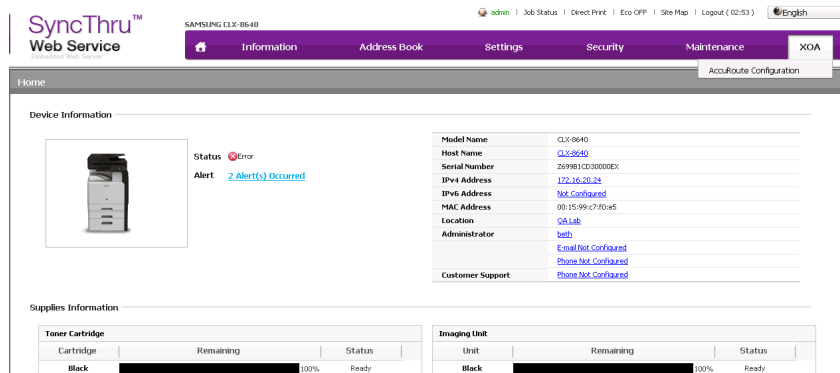
12 Select the **XOA** tab and on the left side of the screen open **AccuRoute Configuration**. The **Configuration** screen appears:
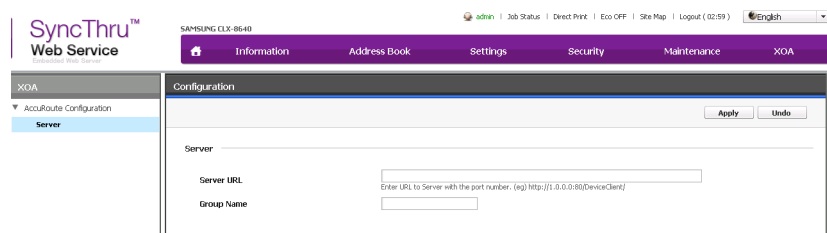
13 Enter the **Server URL** and the **Group Name**. Refer to the following format options for HTTP and HTTPS connections:

▸ **HTTP:** `http://<Server IP address>:<port>/DeviceClient/`

   where you can replace `<port>` with the default value of `80`.

▸ **HTTPS:** `https://<Certificate Common name>:<port>/DeviceClient/`

   where you can replace `<port>` with the default value of `443`.

14 Click **Apply** at the top of the **Configuration** screen.

    This updates the **OmtoolXOAApp** application and you can start testing the application on the device control panel.

15 Power off and then restart the Samsung device.

Installing the certificate on the device

1 Open the Embedded Web Server (EWS) on the device of interest by entering the device IP address in any internet browser. The following example shows a device EWS in Internet Explorer.

2 To log in to the device EWS, click **Login** at the top right of the screen. A **Login** screen appears.

3 Enter the **username** `admin` and the admin **password** and click the **Login** button.

4 Select the **Security** tab and on the left side of the screen open **Network Security > Digital Certificate**. The **Digital Certificate** screen appears.

5 In the **Certificate Management** section, click the **Add** button. The **Digital Certificate Installation** wizard appears.

6   Select **Install new Root certificate** and click **Next**.
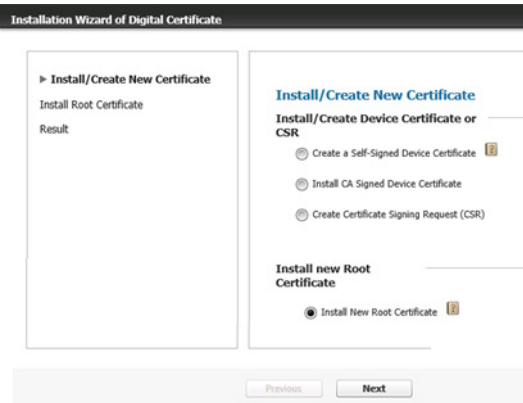
7   Browse to the certificate file. Press **Next**.
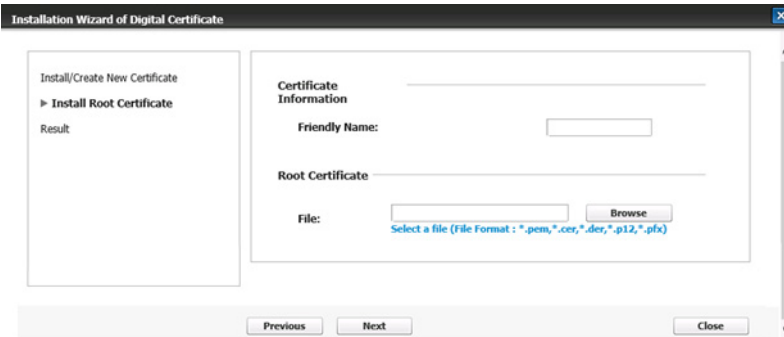
8   When the certificate is successfully imported, the following message appears:

Root Certificate has been successfully installed.

9   Click **Close**.

10   The imported certificate appears in the **Certificate Management** list, as shown below.

11   Once the certificate is installed, power off and then restart the Samsung device.

Configuring the device XOA to use SSL

1   Still in the Embedded Web Server, click the **XOA** tab and select **AccuRoute Configuration**.

2   In the **Server URL** text box, enter `https://FQDN:443/DeviceClient/`, where `FQDN` is a Fully Qualified Domain Name and `DeviceClient` is the name of the device, as in the following example:
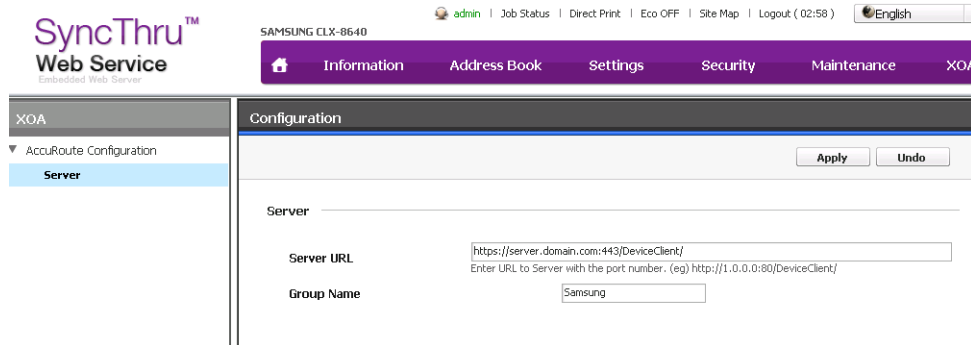
3   Enter the **Group Name** for the device and click **Apply**.

Configuring the AccuRoute Server Administrator to use SSL

1   In the **AccuRoute Server Administrator**, select the **Devices** node.

2   Right-click and select **Device Group Properties**. The **Device Group Properties** page opens

3   Select the **Settings** tab.

4   In the **Web API** text box, enter as `https://FQDN/WebAPI/Scripts/omisapiu.dll`, where `FQDN` is the Fully Qualified Domain Name for the device, as in the example below:
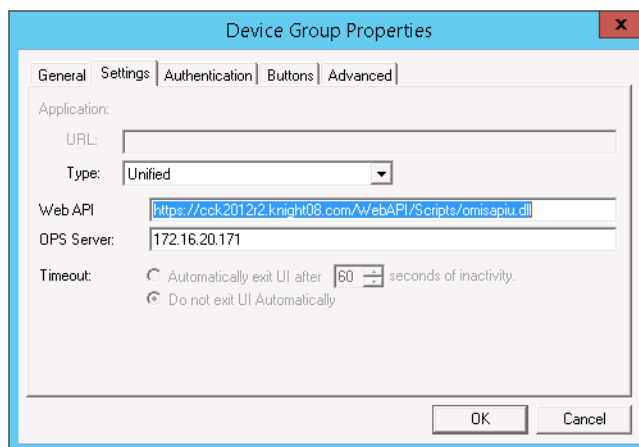
5   Click **OK** to finish.

Section 8: Configuring Xerox Devices

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

This section includes

- Supported Xerox devices (8-1)
- Configuring HTTPS support (8-2)
- Configuring Xerox device authentication on the device (8-6)

> **Note**   Verify that Section 3: Installation has been completed and that the Device Client is installed.

Supported Xerox devices

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

Table 8-1: **List of supported Xerox devices**

Device	Qualified by Omtool	Device Client Version	Software Version
550/560	Color 560	1.5	55.30.61, ESS1.207.3, IOT 64.18.0, IIT 6.16.1, ADF 12.11.0, SJFI3.0.18, SSMI1.16.0
ColorQube 87xx	ColorQube 8700S	2	071.160.101.36000, ESS 071.161.32710
ColorQube 92xx	ColorQube 9203	1.5	061.050.222.24401
Phaser 36xxMFP	Xerox Phaser 3635 MFP	1	20.105.11.000 digital signature now cannot go back, supports card reader, 20.105.14.000 supports card reader
WorkCentre 53xx	WorkCentre 5300	1.5	53.20.31, ESS1.205.1, IOT 30.39.0, ADF 7.10.0, SJFI3.0.18, SSMI1.16.0
WorkCentre 56xx	WorkCentre 5632 v.1 Multifunction System	1.5	025.054.065.190 supports card reader
WorkCentre 57xx	WorkCentre 5755	2	061.132.222.07901 supports card reader
WorkCentre 64xx	WorkCentre 6400	1	061.070.102.23501, 061.070.100.24201, ESS 061.070.22410
WorkCentre 71xx	WorkCentre 7120	1.5	71.22.52
WorkCentre 72xx	WorkCentre 7242	1	1.207.112
WorkCentre 73xx	WorkCentre 7335	1	ESS PS1.227.169, IOT 3.0.5, IIT 22.13.1, ADF 11.6.5, SJFI3.0.8, SSMI1.7.2

Table 8-1: **List of supported Xerox devices**

Device	Qualified by Omtool	Device Client Version	Software Version
WorkCentre 74xx	WorkCentre 7435	1.5	75.13.92, ESS PS1.182.180, IOT 41.1.0, IIT 22.13.1, ADF 20.0.0, SJFI 3.0.12, SSMI 1.11.1
WorkCentre 75xx	WorkCentre 7530	2	061.121.222.32600 supports card reader
WorkCentre 76xx	WorkCentre 7655 v.1 Multifunction System	1.5	0.40.33.53250, ESS 0.040.033.53250, IOT 08.32.00, UI, BIOS 07.11
WorkCentre Pro 245	WorkCentre Pro 245	1	ESS 0.040.022.50115, IOT 50.4.0, UI 0.12.60.12, BIOS 07.07

Note All Xerox devices must be set to SSL mode within the device's internal Web server. See Xerox for further instructions.

Configuring HTTPS support

In order to use HTTPS protocol communication when sending documents from the device to the AccuRoute Server, follow the instructions in this section to create a CA Certificate using Microsoft Certificate Services and enable SSL.

Note If you are using HTTP, skip this section and go to Section 5: Required Configuration.

Also note, HTTP and HTTPS cannot coexist and configuration for the device communication must be either HTTP or HTTPS for all devices.

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.

Complete the following steps in the order presented:

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 the ScanFacts Intelligent Device Client.
- Windows user account that belongs to the Administrators group.

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.

Creating the certificate

1 Open a **Command Prompt (Admin)** 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 01/01/2023 -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   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.

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.

Creating an SSL binding

1   Open the IIS Manager.

2   Click on the **Default Website** and locate **Bindings** under **Edit Site** (in the top-right corner of the window).

3   Click **Bindings**. The **Site Bindings** dialog opens.

4   Click **HTTPS type** and select **Edit**. The **Edit Site Bindings** dialog opens.

> **Note**   If no HTTPS appears in the SSL bindings list, you need to add one. To do so, in the **Site Bindings** dialog, instead of **Edit**, click the **Add** button. The **Add Site Binding** dialog opens. Select **Type: https**, **IP address: All Unassigned**, and **Port: 443**. From the **SSL certificate** drop-down menu, select the certificate that you created earlier and click **OK**. Continue at Step 6 below.

5   In the **SSL certificate** drop-down, select the certificate that was created earlier and click **OK**.

6   Click **Close** to exit the **Site Bindings** dialog.

Requiring SSL for the virtual web sites

1   Open the IIS Manager.

2   Expand **Local machine > Default WebSite** and select **Device Client**.

3   Open **SSL Settings** and check **Require SLL**. Under **Client certificates**, select **Ignore**.

4   Expand **Local machine > Default WebSite** and select **WebAPI**.

5   Open **SSL Settings** and check **Require SLL**.

6   Under **Client certificates**, select **Ignore**.

Enabling directory browsing is IIS

1   Open the IIS Manager.

2   Expand **Local machine > Default WebSite** and select **Device Client**.

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 the SSL binding

1 Open the IIS Manager.

2 Expand **Local machine > Default WebSite** 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 website'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.

Verifying HTTPS browsing

1 Open the IIS Manager.

2 Expand the **Default Web Site**.

3 Expand **Device Client**.

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:

`...\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\`

Editing the OmISAPIU.xml file

1 Navigate to the following path.

`C:\Program Files (x86)\Omtool\Omtool Server\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.

Editing the Bootstrap.xml file

1   Navigate to the following path.

`C:\Program Files (x86)\Omtool\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.

Configuring Xerox device authentication on the device

The following procedure uses an example configured for a ColorQube 8700S. Other devices will have slight differences in the terminology used within the device's web server.

a   Access the device Internal Web server and log in.

b   Click the **Properties** tab. Then, select **Connectivity > Protocols** or **Setup** (depending on the OS version) **> LDAP**.

c   Click **Add New**.

d   In the **General Information** or **Server Information** section (depending on the OS version):

- ▲ Select **IPv4 Address**.

- ▲ Enter a name in the **Friendly Name** text box.

- ▲ Select **ADS** in the **LDAP Server** drop-down.

e   In the **Optional Information** section:

- ▲ Enter the **Search Directory Root** (`DC=DomainName,DC=COM`).

- ▲ Select **System** for the **Login Credentials to Access LDAP Server**.

- ▲ Enter the **DomainName** or **Login Name** (depending on the OS version).

- ▲ Enter the **Password**.

- ▲ Select the option to **Select to save new password**. (If you return to this window, the login information will display as blank.)

f   Apply SSL and other settings, if necessary. Defaults were used in this example.

SSL

☐ Enable SSL (Secure Socket Layer)
☐ Validate Repository SSL Certificate (trusted, not expired, correct FQDN)
   View Trusted SSL Certificates

Trusted SSL Certificates

[No Validation ▾]

[View/Save]

Maximum Number of Search Results

○ Use LDAP Server Maximum
◉ Maximum Number of Search Results
   [25]   (5 - 100)

Search Timeout

○ Use LDAP Server Timeout
◉ Wait
   [30]   seconds (5 - 100)

LDAP Referrals

☐ Enabled

Perform Query on

◉ Mapped Name Field
○ Surname and Given Name Fields

[Close] [Undo] [Apply]

g   Verify all information and click the **Apply** button.

h   Click the **Contexts** tab and select defaults.

i   Click the **User Mappings** tab. Verify that all information is correct.

j   In the **Search** section, enter a name to verify LDAP connectivity. (All Imported Heading defaults were used.)

All available attributes will be displayed under the Sample header if the query was successful.

k   In the left menu under **Security > Authentication**, select **Setup** to display the **Authentication**, **Authorization**, and **Personalization** settings.

l   Click the **Authentication Method on the machine's touch user interface (Touch UI)** option. Then, click the **Edit** button.

m   From the drop-down, select **User Name / Password Validated Remotely on the Network** option.

n Check the **Configuration Settings**:

Configuration Setting	Method (Defined Above)	Required / Optional; Status	Action
Authentication Servers	Authentication (Touch UI & Web UI)	✔ Required; Configured	🖉 Edit…
Machine's User Information Database	Authorization	✔ Required; Configured	🖉 Edit…
Tools and Feature Access (Lock / Unlock)	Authorization	✔ Optional; Configured	🖉 Edit…
LDAP Servers	Personalization	✔ Required; Configured	🖉 Edit…
Service Registration	(Convenience Link)	✔ Optional; Configured	🖉 Edit…

Note Under Configuration Settings, if **LDAP Servers > Personalization** shows a red exclamation mark, you need to define which LDAP server to use. (This might not be necessary.) If there is a red exclamation mark, select **LDAP Servers**. Then, click the **Edit** button and choose the LDAP server you have configured.

Graphic Key

❗	Required configuration to enable the Authentication, Authorization, and/or Personalization methods.
✳	Optional configuration expanding feature offering.
✔	Minimum configuration using factory defaults.
✔	Fully configured.

o Verify the LDAP server you configured is in the device list of LDAP servers. In the left menu under **Protocols**, select **LDAP** to display the LDAP Servers.
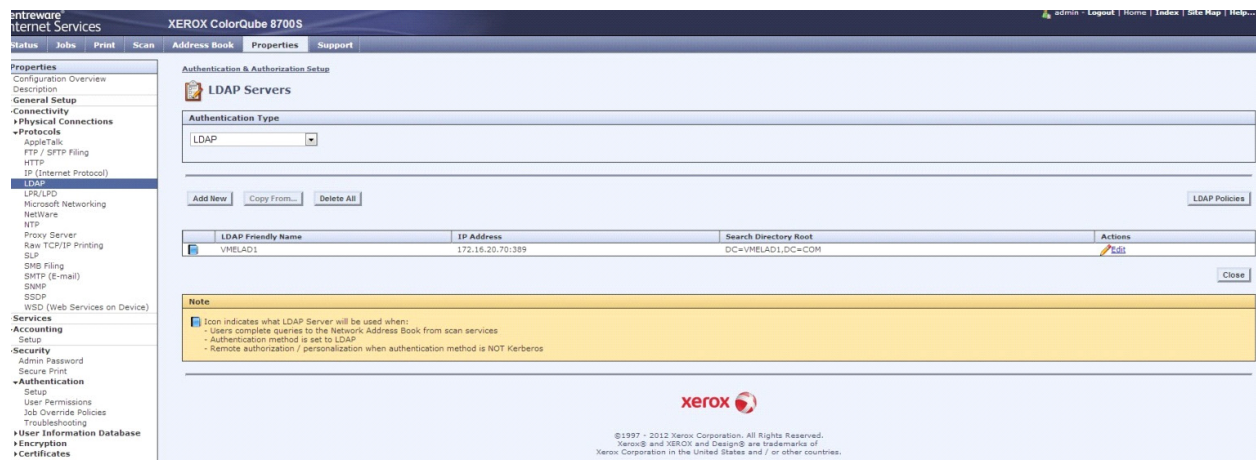
p In the left menu under **Security > Authentication**, select **User Permissions > Non-Authenticated Users > Edit**.

q Select **Service & Tools**.

Manage User Permissions (Non-Authenticated User)

Role Name	Description
Non-Authenticated User	Prevent non-logged in users access to features.

Print   **Services & Tools**

Presets

- Allow access to everything except Tools (Standard Access)
- Allow access to everything including Tools (Open Access)
- Restrict access to all Services and Tools
- Restrict access to everything
- ● Custom

Note   This example uses custom presets. For more information on presets, see the Xerox Administrator Guide.

r For the Omtool feature button(s) desired for device authentication login, select **Not Allowed** in the **Role State** column. For example, you might select **Personal Distributions** and **Scan to Me**. The **Not Allowed** option locks those features requiring authentication.

Omtool.RoutingSheet0		Allowed
Omtool.PersonalED1	🔒	Not Allowed
Omtool.GroupED2		Allowed
Omtool.MyAccuRoute3	🔒	Not Allowed

s Click **Apply**.

t On the main page of the Device Internal Web server, select **IP (Internet Protocol)** under the **Protocols** heading in the left menu.

u Click the **DNS** tab and verify that the **Requested Domain Name** and **DNS Server Addresses** match the Omtool DNS server settings. Click **Apply** when finished.

v Reboot the device.

Section 9: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

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

Supported Devices

The following devices are supported:

Table 9-1: **AccuRoute Embedded Device Series Matrix**

Device	Operating System		Device	Operating System
Color LaserJet CM 4730 MFP	Oz		Color LaserJet CM 4540 MFP	FutureSmart
Digital Sender 9250c	Oz		ScanJet 7000n	FutureSmart
LaserJet M3035 MFP	Oz		ScanJet 8500	FutureSmart
LaserJet M4345 MFP	Oz		LaserJet Flow M525 MXP	FutureSmart
LaserJet M4349 MFP	Oz		LaserJet Flow M575 MXP	FutureSmart
LaserJet M5035 MFP	Oz		LaserJet M775 MFP	FutureSmart
LaserJet M5039 MFP	Oz		LaserJet M4555 MFP	FutureSmart
LaserJet M9040 MFP	Oz		HP Color LaserJet Flow M880	FutureSmart
LaserJet M9050 MFP	Oz		HP Color LaserJet Flow M830	FutureSmart
LaserJet M9059 MFP	Oz		HP LaserJet MFP M725	FutureSmart
Color LaserJet CM 6030 MFP	Oz		HP X585 MFP group	FutureSmart
Color LaserJet CM 6040 MFP	Oz		HP M680 MFP group	FutureSmart

Table 9-1: **AccuRoute Embedded Device Series Matrix**

Device	Operating System		Device	Operating System
Color LaserJet CM 6049 MFP	Oz		HP M630 MFP group	FutureSmart
Color LaserJet CM 3530 MFP	Oz			

Exporting the XML files

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

1   Once the configuration is complete (as described in Installation, Creating Device Groups on the AccuRoute Server Administrator and Installing Buttons on a New Device), 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:
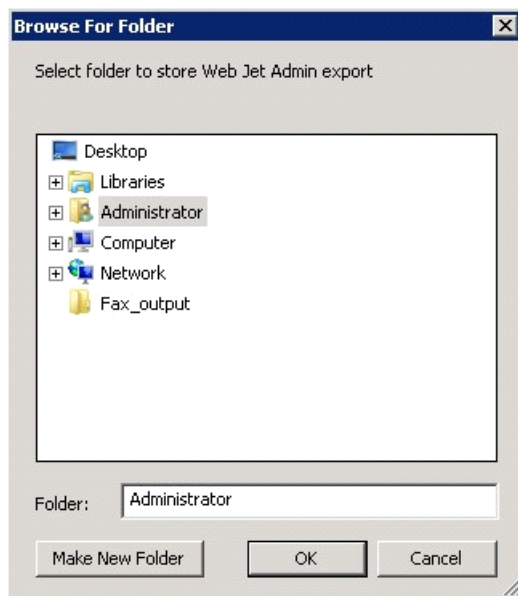
Make New Folder:
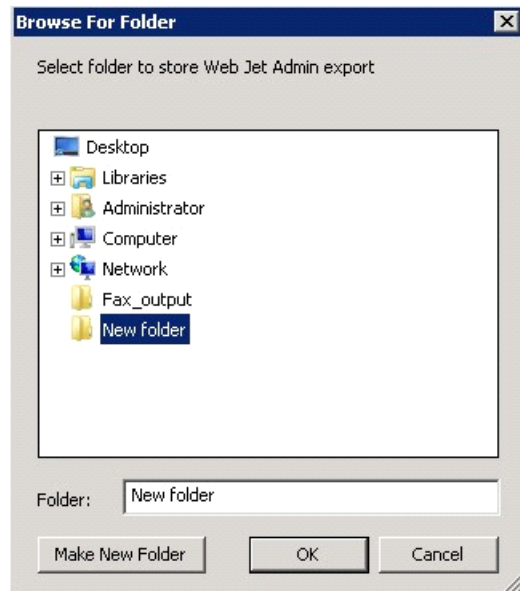
3   Click **OK** and verify the correct buttons are represented in XML format.
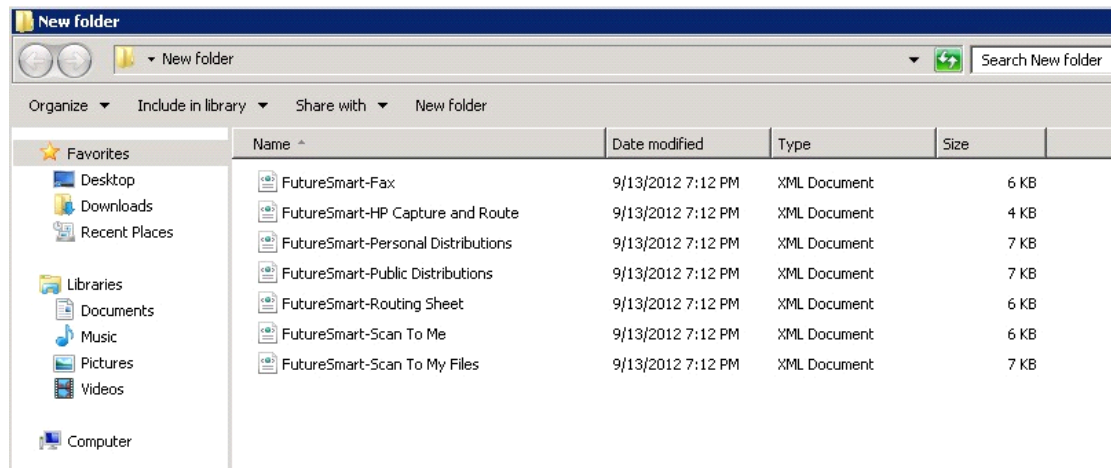
Manually importing a certificate

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.
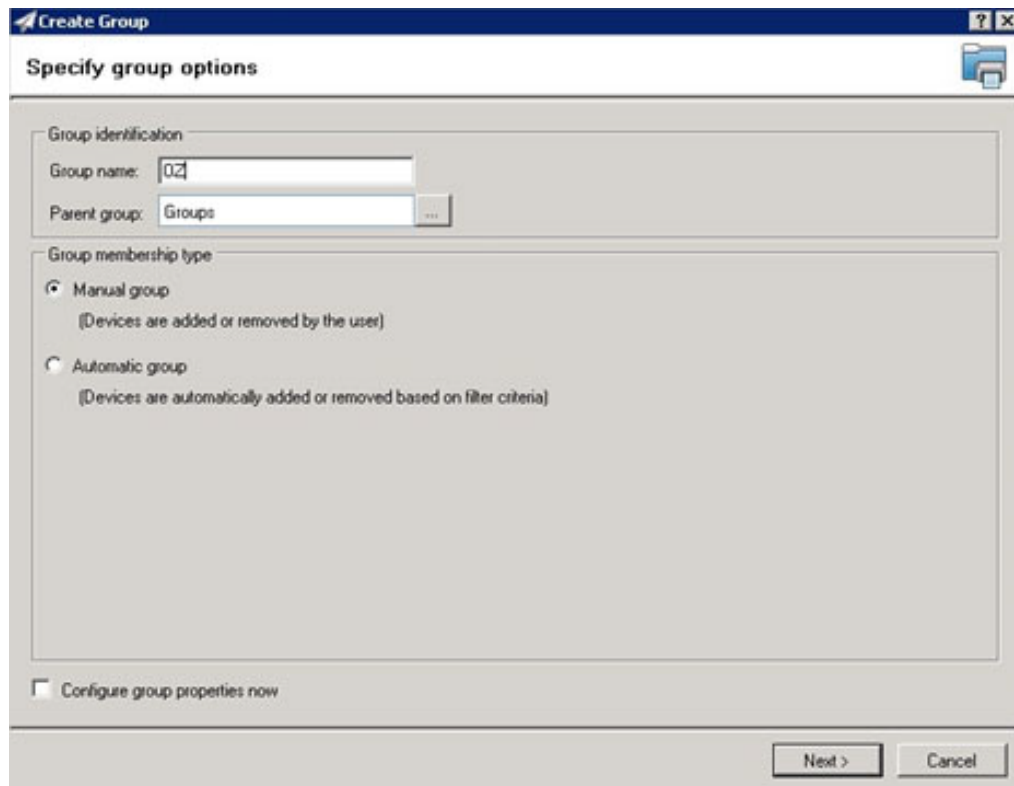
Installing AccuRoute Embedded Device Client buttons

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

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

The **Specify group options** page appears.

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

3 Click **Next** and verify that the group name is correct. The **Confirm** page appears, showing the settings for the group.
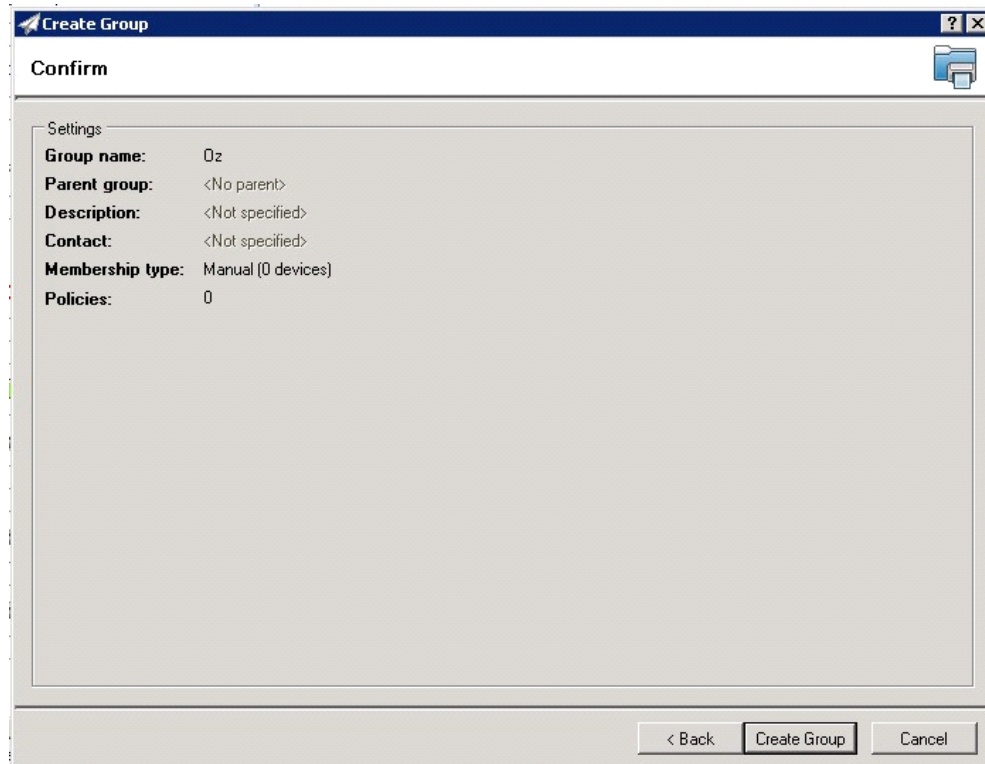
4 Click **Create Group** and then **Done**.

5 Right-click the newly-created group and select **Add devices to group**.
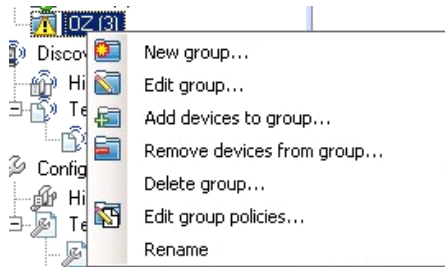
Note For more options to use the Web Jetadmin device filters to find or add devices, consult Omtool's Web Jetadmin team for a complete Web Jetadmin installation guide.
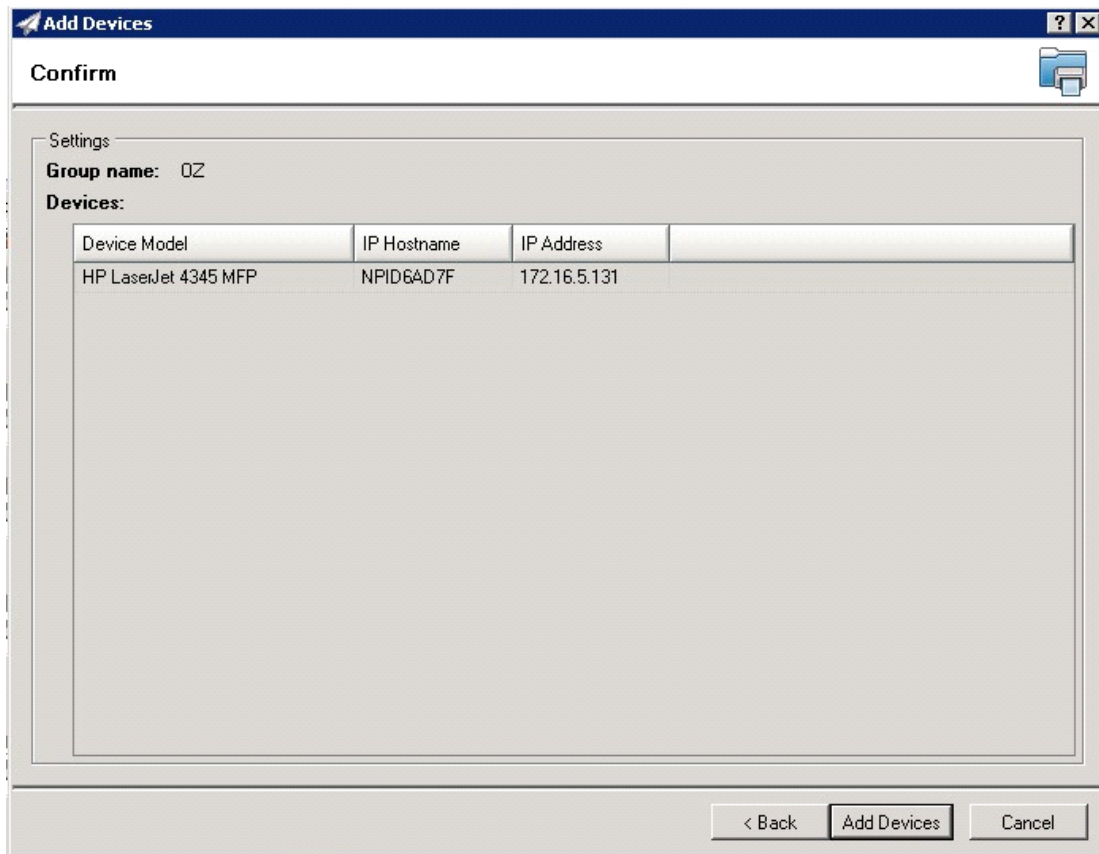
The **Select Devices** page appears.
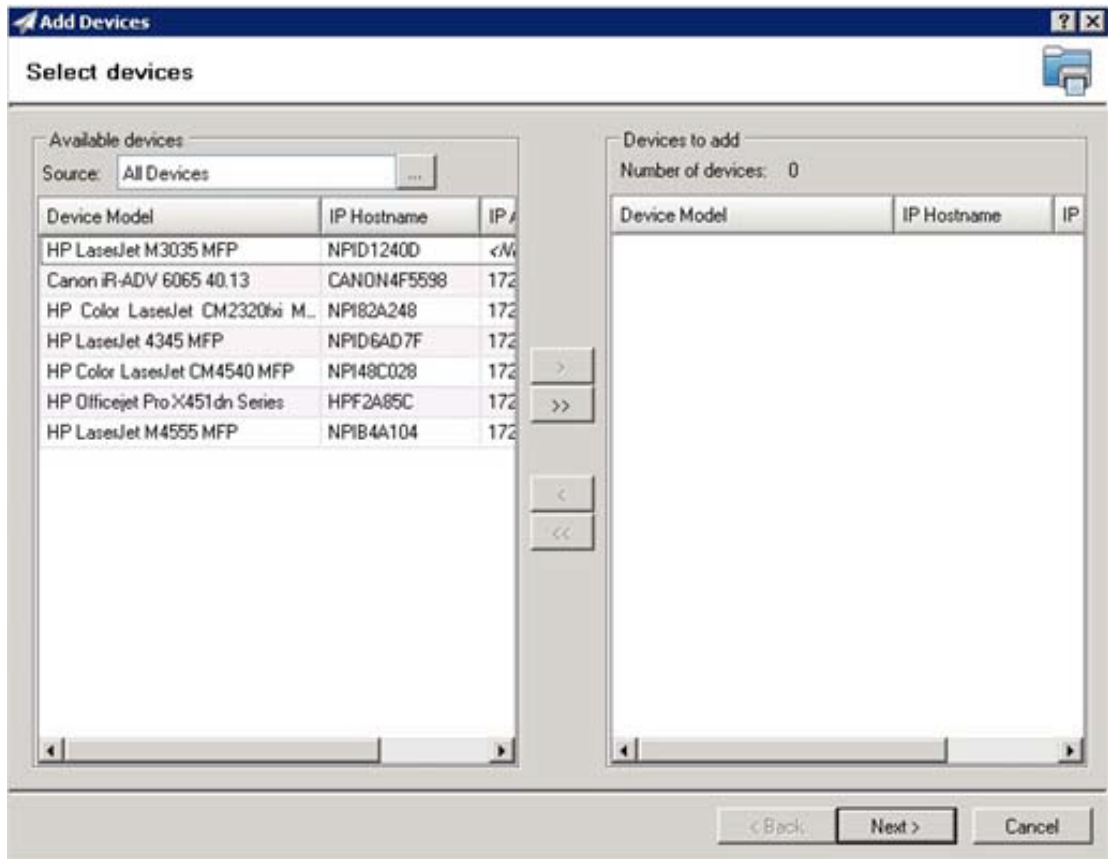
6 In the **Available devices** list (on the left), highlight the device(s) to be added to the group. Then click the **>** (add) button. The selected device(s) are added to the **Devices to add** list (on the right).
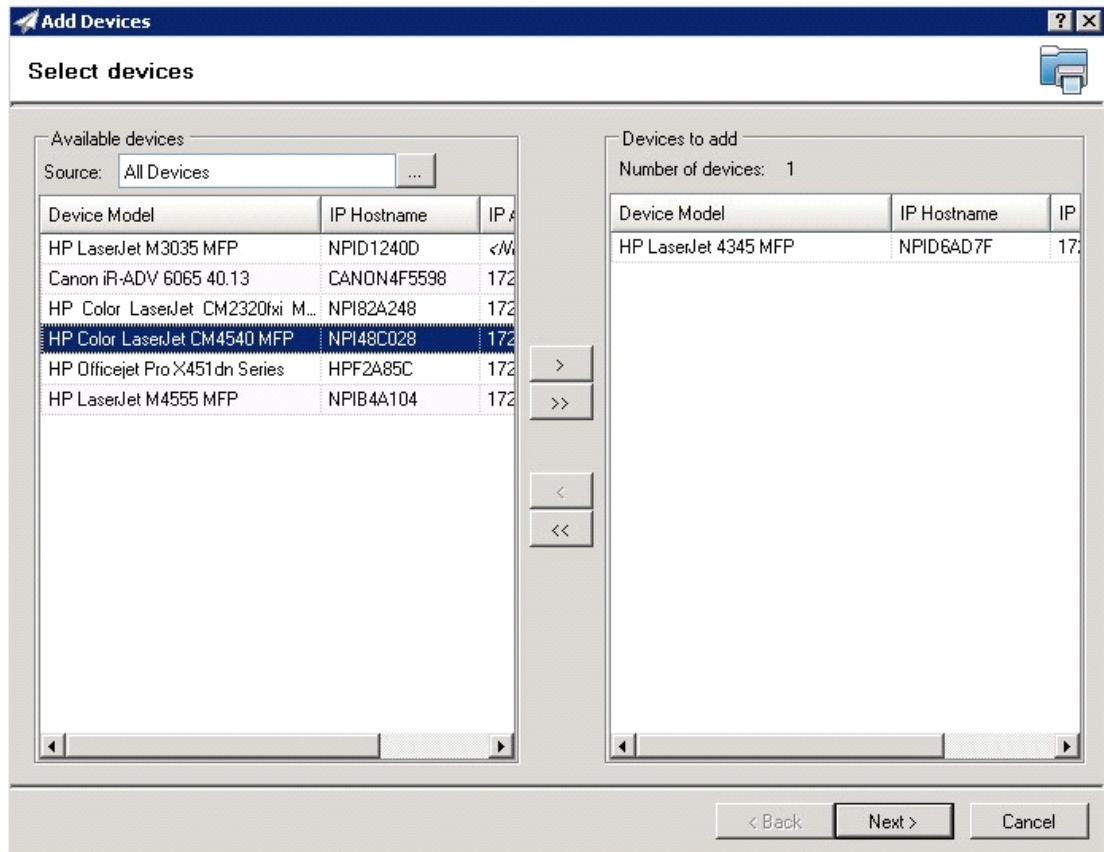
7 Click **Next**. The **Confirm** page appears.

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

9 Highlight the device(s) on which you want to install buttons.
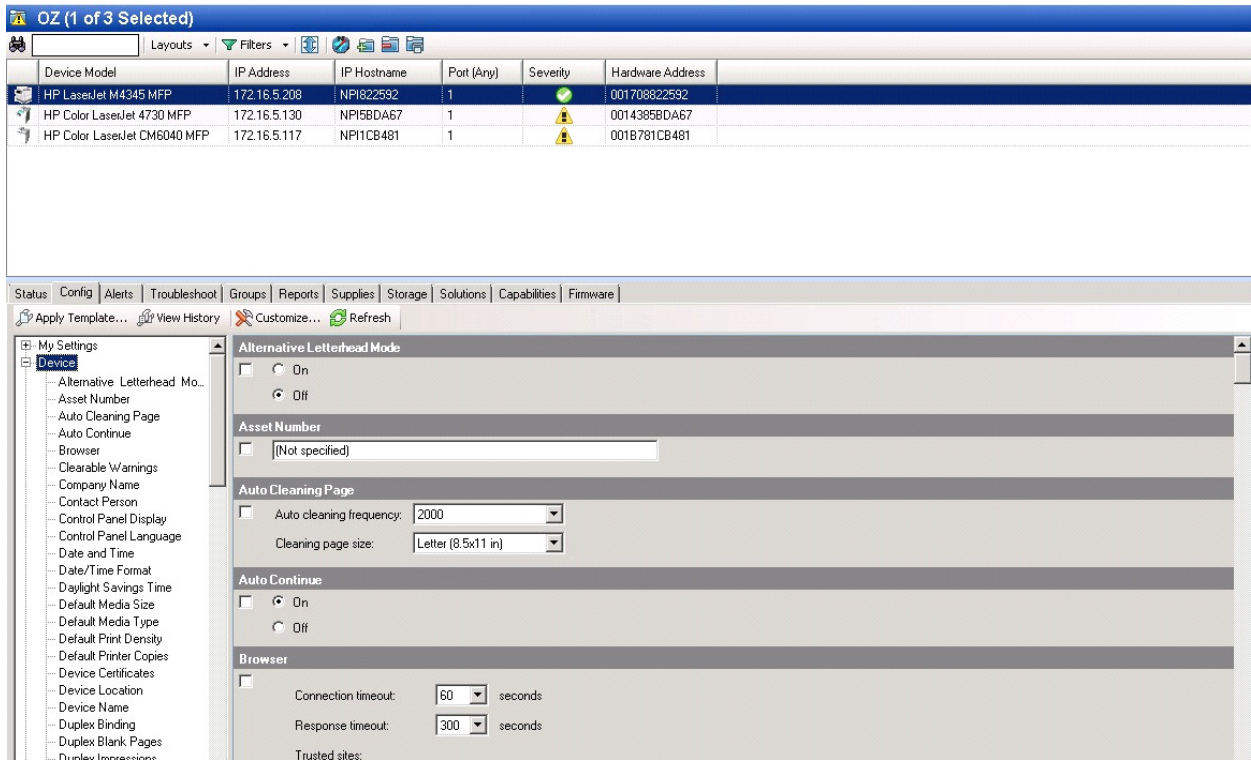
10 Click the **Config** tab and scroll to the **Embedded Device Functions** subset (as shown below) and check the box in the upper left corner of the center screen. The title bar of that area will read: *Embedded Device Functions (Changes Pending - Click 'Apply' to continue)*.
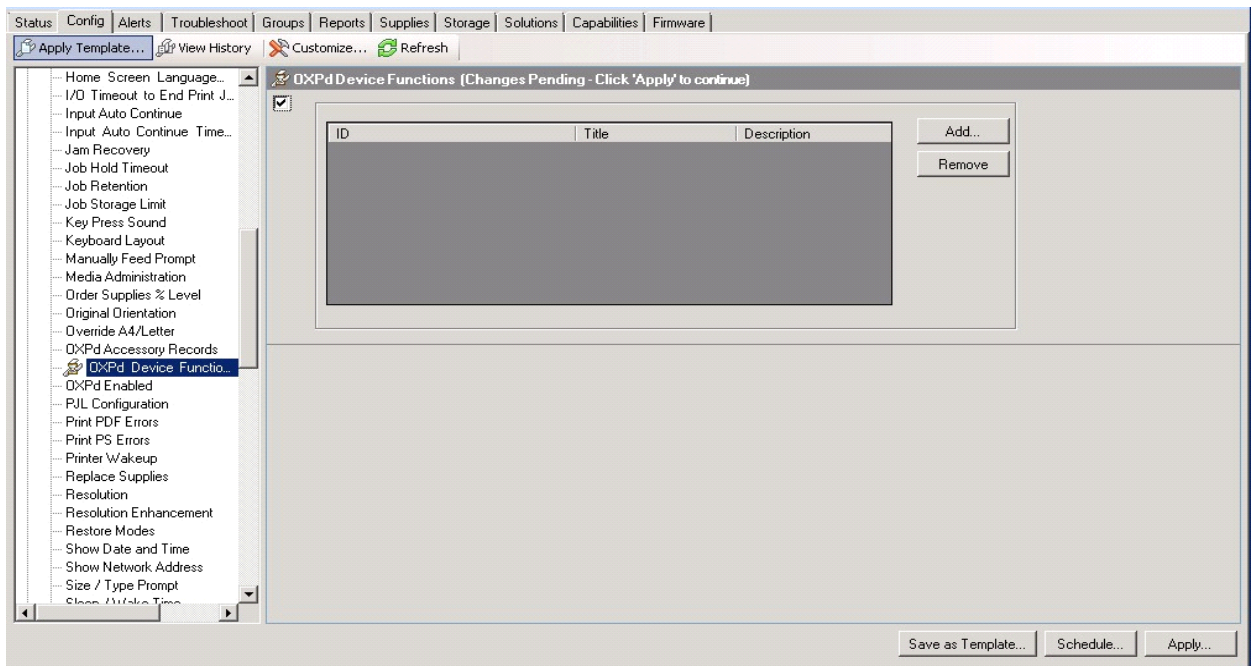
11   Click the **Add** button. The **Add Embedded Device Functions** page appears.
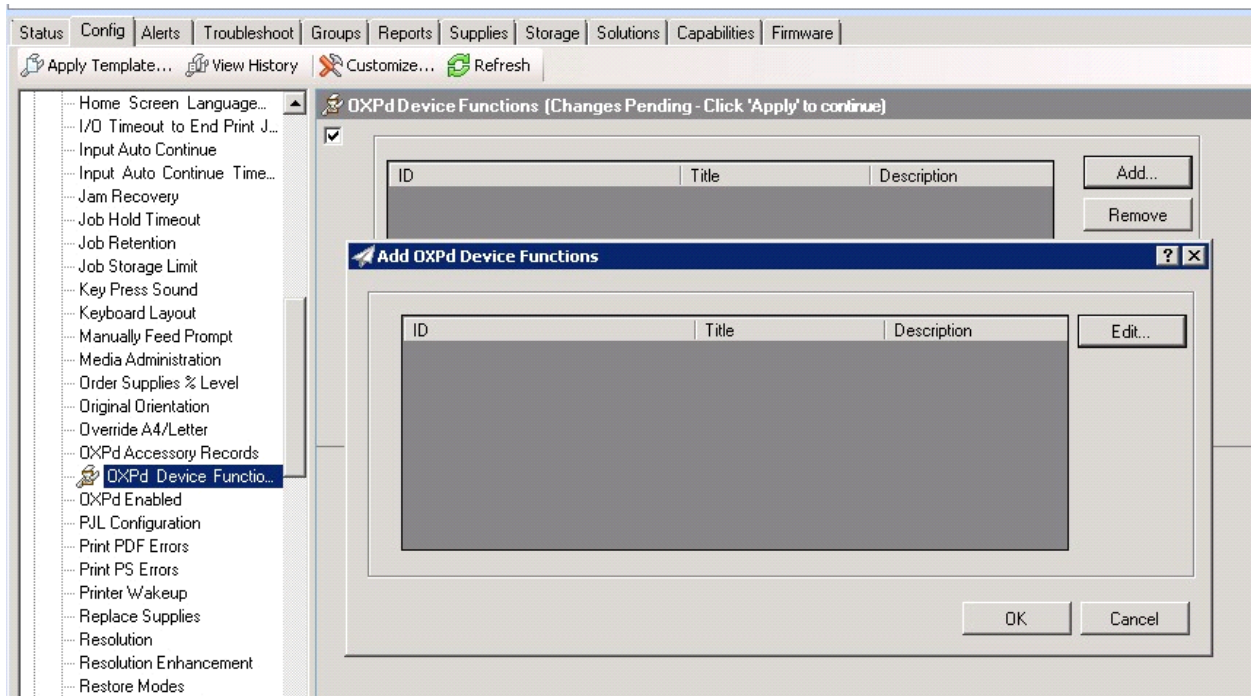
12 Click the **Edit** button. The **Embedded Device Function Repository** page appears and enables you to import the edited Embedded Device solutions XML files (from Exporting the XML files on page 9-2).
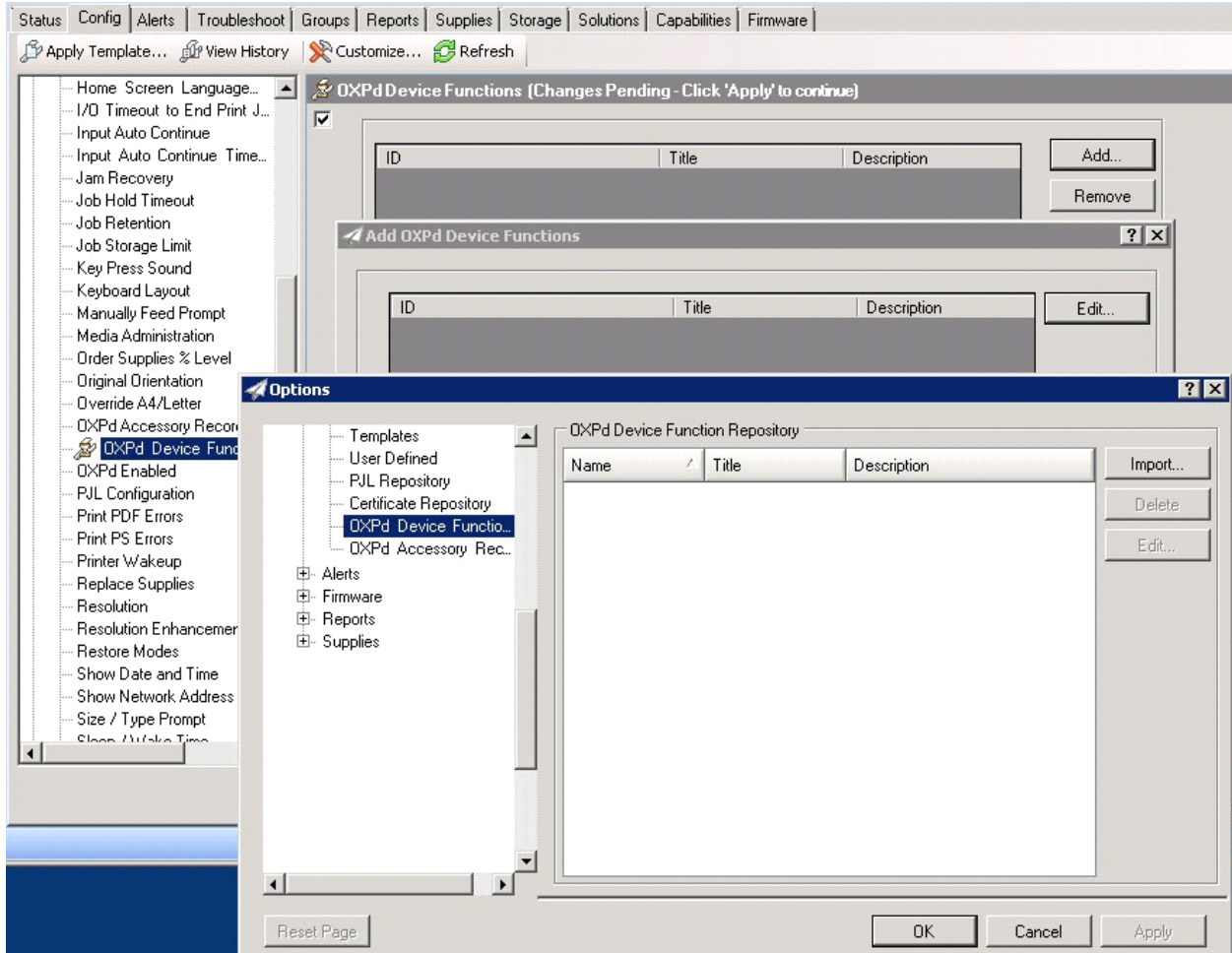
13 Click **Import**. In the **Open** page, search for your XML files.
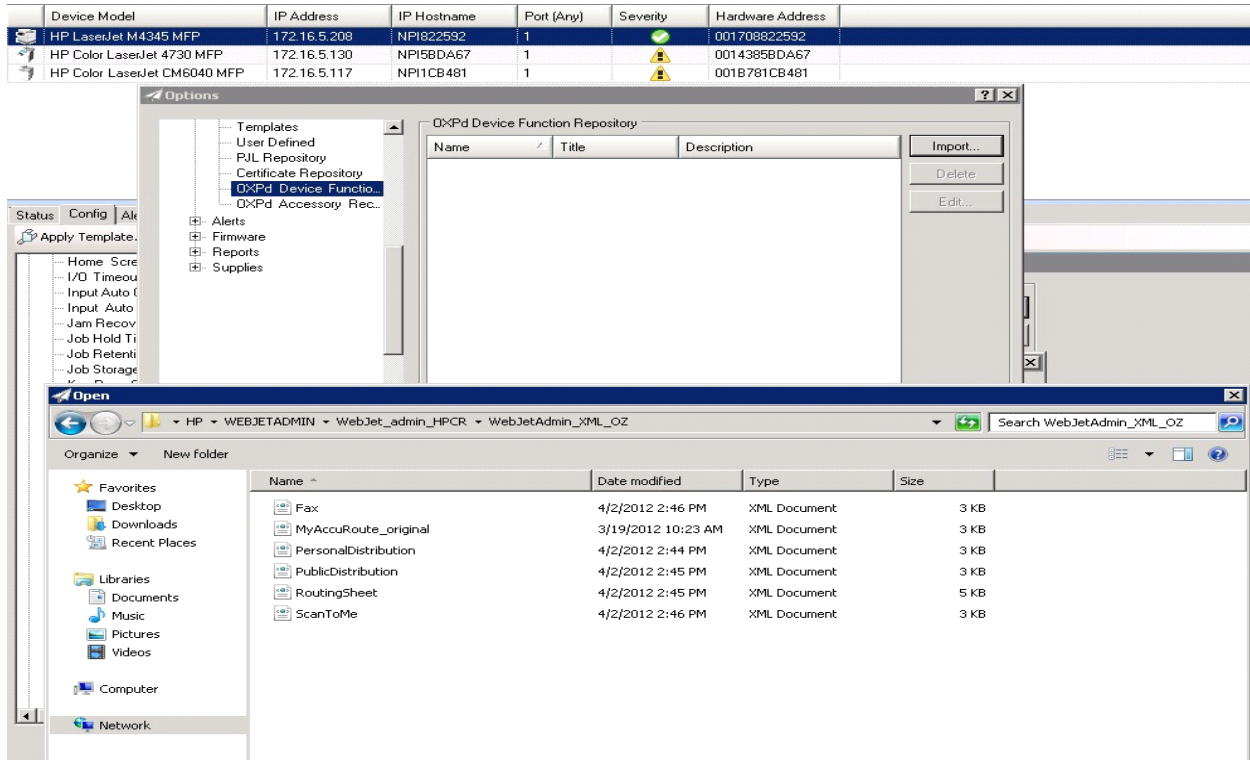
14 Select and highlight the file and then click **Open** to add the file. (You can import only one file at a time in the **Open** page.)

15 Verify that the selected feature XML file is reflected in the **Embedded Device Function Repository** page.
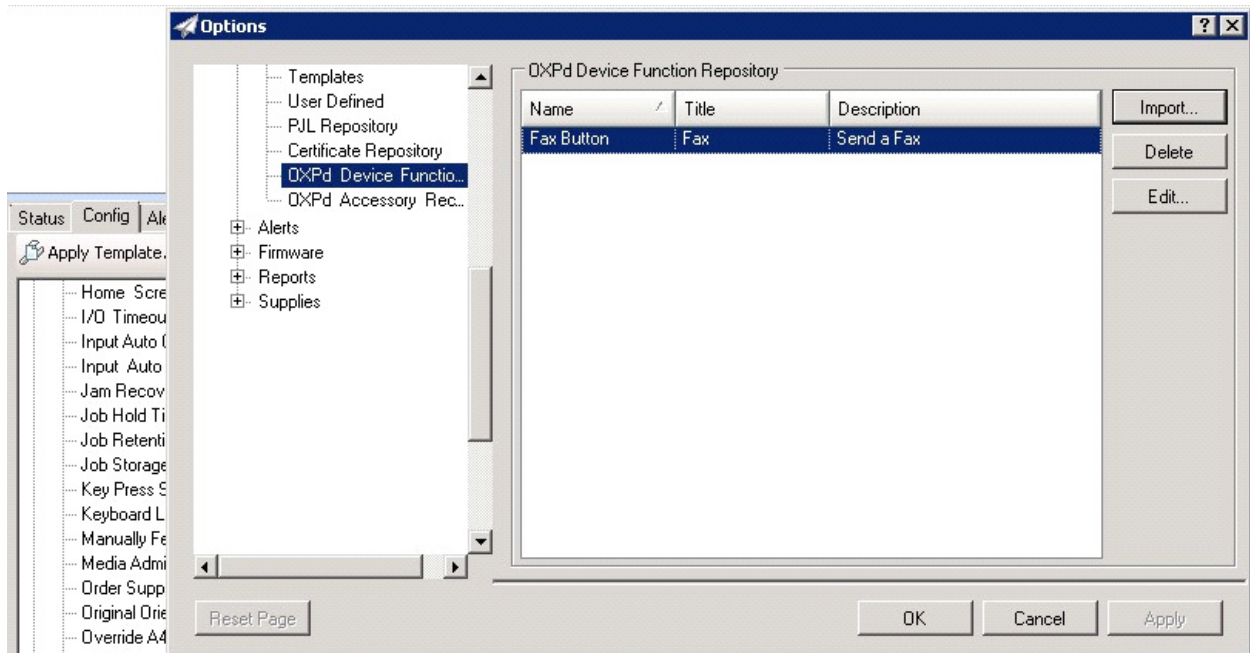
**16** Click **OK**. The **Add Embedded Device Functions** page appears.
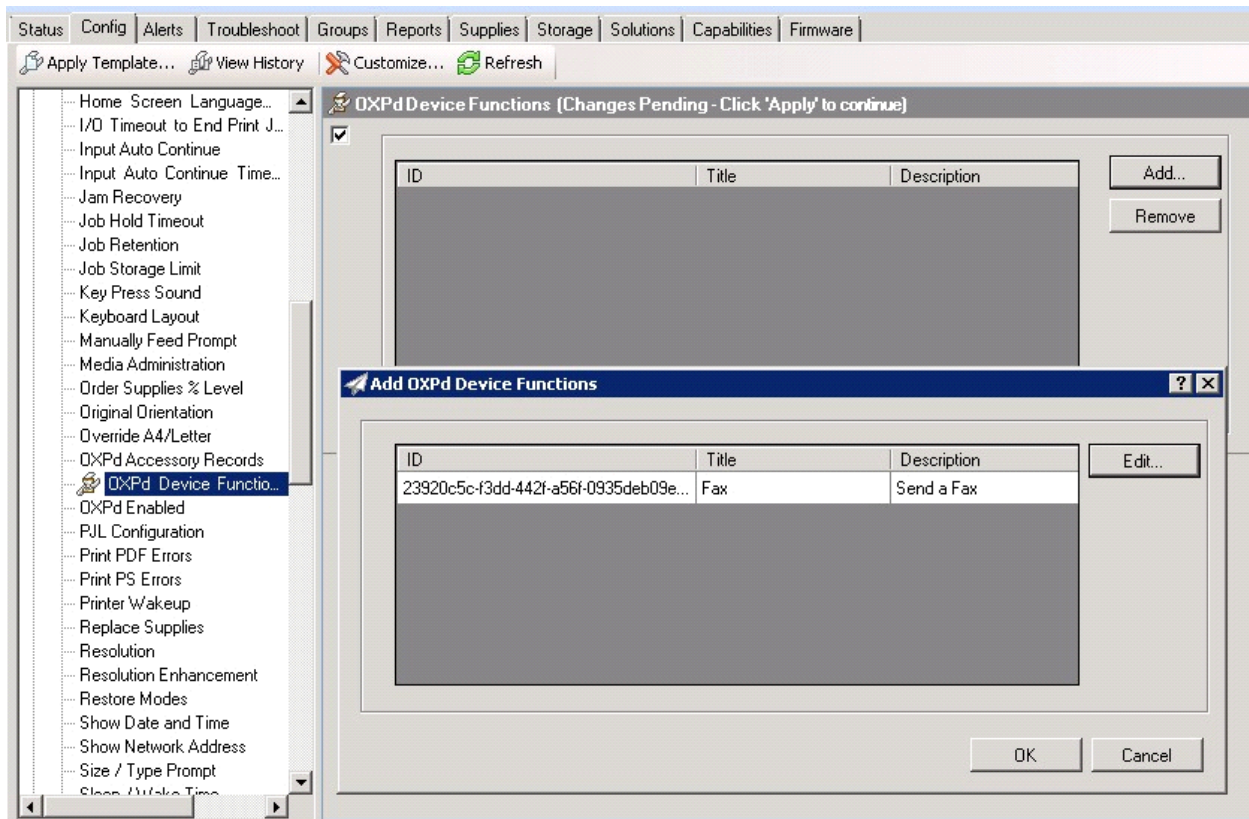
17 You should see the file referring to the feature(s) or button(s) you are about to install onto the device. Click **OK** to close the **Add Embedded Device Functions** page and return to the **Embedded Device Functions** page.

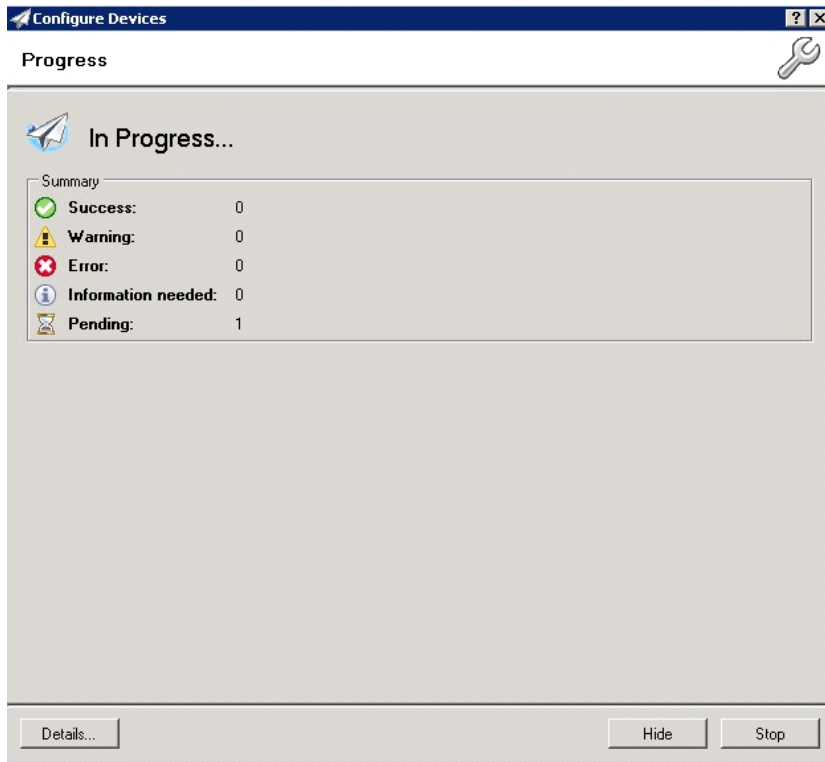At this point, you can continue to add another feature or button (repeating Steps 11 through 16).
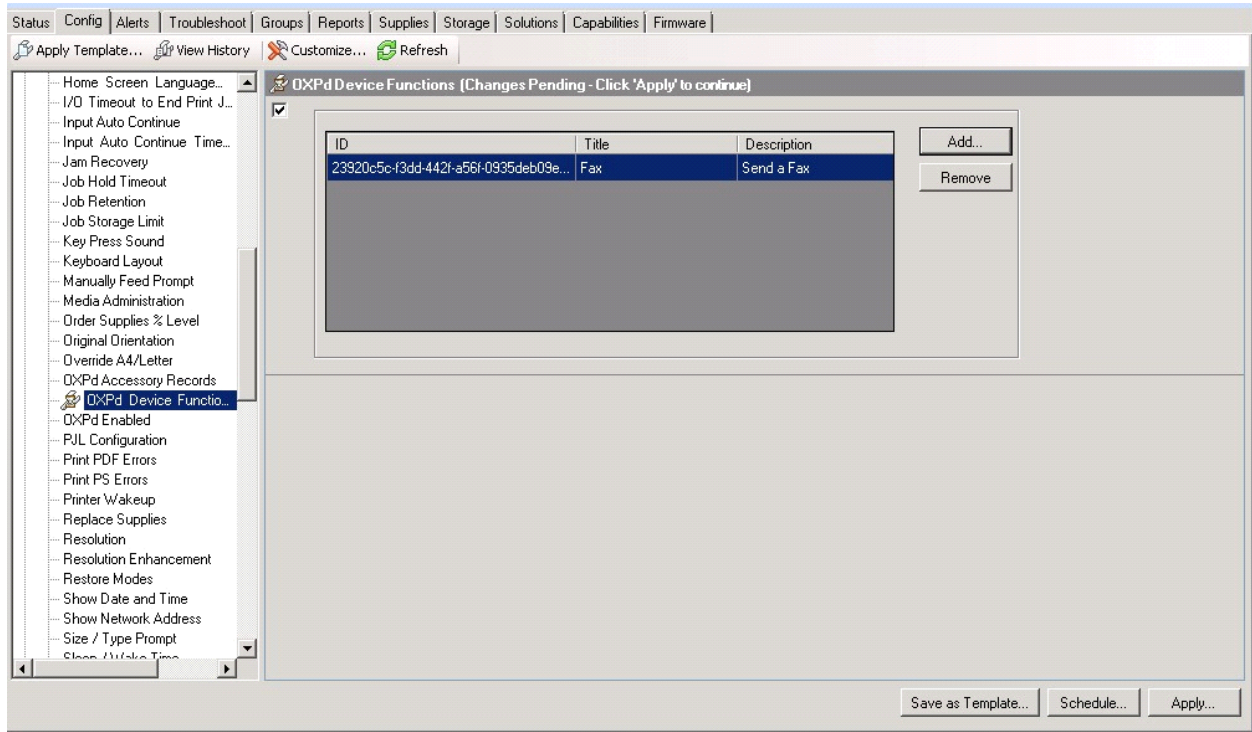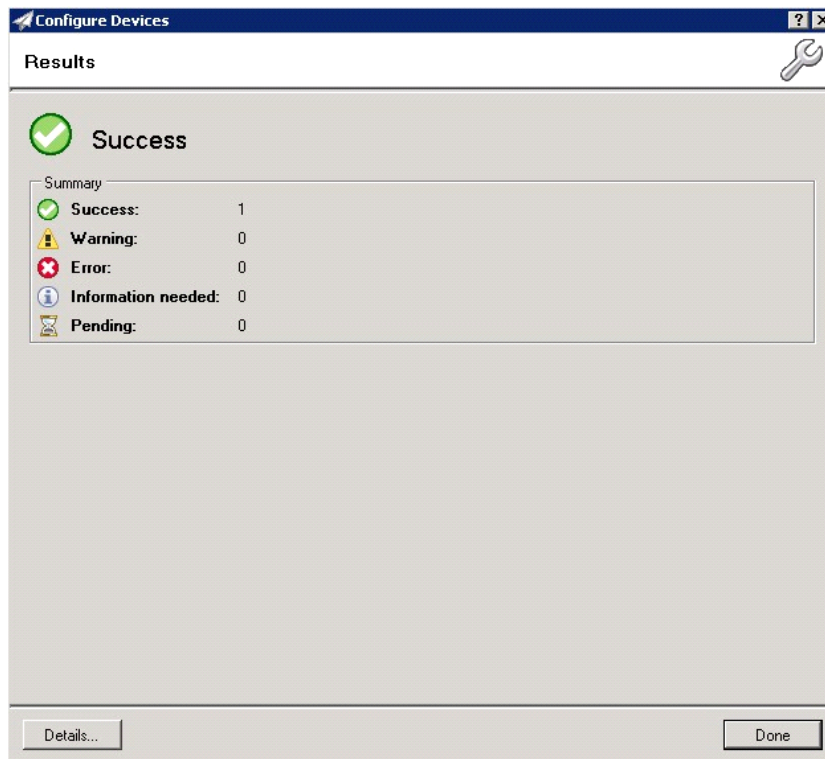
18 After you have added and confirmed all of the features/buttons of interest, click **Apply**. **Confirm** page appears.
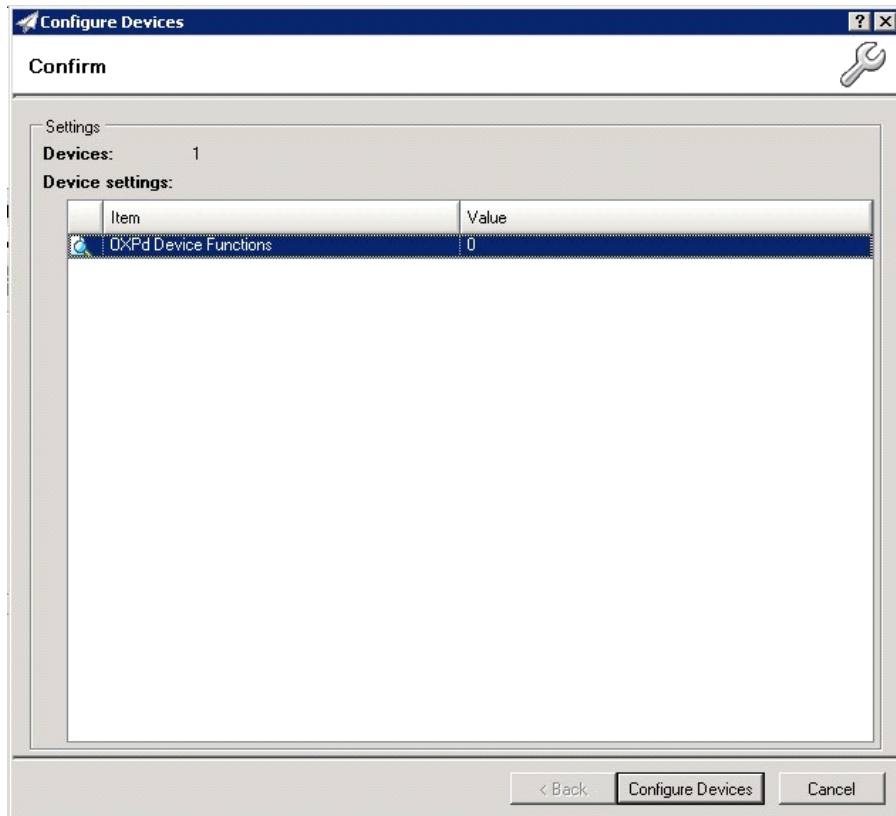
19 Click the **Configure Devices** button. The **In Progress** page appears.

The **Results** page indicates whether the installation was successful or an error was received.
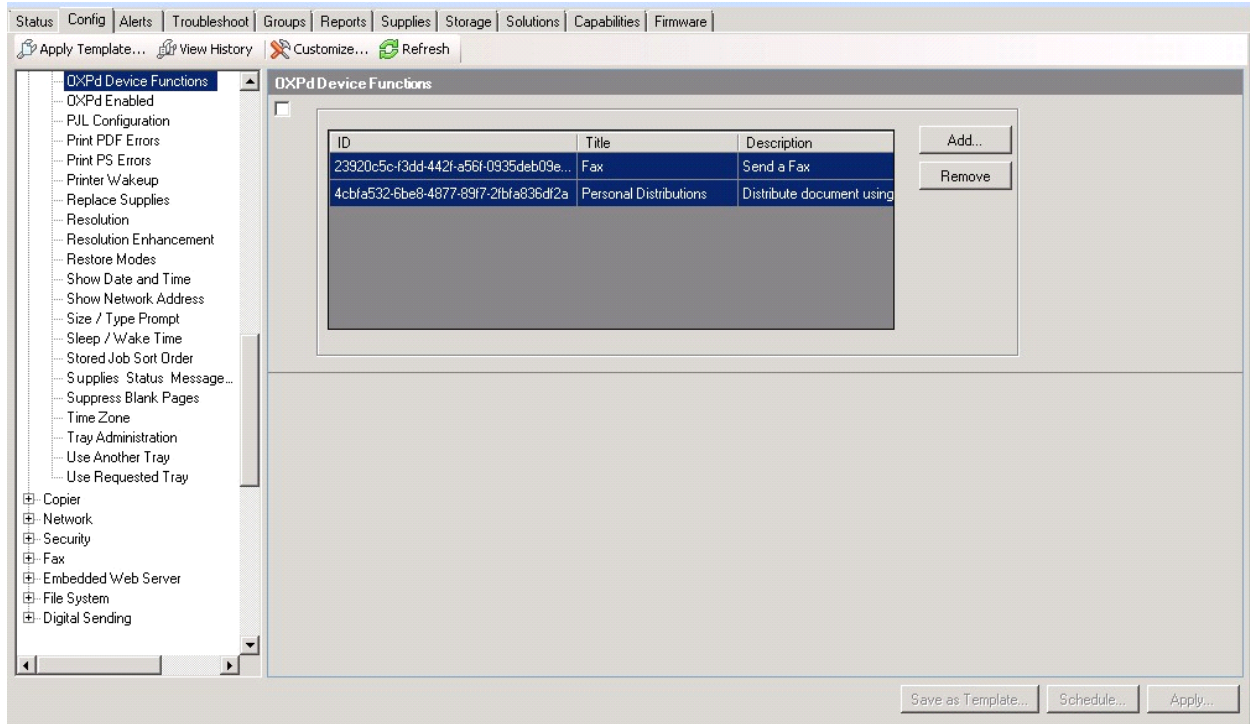
> **Note**   You can click the **Details** button to show additional notes if an error has occurred.

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

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

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

Section 9: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

Section 10: 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. This section includes:

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 AccuRoute Desktop or the AccuRoute Web Client 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:
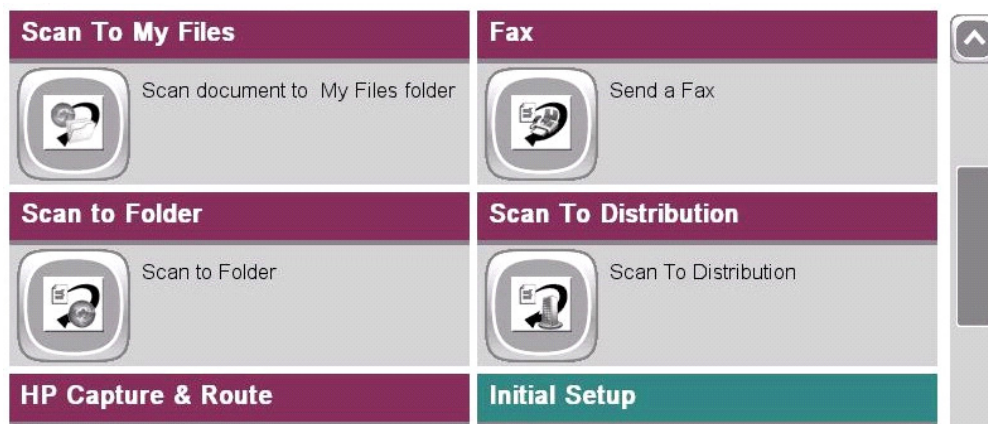
4 Load the document into the document feeder.

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**.

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

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

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

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

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

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

The message is transferred to the AccuRoute 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. Go to Section 11: Troubleshooting.

7   To scan another document using the Routing Sheet option, click **Back**. To end the session and go back to the main AccuRoute menu, click [🏠] or the **OK** button.

Important   If you see that the AccuRoute server cannot decipher or interpret the Distribution Rule instructions on the Routing Sheet, you must change the device setting from **mixed** to **text**. For instructions, see Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet (11-6)

Testing the Device Administrator user interface

To test the Device Administrator user interface, complete the procedure for Creating a group of devices (4-1).

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

- Email

- PIN

- Login

- Device

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

Section 11: Troubleshooting

This section includes:

If you cannot resolve an issue, contact Omtool support.

Detecting workflow issues

After a document has been scanned on the device, the document should arrive at its destination momentarily but can take up to several minutes when the server workload is high. If a document does not arrive at its destination within a reasonable period of time, begin troubleshooting the environment. Omtool recommends troubleshooting the workflow in reverse order because this is the easiest way to troubleshoot the setup on your own.
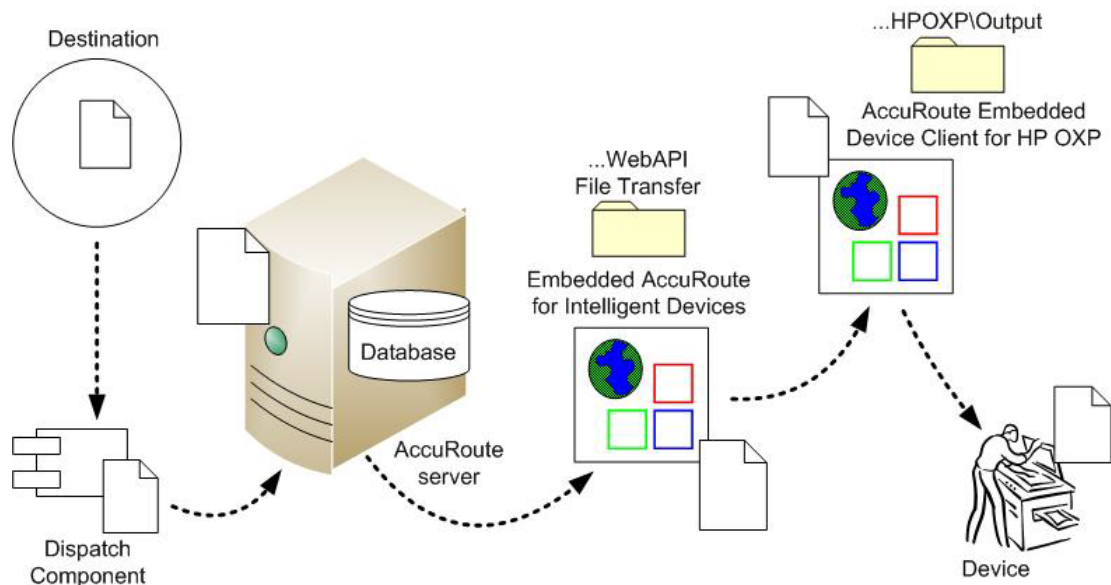
When a document does not arrive at its destination, troubleshooting starts with the delivery mechanism such as the mail server or DMS application, and then continues to the AccuRoute server, the AccuRoute Embedded Device Client for HP OXPd, the Web server, and the device.

Figure 11-1: **Troubleshooting the workflow in reverse order**

Troubleshooting the delivery mechanism

When the AccuRoute server finishes processing a message, an outbound connector routes the message directly to its destination or passes the message onto a delivery agent. If a delivery agent such as a mail server or DMS application is involved in the delivery process, do some basic troubleshooting on the delivery agent. If the delivery agent is functioning correctly, troubleshoot the message on the AccuRoute server. Continue to Troubleshooting messages on the AccuRoute server.

# Troubleshooting messages on the AccuRoute server

There are two important questions that can be resolved when troubleshooting a message on the AccuRoute server:

- Was the message submitted to the AccuRoute server?

- Assuming the message was submitted to the AccuRoute server, what caused the delivery failure? The state and status of the message, along with details in the message journal, provide some important clues.

Start troubleshooting by trying to locate the message on the AccuRoute server:

1   Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.

2   In the console tree, expand the AccuRoute Server Administrator and go to **[ServerName] > Messages**.

3   Look for the message in the In Process queue:

   a   Click **In Process**.

   b   View **All Items**.
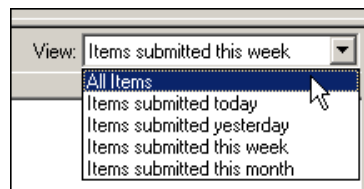
   c   Sort all items by the date submitted.

   d   Look for the message.

   ▸   **Message found** - View the message journal to determine the current state and status of the message. Then monitor the components and confirm that the message is moving through the processing queues on the AccuRoute server. If the AccuRoute server stops processing the message (for example, the message seems to be stuck in a processing queue), restart all the Omtool services.
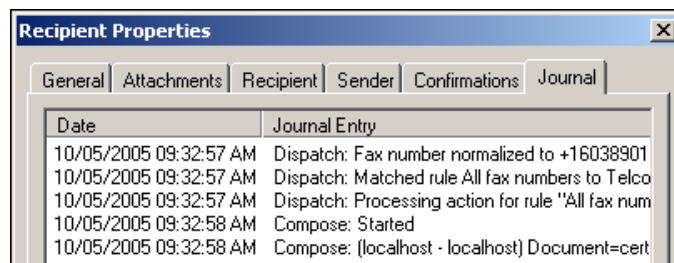
   ▸   **Message not found** - Go to step 4 and look for the message in the History queue.

4 Look for the message in the History queue:

a Click **History**.

b View **All Items**.
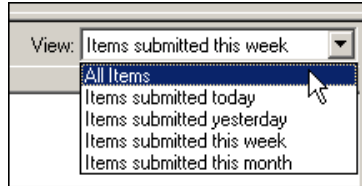
c Sort all items by the date submitted.

d Look for the message.

▸ **Message found** - View the message journal to determine the cause of the failure.
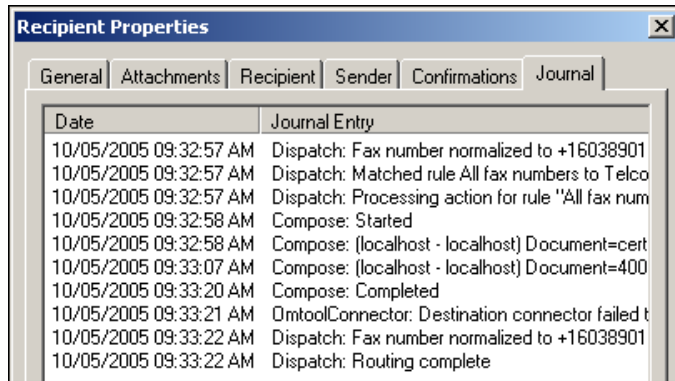
If the message failed, correct the issue and send the message again. Contact Omtool if you are unable to resolve the issue.

If the journal states that AccuRoute server delivered the message but it still has not arrived at its destination, this indicates that the AccuRoute server transferred the message to the delivery agent successfully. Do some advanced troubleshooting on the delivery agent to determine why the message is not being delivered to its destination. Contact Omtool if you are unable to resolve the issue.

▸ **Message not found**

Troubleshooting the Web server

The *Embedded AccuRoute for Intelligent Devices Installation Guide* has instructions on troubleshooting the Web server. For documentation related to AccuRoute v4.0, consult the [AccuRoute v4.0 documentation page](#).

If you cannot identify any issues with the Web server, troubleshoot the device. Continue to [Troubleshooting the multifunction device](#).

Troubleshooting the multifunction device

After troubleshooting all other components in the workflow, troubleshoot the device. Consult the HP documentation.

Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd

Problem:

When installing AccuRoute Embedded Device Client for HP OXPd v1.6 on a Windows 2008 R2 system, this message appears.

```
.NET Framework 3.5.1 must be installed using Server Roles before
continuing.
```

Solution:

.NET Framework v3.5.1 is not installed in your system. Install .NET Framework v3.5.1before proceeding with the AccuRoute Embedded Device Client for HP OXPd v1.6 installation.

For information on how to install .NET Framework v3.5.1, consult:

http://blogs.msdn.com/b/sqlblog/archive/2010/01/08/how-to-install-net-framework-3-5-sp1-on-windows-server-2008-r2-environments.aspx

Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster

Problem:

Issues related to permissions occur when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster environment.

Solution:

When setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster, you must configure permissions for the Anonymous user.

Procedures for setting up Embedded AccuRoute for Intelligent Devices in a cluster are provided in the appendix titled, *Setting up an AccuRoute server cluster*, in the [AccuRoute v4.0 Server Installation Guide.](#)

Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet

Problem:

When using an HP device to scan a document with a Routing Sheet, the AccuRoute server cannot decipher the instructions on the Routing Sheet and process the document.

Solution:

Change the device setting from scanning a Mixed document to scanning a Text document. To do so:

1   Open a Web browser and enter the IP address of the device.

2   Click **Log In** and login to the device using the device administrator name and password.

3   Click **Digital Sending > Preferences**.

4   For **Document Type**, change the chosen option from **mixed** to **text**.

Troubleshooting problems associated with applying all additional scan attributes

Problem:

All additional scan attributes are configured together (Darkness, back ground cleanup, contrast, sharpness, Heavy originals), and the following message appears when attempting to scan a document at the HP device:

> The action cannot be performed because options specified in the configuration file are not supported by this device. Try again on a different device.

Solution:

This message is displayed because the scan options are not supported by the device. Consult your HP manual or with your Administrator and find out which scan options are supported for your device model. The list of scan options commented in the configuration file are not supported by all the devices. Only those options that are supported by a particular device model should be un-commented and used.

Troubleshooting problems when scanning large documents

Problem:

After a document is scanned, the message indicating scan completion with delivery information is missing. However, the document is routed to the AccuRoute server for processing.

Solution:

Configure the following:

- Increase the sleep schedule from 10 minutes to the maximum, which is 4 hours
- Increase the inactivity timeout in the device Embedded Web Server to 300 seconds
- Increase the Content length in Internet Information Service Manager (IIS)

To increase the sleep schedule:

1 Log in to the Embedded Web Server.

2 Select the **General** tab.

3 In the left pane, locate **Sleep Schedule**.

4 Increase the Sleep Delay to the maximum allowable time: 120 minutes. Click **Apply**.

To increase the inactivity timeout in the device Embedded Web Server:

1 Log in to the Embedded Web Server.

2 Select the **General** tab.

3 In the left pane, locate **Control Panel Administration Menu**.

4 In the center pane, expand **Administration**.

5 Click on **Display Settings**.

6 Locate **Inactivity Timeout** and increase the value to 300 seconds.

To increase content length in IIS:

> **Note** The content length must be modified on both the OmtoolDXPWebApp1.6 and the OmtoolWebAPI sites.

1 Go to the Internet Information Services manager and select **OXP1.6** under **Sites**.

2 Double-click on **Request Filtering**.

3 Select **Edit Feature Settings** under the **Actions** menu.

4 Increase the value in **Maximum allowed content length**. The default value is 30000000. Modify the value to **3000000000**.

5 Select **WebAPI** under **Sites**.

6 Double-click on **Request Filtering**.

7 Select **Edit Feature Settings** under the **Actions** menu.

8 Increase the value in **Maximum allowed content length**. The default value is 30000000. Modify the value to **3000000000**.

9 Reset IIS.

Troubleshooting problems when scanning 100+ color pages

Problem:

When scanning more than 100 color pages, it takes additional time for the scans to arrive on the AccuRoute server.

Solution:

To improve performance.

1 Go to the Internet Information Services (IIS) manager configured for AccuRoute 4.0.

2 Open the following file for editing (such as with Notepad):

C:\Program Files (x86)\Omtool\OXP1.6

3 Locate <httpRuntime maxRequestLength="500000" executionTimeout=1800>. Change the executionTimeout to 5400:

<httpRuntime maxRequestLength="500000" executionTimeout=5400>

4 Save the file and restart IIS.

Troubleshooting an SNMP error

Problem:

When you perform an nvram full init, the Set Community string and the Get Community string are both set to public. However, when you set the admin password, it sets the Set Community string to the admin password. The networking tab of the Embedded Web Server of the device does not display the value if it is set. Instead it shows asterisks (***). The best practice is to set the value to blank, as it will assume public for both and display the value as "Not Set (default to public)."

Solution:

To display the value.

1   Log in to the Embedded Web Server.

2   Select the **Networking** tab.

3   Choose settings under security.

4   Under **SNMPc1/2** on the **Status** tab, there are two fields: **Get Community Name** and **Set Community Name**.

     Change the community name values by setting the values as blank for **Get Community Name** and **Set Community Name**.

5   Click **Apply** to remove any value. Now, no values are set for the two fields.