

AccuRoute[®] Embedded Device Client Installation Guide



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

About Upland Software

Upland Software (Nasdaq: UPLD) is an enterprise cloud software company that provides award-winning solutions in Project and IT Management, Workflow Automation and Digital Engagement. Our goal is 100% customer success, achieved through a unified operating platform that delivers the performance, scalability and support that over 2,500 Upland customers worldwide demand every day. Learn more at uplandsoftware.com.



© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute, Genifax, Image-In, ObjectArchive, ScanFacts, and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

Omtool product documentation is provided as part of the licensed product. As such, the documentation is subject to the terms outlined in the End User License Agreement. (You are presented with the End User License Agreement during the product installation. By installing the product, you consent to the terms therein.)

Permission to use the documentation is granted, provided that this copyright notice appears in all copies, use of the documentation is for informational and non-commercial or personal use only and will not be copied or posted on any network computer or broadcast in any media, and no modifications to the documentation are made. Accredited educational institutions may download and reproduce the documentation for distribution in the classroom. Distribution outside the classroom requires express written permission. Use for any other purpose is expressly prohibited by law.

Omtool and/or its suppliers make no guaranties, express or implied, about the information contained in the documentation. Documents and graphics contained therein could include typographical errors and technical inaccuracies. Omtool may make improvements or changes to the documentation and its associated product at any time.

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 I: Introduction

Overview of AccuRoute Embedded Device Client	. -
Main components of the environment	. I -4
Installation components	
Document workflow	
Workflow for the Fax, Routing Sheet, Scan to Destination, and Scan to Distribution features	. I -6
Workflow for the Fax Release feature	
Workflow for the Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files features	sI-8
Deploying AccuRoute Embedded Device Client	
Related documentation	

Section 2: Requirements

Supported devices	2-1
AccuRoute server requirements	2-1
Device authentication requirements	
Supporting large color documents	
Planning for Device Deployment	
Planning for HTTPS	
Device Group Planning	

Section 3: Installation

Installing the AccuRoute Embedded Device Client	3-	- 1
Installing the AccuRoute Embedded Device Client on a remote system	3-	-2

Section 4: Creating Device Groups on the AccuRoute Server Administrator

Creating a group of devices	4-1
Creating a group	4-1
Configuring authentication	
Specifying buttons for devices	
Adding new buttons	. 4-11
Configuring button properties	
Updating the Deviceloader.xml to support new devices	

Section 5: Installing Buttons on a New Device

Adding a new device and installing buttons	5-1
Configuring device authentication	
Configuring LDAP authentication	
Configuring AccuRoute device authentication	
Configuring the server	

Contents

Section 6: Configuring HP MFP Devices

Supported HP devices
Supported HP devices
Enabling HTTPS for SSL on HP S900 Series devices6-4
Adding buttons to HP S900 Series MFP devices6-4
Device authentication
Configuring FutureSmart and OZ devices6-6
Requirements for setting up a CA certificate6-6
Configuring HP Pro Devices (only)
Installing the AccuRoute Embedded Device Client on the server
Installing the OPS kit on the server
Adding the OPS server certificate to the Client certificate directory
Importing the OPS certificate into the device EWS
OPS registration
HTTPS support using the OPS-created certificate
Configuring HP Pro Devices on a remote OPS Server with HTTPS support
Installing the AccuRoute Embedded Device Client on the local server
Installing the OPS kit on the remote server
Exporting the OPS server certificate
Importing the OPS certificate into the device EWS
OPS registration
HTTPS support using the OPS-created certificate
Configuring HP FutureSmart, OZ, and PRO devices to use the OPS Server Certificate for HTTPS environments. 6-29
Exporting the certificate to the Embedded Device Client directory for FutureSmart and OZ devices 6-29

Section 7: Configuring Samsung Devices

Supported Samsung devices	7-1
Server Requirements	
Installation	
Installing the Device Client	7-2
Creating device groups	
Saving the Samsung .PAR file to the Clients directory	
Configuration	
Integrating the Samsung device with the AccuRoute Server Administrator	

Section 8: Configuring Xerox Devices

Supported Xerox devices	8-1
Configuring HTTPS support	8-2
Requirements for setting up a CA certificate	8-3
Downloading the MakeCert executable	8-3
Creating the certificate	8-3
Installing the certificate to Internet Information Services (IIS)	8-3
Creating an SSL binding	8-4
Requiring SSL for the virtual web sites	8-4
Enabling directory browsing is IIS	8-4
Verifying the SSL binding	8-5
Verifying HTTPS browsing	8-5
Editing the OmISAPIU.xml file	
Editing the Bootstrap.xml file	8-6
Configuring Xerox device authentication on the device	8-6

Contents

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

Supported Devices	9-	•1
Exporting the XML files	9-	.2
Manually importing a certificate		
Installing AccuRoute Embedded Device Client buttons	9-	.4

Section 10: Testing

0	
Testing the Routing Sheet feature	10-1
Testing the Device Administrator user interface	10-2

Section 11: Troubleshooting

Detecting workflow issues I	1-2
Troubleshooting the delivery mechanism I	1-2
Troubleshooting messages on the AccuRoute serverI	1-3
Troubleshooting the Web server	I-5
Troubleshooting the multifunction device I	I-5
Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd I	1-5
Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent	
Devices (Omtool ISAPI Web Server Extension) in a cluster I	۱-6
Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule	
instructions in a Routing Sheet I	۱-6
Troubleshooting problems associated with applying all additional scan attributes	
Troubleshooting problems when scanning large documents I	I-7
Troubleshooting problems when scanning 100+ color pages I	
Troubleshooting an SNMP error I	1-9

CON-4

Contents

Section I: 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:

Overview of AccuRoute Embedded Device Client (I-I)

Main components of the environment (I-4)

Installation components (1-5)

Document workflow (1-5)

Deploying AccuRoute Embedded Device Client (I-9)

Related documentation (1-9)

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.

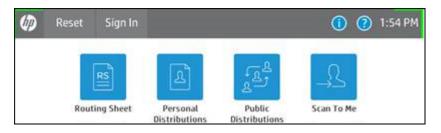


Figure 1-1: AccuRoute scanning features on the HP device running AccuRoute Embedded Device Client

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

|-|

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.)

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 <u>Configuring button properties</u> (4-12) during the device configuration.

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

^{© 2017} by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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 <u>Configuring button properties</u> (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	

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

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 <u>Section 3: Installation</u> for installation instructions.
- HP Device See <u>Supported devices</u> (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

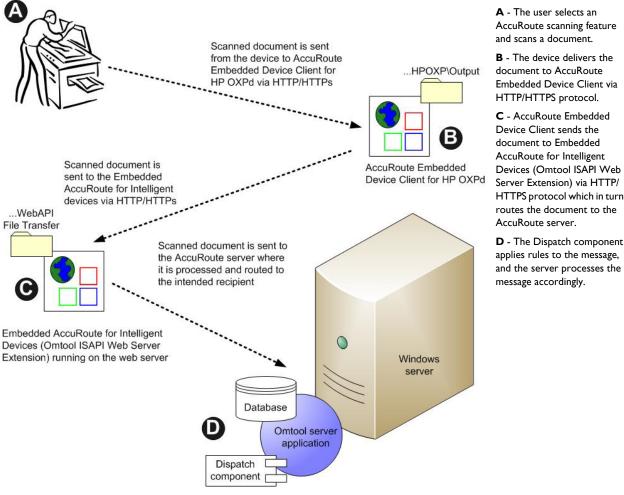


Figure 1-2: Workflow for Fax, Routing Sheet, Scan to Destination, and Scan to Distribution

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.

Workflow for the Fax Release feature

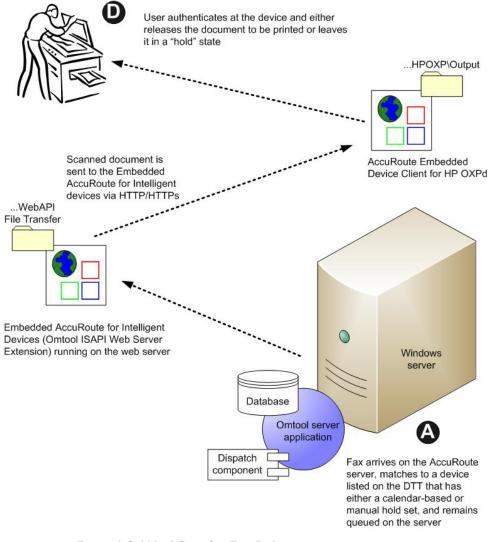


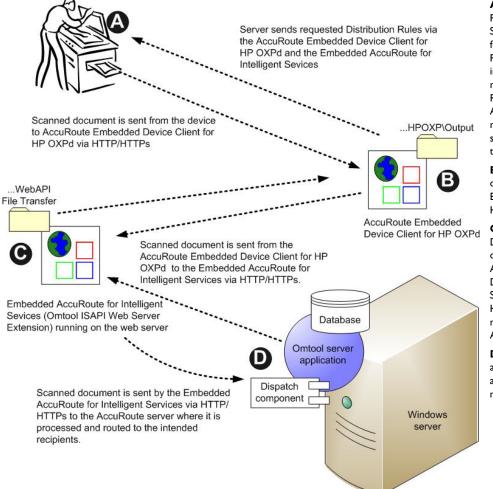
Figure 1-3: Workflow for Fax Release

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 <u>Configuring authentication</u> (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.



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

- I 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 <u>Section 3: Setting up a CA Certificate and SSL</u> (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 <u>http://</u>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 <u>http://www.omtool.com/</u> <u>documentation/accuroute/6.0/documentation.htm</u>.
- 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 I: Introduction

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

Section 2: Requirements

This section includes:

Supported devices (2-1)

AccuRoute server requirements (2-1)

Device authentication requirements (2-2)

Supporting large color documents (2-2)

Planning for Device Deployment (2-4)

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:

- I 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:

- I 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 I.6 and WebAPI sites.

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

- I 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:

- I 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 <u>Configuring</u>. <u>HP Pro Devices (only)</u> (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 <u>Creating</u> 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 <u>Creating a group of devices (part 1)</u> (39).

Section 3: Installation

This section includes:

Installing the AccuRoute Embedded Device Client (3-1) Installing the AccuRoute Embedded Device Client on a remote system (3-2)

Installing the AccuRoute Embedded Device Client

- I 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.

🛃 AccuRoute Embedded Device Client	for HP OXP 1.6	- InstallShield Wi	zard 🔀
AccuRoute Embedded Device Client	for HP OXP 1.6 (Configuration	
Enter the AccuRoute Intelligent Devi	ce Client Server na	ame:	
AR40East			
InstallShield			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

- 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 Section 4: Creating Device Groups on the AccuRoute Server Administrator.

Installing the AccuRoute Embedded Device Client on a remote system

I 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.

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.

3-2

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.

Section 4: Creating Device Groups on the AccuRoute Server Administrator

This section describes:

Creating a group of devices (4-1)

Specifying buttons for devices (4-10)

Updating the Deviceloader.xml to support new devices (4-30)

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

See also <u>Section 10: Testing</u> (10-1) and the <u>AccuRoute server administrator on-line help</u> (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

- <u>Creating a group</u> (4-1)
- Configuring authentication (4-6)

Creating a group

- I 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.

Section 4: Creating Device Groups on the AccuRoute Server Administrator

🚟 server - [Console Root]	
🚟 File Action View Favorites Window Helj	0
Console Root	Name
🗉 💭 Server Administrator	Server Administrator
E Selwinoshpdcr	
🛨 📬 Messages	
🗼 Connectors	
A Components	
🖃 🥮 Rules	
🔄 📩 Inbound Faxes	
🔄 💁 Outbound	
🖃 🌇 Configuration	
📑 Custom Options	
Normal Strategy Properties	
Folders	
🛃 Document Stamps	
Distribution Collections	
関 Web Client Views	
3 Groups	
C Devices	
	IP OXPd 1.4 group
New Window from Here	IP OXPd group
Help	

The **New Group** page opens.

ew Group		×
General Settings Authentication Buttons Advanced		
Type: HP 0XPd		
Name:		
Description		X
	OK	Cancel

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

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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

New Group	X
General Set	tings Authentication Buttons Advanced
Application:	
URL:	http://SERVER_IP/DeviceClient/
Type:	Unified
Web API	http://SERVER_IP/WebAPI/Scripts/omisapiu.dll
OPS Server:	172.16.20.74
Timeout:	C Automatically exit UI after 🙃 🚍 seconds of inactivity.
	C Do not exit UI Automatically
	OK Cancel

• 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: <u>Creating an SSL binding</u> (4-3) through to <u>Editing the OmISAPIU.xml file</u> (4-5).

Otherwise, continue the procedure below at <u>Configuring authentication</u> (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

- I 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

- I 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

- I 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

- I 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

- I 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).
- **II** Verify that the **localhost** page is displayed:

.../WebAPI/

12 Select Continue to this website (not recommended).

Editing the OmISAPIU.xml file

I 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 <u>Configuring authentication</u> below.

Configuring authentication

4-6

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

	ettings Authentication Buttons Advanced
	Domain User Entered Properties User User Entered Password User Entered
LDAP Look	kup Settings
Server:	VMELAD.VMELAD1.COM
Port:	389 🔽
Search B	ase: DC=VMELAD1,DC=COM
Filter:	(&(objectClass=user)(employeeID=[USER_NAME]))
Username	e: administrator
Password	t: WRENNER
Attribute I	Map: Exchange.default.xml
🔽 Bind u	using Windows Generic Security Services
	Attribute Aliases Test LDAP Lookup
	authentication
Confirm	

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:

Domain Field Properties	×
Label: @authDomainLabel	
Default_value:	
• User must enter a value for Domain	
Enable input validation	
Regular Expression:	
Error message: @authDomainErrorText	
O User must select a value for Domain from one of the following:	
	<u>A</u> dd
	<u>R</u> emove
	Set Default
	∧ v
C User may not enter a value for Domain	
\square Display the default value to the user (read-only)	
ОК	Cancel

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

- User must enter a value for Domain The device user will need to enter a domain for authentication during login at the device.
- User must select a value for Domain from one of the following If there are multiple domains in the environment, use this option to create a list of domains from which the user can select.
- User may not enter a value for Domain This option prohibits the user from entering a domain value. When you select this option, you can indicate that the device will Display the default value to the user (read-only). The user will see the Default value, but cannot change it.

Note Domain definition is optional for all authentication types.

Defining User Properties

4-8

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

User Field Prop	perties	×
Label:	PIN	
Default value:		
C User must er	nter a value for User	
🔲 Enable ir	nput validation	
Regular	Expression:	
Error me	essage: @authUserErrorText	
User must se 1234	elect a value for User from one of the following:	Add
4567		
		Remove
		Set Default
		~ v
C User may no	t enter a value for User	
🔲 Display t	he default value to the user (read-only)	
	ОК	Cancel

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

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

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

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:

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

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

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

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

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

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

New Group				×
General Setting	gs Authentication Butte	ons Advanced		,
Type: Email			•	
Fields: Dom User Pass		User Entered User Entered User Entered		Properties
LDAP Lookup S	ettings			
Server: VMEL	AD.VMELAD1.COM			_
Port: 389	•			
Search Base:	DC=VMELAD1,DC=COI	м		
Filter:	(&(objectClass=user)(pro	xyAddresses=SMTP:[U	ISER_NAME]))	
Username:				
Password:				
Attribute Map:	Exchange.default.xml			•
🔽 Bind using	Windows Generic Securi	ty Services		
		Attribute Aliases	Test LD	AP Lookup
Confirm authe	entication			
Message: 🧔	PmsgConfirmation			
			ОК	Cancel

- 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)
- <u>Configuring button properties</u> (4-12)

Adding new buttons

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

New Grou	р			X
General	Settings	Authentication Buttons Advan	ced	
Roi Per Put	Home Scr uting Shee sonal Distr blic Distribu an to me Files	t butions		Properties Add Remove Move ^ v
	Add But	ton		X
	Type: Name:	Fax Fax Release Mobile Reservation Nested Button Personal Distributions Public Distributions Routing Sheet Scan to Destination Scan to Distribution Scan to Distribution Scan to Didler Scan to me		×
			OK	Cancel

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

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

Add But	ton			×
Type:				_
Name:				
			OK	Cancel

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

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

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

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. <u>General Properties</u> 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)
- <u>Scan to Distribution</u> (4-15)
- <u>Fax</u> (4-17)
- Routing Sheet, Scan to Destination, Scan to Distribution, Scan to Me, and Scan to My Files (4-19)
- Fax Release (4-21)
- <u>Job Queue</u> (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

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

Button Properties 🛛 🛛 🗙				
General Jot	b Properties Prompts Device Settings			
Туре:	Scan to me			
Name:	Scan to me			
Display Text:	@buttonscantomeText			
Description:	@buttonscantomeDesc			
Image:	scantome			
Location:	Auto assign based on configured ordering Use specific ordering priority:			
Options:	 ✓ Enable this button for use on the device Enable Job Build mode by default Enable One-Touch scanning Enable Scan preview by default (only on supported devices) ✓ Require authentication ✓ Capture user password ✓ Always prompt user for password 			
	OK Cancel			

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 passthrough 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 I 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:
 - | 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

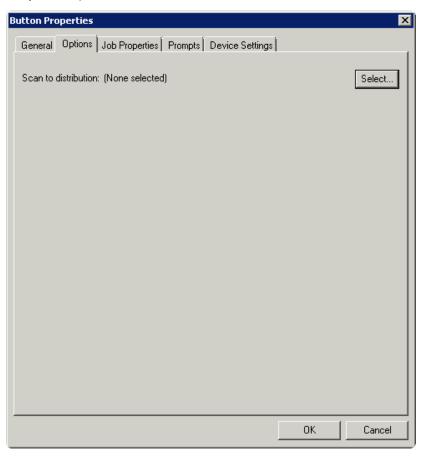
I If you are adding a **Personal Distributions** or **Public Distributions** button, click the **Options** tab.

Button Properties 🛛 🗙					
General Options Job Properties Prompts Device Settings					
Enable Public Distributions for the following user:					
Email: administrator@VMELAD1.COM					
Collection Name: Default Distributions					
Distribution Listing:					
 Display multiple Distribution Collections as a single List Display multiple Distribution Collections grouped by Distribution Collection name 					
Display the following Distribution Collections					
Name					
OK Cancel					

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

Scan to Distribution

I 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.

Select Empeda	d Directive	×
 Title Owner e-mail: Date created: Date last used: Expired Single use 	8/15/2012 8/15/2012 ★ to 8/15/2012 ★ to 8/15/2012	
Public		
		Find
Title 🔺 Owr	er Created Last U	sed Single Use Expires Select Cancel Properties

- 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

- I 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.

Button Properties 🛛 🗙
Button Properties Image: Confirmations is a properties is a prompt is in the properties is a prompt is in the properties is a prompt is include Coverpage to be specified Image: Coverpage is a prompt is prompt is a prompt is a prompt is a prompt is a prompt is
Comment:
Recipient Name: Sender Name:
OK Cancel

- 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).

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

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

I 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.

Job Property	Value	Properties
Originator OriginatorType	AccuRoute	Add
Destination RecipientType	routingsheet N	Remove

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

		Set Jol	b Property	i.	×
Property:	Destination				
Value:	routingsheet				
				ОК	Cancel

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

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

The default 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.

utton Properties	
General Job Properties Prompts Device Settings	
	Properties
proriginator = HPCapture&Route proriginatorType = 0	Add
Recipient prDestination = myfiles prRecipient Type = 0 Transformations	Remove

Fax Release

If you are adding a **Fax Release** button, once you define its <u>General Properties</u>, 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.

- I 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.

Group		×
General Clients Access Image-In Connect Mobile	We b Image: The provided of the property of the provided of	•
Web ✓ Features Custom Options Distribution Collections Document Stamps Fax Cover Pages Prompts Scan Settings		
 Jobs Apply Properties Destinations Folders Printers 		
L	OK Cancel He	elp

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**.

t View Properties		Folders	2
 Inbox Outbox SentItems Approval ibutions MyRules SubscribedRules Mobile Reservations es Files erences inistration Routing Calendars Help Desk	5		Properties
		ОК	Cancel

- 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.

New Fax Release S	Scheduling Calendar	Emai
~~ (
🗟 Messages		
Distributions	Name:	production hours
	Monday - Friday:	Start Time 07:00 💌 End Time 17:00 🗸
🍯 My Files	🗖 Saturday:	Start Time 00:00 💌 End Time 00:00 💌
🀱 Preferences	🗖 Sunday:	Start Time 00:00 💌 End Time 00:00 💌
dministration		OK Cancel
🖑 Help		

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

New Routing De	estination	
New Routing De « Messages Distributions My Files Feferences Administration Help	Fax number: Device Serial Number: Business Unit: Manual Hold: Intermediation Print on Device Printer: Regulated Printer? Regulated Destination Print on specific Media Letter Apply Document Stamp C Route via RightFax Destination Destination Destination Destination Destination Destination Delivery Format DOC (OCR Text	b)
	C Route via RightFax C E-Mail Destination Delivery Format DOC (OCR Text	:)

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.
- II Click OK.

^{© 2017} by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

Job Queue

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 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:

- I 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:

- I 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 Web Client, see the 'Configuring primary customized options on the Web Client Views Node' in the <u>AccuRoute Server Administrator Help</u>.
- 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:

- I 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:

- I 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 <u>AccuRoute Server Administrator Help</u>.

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.

Button Properties
General Job Properties Prompts Device Settings
Add Remove
Select Property Dictionary Field
AppCode DEFICIENCYSTATUS DeficiencyComments DeficiencyDescription DeliveredDocumentName DeliveredFormat DocumentStamp FolderID JobIDText LockUser Originator
OK Cancel
OK Cancel

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.

Button Properties		×
General Options J	lob Properties Prompts Device Settings	
		1
Setting	Value	Properties
Resolution	300 DPI	
Duplex	False	
Color Mode Compression	Monochrome Medium	
Orientation	Portrait	
Media Size	Letter	
incold bize	Editor	
	OK	Cancel

Setting	Value	Properties
Resolution	300 DPI	
Duplex Color Mode	False Monochrome	
Compression	Monochrome Medium	
Drientation	Portrait	
Media Size	Letter	
evice Setting	Properties	×
Resolution:	300 DPI	•
(Cooldon)	150 DPI	
	200 DPI	
	300 DPI	
	600 DPI	

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.

Device Group Properties х General Settings Authentication Buttons Advanced Name Value ConfigurationRefreshInterval 1800 Add DelayCount 100 JobRefreshTimer 3. ConnectionTimeout 60 300 ResponseTimeout RetryInterval 60 **MaxConsecutiveRetries** 3 UllnactivityTimer 60 NOTE: These settings are advanced and changing them could cause the button to no longer work and should only be done when requested by Support. ΠK. Cancel

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 <u>Installing AccuRoute Embedded Device Client buttons</u> (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 <u>AccuRoute server</u> 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:

Adding a new device and installing buttons (5-1)

Configuring device authentication (5-4)

Configuring the server (5-6)

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

Adding a new device and installing buttons

- I 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.

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

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

Propertie	s for I	HP OXPd de	vice				X
General	Conr	nection Jou	imal				
Device /	Authen	tication			 		-
Pass	word:						-
SNMP C	ommu	nity Strings –					-
Public	5 :	public					
Privat	e:						
				ОК	Cancel	Help	

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.

Properties for	HP OXPd 1.4 device		×
	rice Configuration Journal		1
Device Auther			
Username: Password:			[
	L for secure communication		
	ОК	Cancel	Help

- 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.
- **II** 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.

Section 5: Installing Buttons on a New 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:

- <u>Configuring LDAP authentication</u> (5-4)
- <u>Configuring AccuRoute device authentication</u> (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 <u>Defining Password Properties</u> (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 <u>AccuRoute v6.0 Documentation</u>.)

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)

Information Sett	ings Digital Sending Networking	
Configure Device	LDAP Authentication	
E-mail Server	LDAP Authentication	
Alerts		
AutoSend	Accessing the LDAP Server	
Security	LDAP Server Bind Method:	Simple
Authentication Manager	LDAP Server:	1711830785
LDAP Authentication	Port	389
Kerberos Authentication	1.012	389
PIN Authentication	Credentials	
Edit Other Links	Creuentiais	
Device Information	O Use Device User's Credentials	
Language	Bind Prefix:	cn
Date & Time	O Use LDAP Administrator's Credentials	
Wake Time	LDAP Administrator's DN	
A.4	Password:	

		① Device Administrator			
				Local Device	- 1
E Fax application	a			Use Default	2
E-mail application	a		v	Use Default	
E Address Book				Use Default	1
Save to USB application		1		Use Default	3
Save to SharePoint®				Use Default	1
Network Folder application				Use Default	1
Job Status application				Use Default	2
Administration application				Use Default	1
Device Maintenance application				Use Default	1
Public Datributions		V	v	Use Default	
Personal Distributions			V	LDAP	2
Fax		V		Use Default	1
Routing Sheet			v	Use Default	1
MyAccuRoute			V	LDAP	1
			N	Use Default	

Configuring AccuRoute device authentication

- I 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.

Configure Device	Authentication Manager	
Tray Sizes/Types	Addicition Manager	
E-mail Server		
Alerts	Set the Device Functions that require users to succe	ssfully sign in before use. Each function can require a different Sign In Method.
AutoSend		
Security	Home Screen Access	Sign In Method
Authentication Manager		
LDAP Authentication	Sign In At Walk Up	None
Kerberos Authentication	Device Functions	Sign In Method
Device PIN		
User PIN	Сору	None
Edit Other Links	Color Copy	None
Device Information	Send to E-mail	None
Language	Send Fax	None
Date & Time	Send to Folder	None
Sleep Schedule	Job Storage	None
Restrict Color	Create Stored Job	None
Certificate Management	Digital Sending Service (DSS) Secondary E-mail	None
Home Screen Setup	Digital Sending Service (DSS) Workflow	None
HPAC-Agent	Simplex Copy	None
Other Links	Public Distributions	None
hp instant support	Personal Distributions	None
Shop for Supplies	Fax	None
Product Support	Routing Sheet	None
	Scan To Me	LDAP
	Scan To Folder	None
	HP AC Express	HPAC - PIC Server
	Scan To My Files	
	· · ·	
	Future Installations	Sign In Method

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 <u>AccuRoute server administrator on-line help</u>.

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 <u>Section 10: Testing</u> (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...

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

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners

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	I.7, I.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	I.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

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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	I.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	ХХ	2403732_013003	1.7.3

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

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 <u>Section</u> <u>3: Setting up a CA Certificate and SSL</u>.

- I 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 <u>Using Nested</u> <u>buttons</u> (6-5).

I 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.

Dump XML	
New	٠
New Window from Here	
Help	

- 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:



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 <u>AccuRoute scanning features in AccuRoute Embedded Device</u> <u>Client</u> (1-2).

Device authentication

- I 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.
- II 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 <u>Section 4: Creating Device Groups on the AccuRoute</u> <u>Server Administrator</u> (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:

Downloading the MakeCert executable (6-7)

Creating the certificate (6-7)

Installing the certificate to Internet Information Services (IIS) (6-7)

Adding the certificate to the Client certificate directory (6-8)

Creating an SSL binding (6-8) Requiring SSL for the virtual web sites (6-18) Verifying the SSL binding (6-18) Enabling directory browsing in IIS (6-18) Verifying HTTPS browsing (6-19) Editing the OmISAPIU.xml file (6-19) Editing the Bootstrap.xml file (6-10)

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 <u>Microsoft</u> <u>documentation</u>.

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

Creating the certificate

- I 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 <u>On-line help for the administrator</u>. If you key in the command text, note that there is a space at the end of the first three lines shown above.

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

Installing the certificate to Internet Information Services (IIS)

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

- I 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.

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

- 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.

- I 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.
- **II** 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

- I 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

- I 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

- I 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

- I 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

- I 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).
- **II** Verify that the localhost page is displayed:

.../WebAPI/

12 Select Continue to this website (not recommended).

Editing the OmISAPIU.xml file

I 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

I 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:

Installing the AccuRoute Embedded Device Client on the server (6-11)

Installing the OPS kit on the server (6-11)

Adding the OPS server certificate to the Client certificate directory (6-16)

Importing the OPS certificate into the device EWS (6-17)

OPS registration (6-17)

HTTPS support using the OPS-created certificate (6-18)

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</u> <u>AccuRoute Embedded Device Client</u> (3-1) for more information.

Installing the OPS kit on the server

- I 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

tatus	Requirement	
ending	GnuWin32_OpenSSL-0.9.8h-1	
ending	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?

OP:	Shield Wizan requires the f alling these red	following items to be installed on	your computer. Click Instal	l to begin
Status Succeeded Installing	(?) T	Fo complete the installation of Apa estart your computer. Would you like to restart now?	ache CouchDB, Setup must Yes No	
	-		Instali	Cancel

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

ConstallShield Wizard
Welcome to the InstallShield Wizard for OPS
The InstallShield(R) Wizard will install OPSv0.4.7 on your
computer. To continue, click Next.
WARNING: This program is protected by copyright law and
international treaties.

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

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

OPS - InstallShield Wizard			×
License Agreement Please read the following license agree	ment carefully.		2
HP OXPd Professional Services As-Is Warranty	(OPS) End Use	r License Agre	eement and
PLEASE READ CAREFULLY BEF PRODUCT: This End-User License a contract between (a) you (either a (b) Hewlett-Packard Company ("HF software product ("Software"). This license agreement between you an including a license agreement in or may include (i) assessized media.	Agreement and an individual or tl ") that governs y EULA does not d HP or its supp line documenta	As-Is Warranty he entity you re your use of HP's apply if there is pliers for the Sol tion. The term	/ ("EULA") is present) and s OPS a separate ftware, Software"
• I accept the terms in the license agreen	nent		Print
I do not accept the terms in the license	agreement		
nstallShield			
	< Back	Next >	Cancel

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

6-13

The **Destination Folder** screen appears.

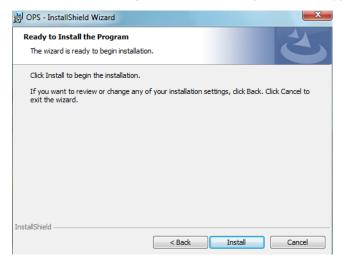
討 OPS - In:	nstallShield Wizard	x
	tion Folder ext to install to this folder, or click Change to install to a different folder.	5
Ø	Install OPS to: C:\Program Files (x86)\Hewlett-Packard\OPS\ Change	
InstallShield -	< Back Next > Cance	el

9 Click Next. The OPS Instance Details screen appears.

OPS Insta	nce Details		
Enter the OPS and DB details for the instance			
PS Details	5:		
lostname	192.168.30.81	Username	admin
Port	0004	Password	
ort	8081		
	,	 	1
B Details:	,	Username	admin
B Details: BName			Jadmin
B Details: BName	oxpdleops	Username Password	admin OPS Debug Log
B Details: BName	oxpdleops	 Username Password	

- 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.
- II 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.

B OPS - InstallShield Wizard	
2	InstallShield Wizard Completed
	The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.
	₽ Launch OPS
	☑ Show the readme file
	< Back Finish Cancel

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.

📴 OPS - InstallShield Wizard		×
2	InstallShield Wizard Completed	
	The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.	
OPS - InstallShie	eld Wizard	
OPS S	erver listening at: https://192.168.30.81:8081	
	ОК	
	< Back Finish Cancel	

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

OP5	Name 🔶	Description	Status	Startup Type	Log On As
	G Office Source Engine	Saves inst		Manual	Local System
Stop the service	G Office Software Pr	Office Soft		Manual	Network S
<u>Pause</u> the service Restart the service	G Omtool Address Bo	Manages t	Started	Automatic	TESTDC\s
vestory are service	🖓 Omtool Component	Manages t	Started	Automatic	TESTDC\s
	G Omtool Connector	Manages t	Started	Automatic	TESTDC\s
	🖓 Omtool Device Man	This servic	Started	Automatic	TESTDC\s
	🖓 Omtool Message Se	Manages al	Started	Automatic	TESTDC\s
	G Omtool Mobile Push	This servic	Started	Automatic	TESTDC\s
	G Omtool Modem Man	Manage all	Started	Automatic	TESTDC\s
	🖓 Omtool Notification	Manages t	Started	Automatic	TESTDC\s
	Contool ObjectArchive	Manages t		Automatic	TESTDC\s
	G Omtool ObjectArchi	Manages b		Automatic	TESTDC\s
	OPS COPS		Started	Automatic	Local System
	Rerformance Count			64-bit processes t	o query performan
	Rerformance Logs	provided by 32	2-bit DLLs.		
	Rug and Play	Enables a c	Started	Automatic	Local System
	RP-X IP Bus Enum	The PnP-X		Disabled	Local System
	Rortable Device En	Enforces g		Manual	Local System
	S Power	Manages p	Started	Automatic	Local System
	Rrint Spooler	Loads files	Started	Automatic	Local System

Adding the OPS server certificate to the Client certificate directory

- I 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

- I 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

I 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 <u>Installing the OPS kit on the</u> <u>server</u> (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 <u>Installing the OPS kit on</u> the server (6-11).

7 The following message appears:

OPS Registered successfully

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

HTTPS support using the OPS-created certificate

Creating an SSL binding

- I 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

- I 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

- I 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

- I 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

- I 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).
- **II** Verify that the localhost page is displayed:

.../WebAPI/

12 Select Continue to this website (not recommended).

Editing the OmISAPIU.xml file

I 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 Installing the OPS kit on the server.

Note XML files can be edited using Microsoft Notepad.

3 Save the file.

Editing the Bootstrap.xml file

- I 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 Installing the OPS kit on the server.

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:

Installing the AccuRoute Embedded Device Client on the local server (6-20) Installing the OPS kit on the remote server (6-20) Exporting the OPS server certificate (6-25) Importing the OPS certificate into the device EVVS (6-26) OPS registration (6-26) HTTPS support using the OPS-created certificate (6-27) 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 Installation (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

- I From the local server (System A), navigate to the \Tools folder on the remote server (System B).
- 2 Right-click and select Run as Administrator.
- **3** Run setup.exe for OPS on System B.
- 4 The OPS InstallShield wizard appears and requests that you install the following two items:

- GnuWin32_OpenSSL-0.9.8h-1
- setup-couchdb-1.2.0 otp R15B

OPS - InstallShield Wizard OPS requires the following items to be installed installing these requirements.	ed on your computer. Click Install to begin
Status Requirement Pending GnuWin32_OpenSSL-0.9.8h-1 Pending setup-couchdb-1.2.0_otp_R15B	
	Install Cancel

- 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?

installin	uires the following items to be installed on your computer. Click Install to begin g these requirements.
Installing	To complete the installation of Apache CouchDB, Setup must restart your computer. Would you like to restart now?
	Yes No

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.

😸 OPS - InstallShield Wizard			X
License Agreement Please read the following license agreen	nent carefully.		2
HP OXPd Professional Services (As-Is Warranty	OPS) End Use	r License Agre	ement and
PLEASE READ CAREFULLY BEF(PRODUCT: This End-User License a contract between (a) you (either a (b) Hewlett-Packard Company ("HP' software product ("Software"). This E license agreement between you and including a license agreement in on may include (i) associated modia. (i)	Agreement and n individual or th) that governs y EULA does not I HP or its supp line documentat	As-Is Warranty ne entity you rep your use of HP's apply if there is liers for the Soft tion. The term "S	oresent) and OPS a separate ware, Software"
• I accept the terms in the license agreem	ent		Print
\bigcirc I do not accept the terms in the license a	greement		
InstallShield			
	< Back	Next >	Cancel

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

The **Destination Folder** screen appears.

👸 OPS - In:	nstallShield Wizard	×
	tion Folder ext to install to this folder, or click Change to install to a different folder.	3
Ø	Install OPS to: C:\Program Files (x86)\Hewlett-Packard\OPS\	nange
InstallShield -		
	< Back Next >	Cancel

9 Click Next. The OPS Instance Details screen appears.

015 1115	tallShield Wizard		
OP5 Instance Details Enter the OPS and DB details for the instance		e instance	2
PS Details	s:		
Hostname	192.168.30.81	Usernam	e admin
Port	8081	Password	
		- Dagers	
	oxpdleops	Usernam	e admin
B Details: DBName Port		Usernam Password	
OBName	oxpdleops	Password	

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

PPS - InstallShield Wizard

 Ready to Install the Program

 The wizard is ready to begin installation.

 Click Install to begin the installation.

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

InstallShield

 ABack
Install
Cancel

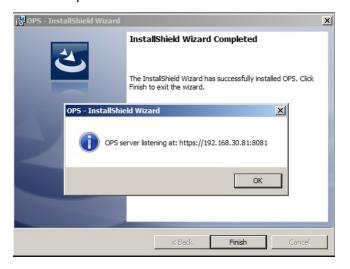
12 Click Next. The Ready to Install the Program screen appears.

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

B OPS - InstallShield Wizard	
	InstallShield Wizard Completed
0	The InstallShield Wizard has successfully installed OPS. Click Finish to exit the wizard.
44.0	I Launch OPS
	Show the readme file
	< Back Finish Cancel

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.

OPS	Name 🔶	Description	Status	Startup Type	Log On As
	G Office Source Engine	Saves inst		Manual	Local System
Stop the service	G Office Software Pr	Office Soft		Manual	Network S
<u>Pause</u> the service Restart the service	G Omtool Address Bo	Manages t	Started	Automatic	TESTDC\s
	G Omtool Component	Manages t	Started	Automatic	TESTDC\s
	G Omtool Connector	Manages t	Started	Automatic	TESTDC\s
	G Omtool Device Man	This servic	Started	Automatic	TESTDC\s
	G Omtool Message Se	Manages al	Started	Automatic	TESTDC\s
	G Omtool Mobile Push	This servic	Started	Automatic	TESTDC\s
	G Omtool Modem Man	Manage all	Started	Automatic	TESTDC\s
	G Omtool Notification	Manages t	Started	Automatic	TESTDC\s
	C Omtool ObjectArchive	Manages t		Automatic	TESTDC\s
	G Omtool ObjectArchi	Manages b		Automatic	TESTDC\s
	CPS CPS		Started	Automatic	Local System
	Performance Count Performance Logs	Enables remote provided by 32		64-bit processes t	o query performan
	Plug and Play	Enables a c	Started	Automatic	Local System
	RnP-X IP Bus Enum	The PnP-X		Disabled	Local System
	Portable Device En	Enforces g		Manual	Local System
	S Power	Manages p	Started	Automatic	Local System
	Rrint Spooler	Loads files	Started	Automatic	Local System

Exporting the OPS server certificate

- I 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.

10 Select Next and then click Finish.

Importing the OPS certificate into the device EWS

- I 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

I 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 <u>Installing the OPS</u> <u>kit on the remote server</u> (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 <u>Installing the OPS kit on</u> 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 <u>Creating a group of devices</u> (4-1) for more information on creating device groups.

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.

HTTPS support using the OPS-created certificate

Creating an SSL binding

- I 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

- I 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

- I 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

- I 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

- I 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).
- **II** Verify that the localhost page is displayed:

.../WebAPI/

12 Select Continue to this website (not recommended).

Editing the OmISAPIU.xml file

- I Navigate to the following path.
 - C:\Program Files (x86)\Omtool\OmtoolServer\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</u> server (6-20).

Note XML files can be edited using Microsoft Notepad.

4 Save the file.

Editing the Bootstrap.xml file

I 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</u> remote server (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</u>. <u>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.

- I 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 6: Configuring HP MFP Devices

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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 <u>Customer Service</u> for the download instructions.

This section includes:

Supported Samsung devices (7-1) Server Requirements (7-2) Installation (7-2) Configuration (7-3)

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

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

Server Requirements

- AccuRoute Server v6.0
- Samsung .PAR file (saved to a known location)

For AccuRoute Server installation and configuration instructions, consult the <u>AccuRoute Server Installation and</u>. <u>Configuration Guide</u>.

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 <u>Section 4: Creating Device Groups on the AccuRoute Server Administrator</u> (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 <u>Configuration</u>, below.

Configuration

This section describes the configuration process for Samsung devices.

Refer to <u>Creating Device Groups on the AccuRoute Server Administrator</u> and <u>Installing Buttons on a New Device</u> 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.

I 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.

SyncThru™	SAMSUNG 50	X-8128NX					Job Status Dire	ect Print Eco OFF Si	te Map Login	English	•
SyncThru [™] Web Service		Information	Address Book	Mainten	ance						
Home											• ي
Device Information											^
					Model Name	SCX-8128					- 8
	Status	80Error			Host Name	SEC00159					- 10
and a state of	Alert	1 Alert(s) Occurred			Serial Number	ZB JEB 1AD					- 88
	Alerc	1 Alertisi Occurred			IPv4 Address	172, 16.5.3					- 88
-					IPv6 Address	Not Config					- 88
=					MAC Address	00:15:99:					- 88
					Location	Not Config					- 88
_					Administrator	Name Not					- 88
						E-mail Not					- 88
							Configured				
					Customer Support	Phone Not	Configured				- 20
Supplies Information											
Toner Cartridge					Imaging Unit						- 88
Cartridge		Remaining	Status		Unit		Remaining		Status		- 10
Black			100% Ready		Black			99%	Ready		- 10
Input Trays					Output Trays						-
							Copyright (C) 1995 Samsung Electroni	cs, All rights reserv	red. SAM	ISUNG

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:

Installation	
Package Name Provider	: OmtoolXOAApp : Omtool Pvt Ltd
Name	Version EULA
OmtoolXOAApp	1.0.0 Not Available
	Show EULA OK Cancel

9 Click **OK** and the following progress screen appears:

Installation								
Don't turn off the machine until 'Completed' message is displayed								
Completed	_							
Job Result								
OmtoolXOAApp - Success								
ОК								

10 Once complete, click **OK** to return to the EWS **Application** screen, where **OmtoolXOAApp** now appears in the application list, as shown below:

SyncThru™	SAMSUNG	ELX-8640		🚇 admin J	Job Status Direct Print	Eco OFF Site Ma	p Logout (02:57) 🛛 🕑	English
Web Service	6	Information A	ddress Book	Settings	Securi	ty	Maintenance	XOA
Maintenance	Application	1						
Maintenance Emware Version Application Management	Selected : 1 1 Add	otal : 12 Delete Detail	Setting					
Application		Namet	1	ersion	Type	State	Samsung Verifi	ed
License		Copy	0.6.2	110513.1-0.1	Platform	ENABLED	Verified	
▼ Backup/Restore	8	Fax	0.6.2	110513.1-0.1	Platform	ENABLED	Verified	
Backup		OmboolXOAApp	1	.0.0.564	Custom	ENABLED	Unverified	
Restore		Scan to Email	0.6.2	110513.1-0.1	Platform	ENABLED	Verified	

II Refresh the EWS screen. The **XOA** tab will appear beside the **Maintenance** tab, as shown:

SyncThru [™] samsums clax-8640 Web Service ☆ Information Addres			vncThru™ samsung clx+8640				🙀 admini i Job Status i Direct Print i Eco OPF i Site Map i Logout (02:53) [
Web Service		Information	Address Book	Settings	Security	Maintenance	XOA					
me						AccuRoute Config	uration					
Device Information												
				Model Name	CLX-8640							
	Status 🧯	SError		Host Name	<u>CLX-8640</u>							
Alert 2 Aler	2 Alert(s) Occurred		Serial Number	269981CD30000EX								
	c nicre()/ occurred		IPv4 Address	172.16.20.24								
				IPv6 Address	Not Configured							
=				MAC Address	00:15:99:c7:f0:e5							
_				Location	<u>QA Lab</u>							
				Administrator	beth							
					E-mail Not Configured							
					Phone Not Configured							
				Customer Support	Phone Not Configured							
Supplies Information					Phone Not Configured							
Toner Cartridge				Imaging Unit								
Cartridge	Remainii	ng	Status	Unit	Remaining	Status						
Black		100%	Ready	Black		100% Ready						

12 Select the XOA tab and on the left side of the screen open AccuRoute Configuration. The Configuration screen appears:

SyncThru™	SAMSUNG CLX-	8640		😔 admin 丨 Job Statu	us Direct Print Eco OFF	Ske Map Logout (02:59)	€English •
Web Service	6	Information	Address Book	Settings	Security	Maintenance	XOA
XOA	Configuration						
 AccuRoute Configuration 						Apply	Undo
Server							
	Server —						
	Server U	RL	Solar IDI ha Sama	with the port number. (eg) hit	to U1.0.0.090/DeviceClasti		
	Group Na	ame		min the part humber, (eg) in	(p.)] 10.0.0.00[Dendedient]		

- **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

I 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.

Status	/ncThru [™] b Service	SAMSUNG S							
Status Status Science			Information	Address Book	Maint	enance			
Status Open Alert LAberifsi Documed Marti LAberifsi Documed Marti LAberifsi Documed Status Open Alert LAberifsi Documed Status Open Internation Status Status Open Status Open Status Open Status Open Status Open Open Open Status Open Open Open Status Open Open Open Status Open Open Status	:								
Status Aret Host tamee 500/1992/788/7 Aret Likerifsi Docurred 104 Artifsi Ocurred 1074 Address 102 Initianational The Address 102 Initianational 100 Processor 104 Address 102 Processor Hitch Address 001 Stratas 001 Stratas 100 Processor 100 Processor Proce National Stratas Initianational Stratas 100 Processor 100 Processor Proce National Stratas Initianational Stratas 100 Processor 100 Processor Proce National Stratas Initianational Stratas 100 Processor 100 Processor									
Statis Server Alert 1.AdertiG.0.courred Prev Address 172,15,27 Prev Address 172,15,27 Prev Address 105,97,750,47 Castion 100,97,97,97 Castion 100,97,97,97 Castion 100,97,97,97 Castion 100,97,97,97	vice Information								
Statis Orient Alert 1.Alert(5) Occurred Hort 1.Alert(5) Occurred						Model Name	SCX-8128NX		
Status Serial Humber 2021002010 Alert 1 Alertifol Occurred Prive Address 172 185 327 Drivé Address 172 185 327 Prive Address 172 185 327 Drivé Address 172 185 327 Prive Address 172 185 327 Drivé Address 172 185 327 Prive Address 172 185 327 Drivé Address 172 185 327 Prive Address 172 185 327 Drivé Address 172 185 327 Prive Address 172 185 327 Drivé Address 172 185 327 Prive Address 172 185 327 Privé Address 172 185 327 Prive Address 172 185 327 Privé Address 172 185 327 Prive Address 172 185 327 Privé Address 172 185 327 Prive Address 172 185 327 Privé Address 182 180 200 100 100 100 100 100 100 100 100 10			Ac						
PrivA Address 1/2, 15, 3, 2/ HVA Address 1/2, 15, 3, 2/ HAC, Address 00:1596/204a7. HAC, Address 00:1596/204. HAC, Address 00:1	and a second		-			Serial Number	ZBJEB1AD100014D		
MAC Address 00:15%0:208a97 Location bits Configured Aministicator bits Configured E-call to: Configured		Alert	1 Alert(s) Occurred			IPv4 Address	172.16.5.27		
Location Mit Configured Administrator Hite Configured E-mail Not Configured E-mail Not Configured More Not Configured More Not Configured Texer Support Nore Not Configured	-					IPv6 Address	Not Configured		
Including Cardinal Status Including Cardinal Status						MAC Address	00:15:99:c7:b8:a7		
E-el Hot Configued E-el Hot Configued Castemer Support Prior Hot Configued Prior Hot Configued Tomer Not Configued Cartridge Temper Not Configued						Location	Not Configured		
Proce Nat Configured Castemer Support Proce Nat Configured Proce Nat Configured Proce Nat Configured Proce Nat Configured Imagine Date Cartridge Remaining Status Unit Status						Administrator			
Customer Support Prome Nat Configured Prome Nat Configured Tomer Contridge Cartridge Remaining Status Unit Remaining Status									
Pipeles Information Texer Cartridge Cartridge Remaining Status Unit Remaining Status									
Tonser Cartridge Imaging Unit Cartridge Remaining Status Unit Remaining Status						Customer Support	Phone Not Configured		
Cartridge Remaining Status Unit Remaining Status	plies Information								
	Toner Cartridge					Imaging Unit			
Black 100% Ready Black 99% Ready	Cartridge		Remaining		Status	Unit	Remaining	Status	
	Black			100%	Ready	Black		99% Ready	
Input Trays Output Trays	Input Trays					Output Trays			

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.

Section 7: Configuring Samsung Devices

6 Select Install new Root certificate and click Next.

 Install/Create New Certificate nstall Root Certificate tesult 	Install/Create New Certificate Install/Create Device Certificate or CSR © Create a Self-Signed Device Certificate © Install CA Signed Device Certificate © Create Certificate Signing Request (CSR)
	Install new Root Certificate Install New Root Certificate

7 Browse to the certificate file. Press Next.

Install/Create New Certificate ▶ Install Root Certificate	Certificate Information	
Result	Friendly Nam	ne:
	Root Certificate	
	File:	Select a file (File Format : ",pem,".cer,",der,",p12,",pfx)

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.

SyncThru™	SAMSUNG CLX-8640		dmin Job Status Direct Pi	int I Eco OFF I Site M	lap Logout (02:50)	€ English
Web Service	🗂 Information	Address Book	Settings	Security	Maintenance	e XOA
ecurity	Digital Certificate					0
Network Security						
Digital Certificate	 A digital certificate is an electronic creder prove a person's or device's identity and 	ntial that can help verify the secure co to provide the secure exchange of en	nnection between communi crypted information.	cation nodes. The mos	st common use of digita	al certificates is to
Secure Connection	Certificate Management					
SNMPv3						
IP Security	Selected : 0 Total : 1 (MAX : 4)					
IP/MAC Filtering	Add Delete Edi				▼Expand All	▶ Collapse All
IPv4 Filtering	Friendly Name	Туре	Used I	n	Valid Date	
IPv6 Filtering	fnccksam	Trusted Root Certificate	Not Use	ed.	21/05/2014 ~ 20/05	2015
MAC Filtering						
000.1.	11					

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

Configuring the device XOA to use SSL

- I 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:

SyncThru [™] Web Service	SAMSUNG ELX-8540	姭 admin Job Status Address Book	Direct Print Eco OF	F Site Map Logo Security	. ,	English tenance	хоа
XOA	Configuration						
 AccuRoute Configuration 					Apply	/ Undo	
Server							
	Server						
	Server URL		ain.com:443/DeviceClier with the port number.		DeviceClient/		
	Group Name		Samsung				

3 Enter the **Group Name** for the device and click **Apply**.

Configuring the AccuRoute Server Administrator to use SSL

- I 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:

Device Group Properties	x			
General Settings Authentication Buttons Advanced				
Application:				
URL:				
Type: Unified 💌				
Web API https://cck2012r2.knight08.com/WebAPI/Scripts/omisapiu.dl				
OPS Server: 172.16.20.171				
Timeout: C Automatically exit UI after 60 🛫 seconds of inactivity.				
O not exit UI Automatically				
OK Cancel				

5 Click **OK** to finish.

Section 7: Configuring Samsung Devices

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

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

Note Verify that <u>Section 3: Installation</u> 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	I	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. I 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	I	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	I	1.207.112
WorkCentre 73xx	WorkCentre 7335	I	ESS PS1.227.169, IOT 3.0.5, IIT 22.13.1, ADF 11.6.5, SJFI3.0.8, SSMI1.7.2

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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. I 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	I	ESS 0.040.022.50115, IOT 50.4.0, UI 0.12.60.12, BIOS 07.07

Table 8-1: List of supported Xerox devices

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:

Downloading the MakeCert executable (8-3)

Creating the certificate (8-3)

Installing the certificate to Internet Information Services (IIS) (8-3)

Creating an SSL binding (8-4)

Requiring SSL for the virtual web sites (8-4)

Enabling directory browsing is IIS (8-4)

Verifying the SSL binding (8-5)

Verifying HTTPS browsing (8-5)

Editing the OmISAPIU.xml file (8-5)

Editing the Bootstrap.xml file (8-6)

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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 <u>Microsoft</u> <u>documentation</u>.

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

Creating the certificate

- I 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.

- I 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? 8-3

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

Creating an SSL binding

- I 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

- I 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

- I 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

- I 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

- I 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).
- **II** Verify that the localhost page is displayed:

 $\dots \ WebAPI \$

Editing the OmISAPIU.xml file

I Navigate to the following path.

C:\Program Files (x86)\Omtool\Omtool Server\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>

Section 8: Configuring Xerox Devices

Note XML files can be edited using Microsoft Notepad.

3 Save the file.

Editing the Bootstrap.xml file

I 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.

Status Jobs Print Scan	Address Book Properties Support				
Properties Configuration Overview	LDAP Server				
Description General Setup	Server Contexts User Mappings Custom Filters				
+Connectivity	Server Information				
Physical Connections	Server Information				
*Protocols	IPv4 Address	Friendly Name			
AppleTalk	C IPV6 Address				
FTP / SFTP Filing					
HTTP	C Host Name	IP Address: Port			
IP (Internet Protocol)					
LDAP		0 . 0 . 0 . 0 . 389			
LPR/LPD					
Microsoft Networking NetWare		Backup IP Address : Port			
NTP		0 0 0 389			
Proxy Server					
Raw TCP/IP Printing					
SLP	LDAP Server				
SMB Filing					
SMTP (E-mail)	Exchange 💌				
SNMP					
SSDP	Optional Information				
WSD (Web Services on Device) Services					
Accounting	Search Directory Root				
Security					
rsecurity					
	Login Credentials to Access LDAP Server	Login Name			
	© None				
C Authenticated User		Password			
C System	C System	Passworu			
		Retype password			
		Select to save new password			

- 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	LDAP Referrals
C Use LDAP Server Maximum	Enabled
Maximum Number of Search Results	Perform Query on
25 (5 - 100)	Mapped Name Field
Search Timeout	C Surname and Given Name Fields
C Use LDAP Server Timeout	
6 Wait	
30 seconds (5 - 100)	
	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.

^{© 2017} by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

- XEROX ColorQube 8700S nternet Services atus Jobs Print Scan Address Book Properties Support Properties Xerox Access Setup Configuration Overview Description Authentication, Authorization, and Personalization General Setup Connectivity Physical Connections Protocols Authentication method on the machine's touch user interface (Touch UI): AppleTalk FTP / SFTP Filing User Name / Password Validated Remotely on the Network HTTP IP (Internet Protocol) LDAP LPR/LPD Microsoft Networking Authentication method on the machine's web user interface (Web UI): NetWare User Name / Password Validated Remotely on the Network Proxy Server Raw TCP/IP Printing SLP Authorization information is stored: SMB Filing Locally on the Xerox Machine (Internal Database) SMTP (E-mail) SNMP SSDP WSD (Web Services on Device) Services Personalize settings on the machine's touch user interface: Accounting Enabled: Automatically Retrieve Information for the Authenticated User Setup Security Admin Password Secure Print Authentication Authentication
 Setup
 User Permissions
 Job Override Policies
 Troubleshooting
 User Information Database Configuration Setting Method (Defined Above) Required / Optional Required; Col Authentication Servers Authentication (Touch UI & Web UI) Required; Co Machine's User Information Database Authorization Encryption ▶Certificates 🕜 Optional; Con Tools and Feature Access (Lock / Unlock) Authorization IP Filtering Audit Log Audit Log IPsec 802.1X System Timeout USB Port Security Image Overwrite Required; Con LDAP Servers Personalization Optional; Con Service Registration (Convenience Link)
- k In the left menu under Security > Authentication, select Setup to display the Authentication, Authorization, and Personalization settings.

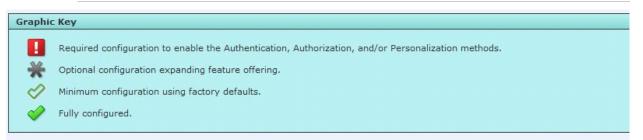
- I Click the Authentication Method on the machine's touch user interface (Touch UI) option. Then, click the Edit button.
- m From the drop-down, select User Name / Password Validated Remotely on the Network option.



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.



• 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.

nternet Services	XEROX ColorQube 8700S			A admin - Logout nome 180EX Site hap neip
Status Jobs Print Scan	Address Book Properties Support			
Properties Configuration Overview Description General Setup Connectivity Physical Connections	Authentication & Authorization Setup LDAP Servers Authentication Type]
Protocols AppleTalik FTP / SFTP Filing HTTP IP (Internet Protocol) LDAP	LDAP			
LPR/LPD Microsoft Networking NetWare NTP Proxy Server	Add New Copy From_ Delete All			LDAP Policies
Raw TCP/IP Printing	LDAP Friendly Name VMELAD1	IP Address 172.16.20.70:389	Search Directory Root DC=VMELAD1.DC=COM	Actions
SLP SMB Filing SMTP (E-mail) SNMP SSDP		172.16.20.70:365	DC-VHEDDT;DC-COM	Ciose
WSD (Web Services on Device)	Note			
Services Accounting Setup Security Admin Password Secure Print	Icon indicates what LDAP Server will be used w - Users complete queries to the Network Addre - Authentication method is set to LDAP - Remote authorization / personalization when i	ss Book from scan services		
 Authentication Setup User Permissions Job Override Policies Troubleshooting 			xerox 🌍	
User Information Database Encryption Certificates ID Elitering			©1997 - 2012 Xerox Corporation. All Rights Reserved. Xerox® and XEROX and Design® are trademarks of xx Corporation in the United States and / or other countries.	

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	
O 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	
Custom	

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

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	8	Not Allowed	•
	Omtool.GroupED2		Allowed	•
	Omtool.MyAccuRoute3	8	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:

<u>Supported Devices</u> (9-1) <u>Exporting the XML files</u> (9-2) <u>Manually importing a certificate</u> (9-3) <u>Installing AccuRoute Embedded Device Client buttons</u> (9-4)

Supported Devices

The following devices are supported:

Table 9-1: AccuRoute Embedded Device Series Matrix

 Color Las
1
ScanJet 70
ScanJet 8
LaserJet F
LaserJet F
LaserJet N
LaserJet N
HP Color
HP Color
HP LaserJ
HP X585
HP M680

Device	Operating System
Color LaserJet CM 4540 MFP	FutureSmart
ScanJet 7000n	FutureSmart
ScanJet 8500	FutureSmart
LaserJet Flow M525 MXP	FutureSmart
LaserJet Flow M575 MXP	FutureSmart
LaserJet M775 MFP	FutureSmart
LaserJet M4555 MFP	FutureSmart
HP Color LaserJet Flow M880	FutureSmart
HP Color LaserJet Flow M830	FutureSmart
HP LaserJet MFP M725	FutureSmart
HP X585 MFP group	FutureSmart
HP M680 MFP group	FutureSmart

^{© 2017} by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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.

- I Once the configuration is complete (as described in <u>Installation</u>, <u>Creating Device Groups on the</u> <u>AccuRoute Server Administrator</u> and <u>Installing Buttons on a New Device</u>), 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:

select fol	r Folder der to store We	b Jet Admi	n export	×
Des	sktop			
🕀 🥽 Li	ibraries			
🕀 🚺 🕂	dministrator			
🕀 🌉 C	Computer			
🕀 🙀 N	létwork			
📔 🔒 F	ax_output			
Folder:	Administrato	r		
Males MI	ew Folder	0		Cancel

Make New Folder:

×

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

anize 🔻 Include in	n library 🔻 Share with 🔻 New folder			
Favorites	Name *	Date modified	Туре	Size
📃 Desktop	🔮 FutureSmart-Fax	9/13/2012 7:12 PM	XML Document	6 KB
\rm Downloads	FutureSmart-HP Capture and Route	9/13/2012 7:12 PM	XML Document	4 KB
🔛 Recent Places	FutureSmart-Personal Distributions	9/13/2012 7:12 PM	XML Document	7 KB
Libraries	FutureSmart-Public Distributions	9/13/2012 7:12 PM	XML Document	7 KB
Documents	FutureSmart-Routing Sheet	9/13/2012 7:12 PM	XML Document	6 KB
J Music	🖻 FutureSmart-Scan To Me	9/13/2012 7:12 PM	XML Document	6 KB
Nictures	FutureSmart-Scan To My Files	9/13/2012 7:12 PM	XML Document	7 KB
📑 Videos				

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:

- I 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.

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

The **Specify group options** page appears.

Create Group			2 3
pecify gro	up options		
Group identific	ation		
Group name:	02		
Parent group:	Groups		
Group member	ship type		
C Automatic	are added or removed b group	y the user) I or removed based on filter criteria)	
Configure gr	oup properties now		
			Next> Cancel

2 Enter the name of the new group that you will use to group similar devices for 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.

Create Group Confirm				?
Settings		 		
Group name:	Oz			
Parent group:	<no parent=""></no>			
Description:	<not specified=""></not>			
Contact:	<not specified=""></not>			
Membership type:	Manual (0 devices)			
Policies:	0			
		< Back	Create Group	Cancel

- 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.

Available devices Source: All Devices				Devices to add Number of devices: 0		
Device Model	IP Hostname	IP/		Device Model	IP Hostname	IF
HP LaserJet M3035 MFP	NPID1240D	<ni< td=""><td></td><td></td><td></td><td>-</td></ni<>				-
Canon iR-ADV 6065 40.13	CANON4F5598	172				
HP Color LaserJet CM2320bi M	_ NPI82A248	172				
IP LaserJet 4345 MFP	NPID6AD7F	172				
P Color LasesJet CM4540 MFP	NP148C028	172	>			
IP Officejet Pro X451 dn Series	HPF2A85C	172	>>	1		
HP LasesJet M4555 MFP	NPIB4A104	172				
			c			
		10	-44			
d				4		10

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

Available devices				Devices to add		
ource: All Devices				Number of devices: 1		
Device Model	IP Hostname	IP A		Device Model	IP Hostname	1
IP LaserJet M3035 MFP	NPID1240D	<ni< td=""><td></td><td>HP LaserJet 4345 MFP</td><td>NPID6AD7F</td><td>1</td></ni<>		HP LaserJet 4345 MFP	NPID6AD7F	1
anon iR-ADV 6065 40.13	CANON4F5598	172				
IP Color LaserJet CM2320fxi M	NPI82A248	172				
IP Color LaserJet CM4540 MFP	NPI48C028	172				
IP Officejet Pro X451dn Series	HPF2A85C	172				
			>			
IP LaserJet M4555 MFP	NPIB4A104	172	> >>			
HP LaserJet M4555 MFP	NPIB4A104					
HP LaserJet M4555 MFP	NPIB4A104					
HP LaserJet M4555 MFP	NPIB4A104					
IP LaserJet M4555 MFP	NPIB4A104		>>>			
IP LaserJet M4555 MFP	NPIB4A104		»>			
IP LaserJet M4555 MFP	NPIB4A104		»>			
IP LaserJet M4555 MFP	NPIB4A104		»>			
IP LaserJet M4555 MFP	NPIB4A104		»>			
IP LaserJet M4555 MFP	NPIB4A104		»>			
IP LaserJet M4555 MFP	NPIB4A104		»>			

7 Click Next. The Confirm page appears.

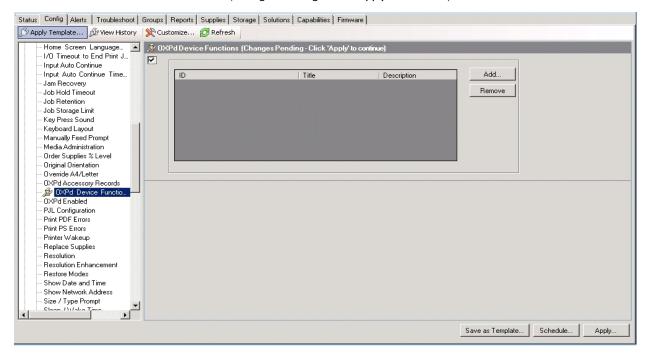
d Devices			
nfirm			
ettings oup name: OZ evices:			
Device Model	IP Hostname	IP Address	
HP LaserJet 4345 MFP	NPID6AD7F	172.16.5.131	

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

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

🛣 O.	Z (1 of 3 Selected)							
ä		🖌 Filters 🔹 🚺	🖉 📾 🖬 🗟					
C	evice Model	IP Address	IP Hostname	Port (Any)	Severity	Hardware Address		
18 H	P LaserJet M4345 MFP	172.16.5.208	NPI822592	1	0	001708822592		
	P Color LaserJet 4730 MFP	172.16.5.130	NPI5BDA67	1		0014385BDA67		
*) H	P Color LaserJet CM6040 MFP	172.16.5.117	NPI1CB481	1		001B781CB481		
	Config Alerts Troubleshoot			e Solutions Ca	pabilities Firm	ware		
De De	Settings	Alternative Let	terhead Mode					-
	Alternative Letterhead Mo	C On						
	- Asset Number	○ Off						
	Auto Cleaning Page	Asset Number						
	- Auto Continue - Browser	[Not speci	fied)					
	- Clearable Warnings	Interspec	neuj					
	- Company Name 📃 📃	Auto Cleaning	Page					
	Contact Person		ning frequency: 2	000	-			
	- Control Panel Display - Control Panel Language							
	-Date and Time	Cleaning p	age size:	.etter (8.5x11 in)	-			
	Date/Time Format	Auto Continue						
	Daylight Savings Time	and the second se						
	Default Media Size	□ ⊙ On						
	- Default Media Type - Default Print Density	O Off						
	- Default Printer Copies	Browser						
	Device Certificates							
	Device Location		ction timeout:	60 🔻 sec	onds			
	Device Name	-						
	- Duplex Binding - Duplex Blank Pages	Hespo	nse timeout:	300 💌 sea	conds			
	- Duplex Inpressions	Truste	d sites:					

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).



© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

II Click the Add button. The Add Embedded Device Functions page appears.

Status Config Alerts Troubleshoot (Groups Reports Supplies	Storage Solutions Capabilities Fir	rmware	
🕉 Apply Template 🕼 View History	💥 Customize 💋 Refre	esh		
Home Screen Language I/O Timeout to End Print J Input Auto Continue Input Auto Continue Time	ØXPd Device Functi ▼	ions (Changes Pending - Click 'Appl		Add
- Job Hold Timeout			Description	Remove
Job Storage Limit Key Press Sound Keyboard Layout	Add OXPd Device	e Function s		? ×
Manually Feed Prompt Media Administration	ID	Title	Description	Edit
Order Supplies % Level Original Orientation Override A4/Letter				
OXPd Accessory Records Source Functio OXPd Device Functio OXPd Enabled				
PJL Configuration Print PDF Errors Print PS Errors		_	_	
Printer Wakeup Replace Supplies Besolution			ОК	Cancel
Resolution Enhancement Restore Modes				

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).

Status Config Alerts Troublesh	hoot Groups Reports Supplies Storag	ge Solutions Capabi	ilities Firmware	•	
🗳 Apply Template 🍿 View His	story 🛛 👷 Customize 🔁 Refresh				
Home Screen Language	🔄 🏂 OXPd Device Functions (Cl	anges Pending - Cli	ek 'Applu' to e	ontinue)	
- I/O Timeout to End Print J		langes i enang-ci	ck Abbia ac		
- Input Auto Continue					
- Input Auto Continue Time.	ID	Title		Description	Add
Jam Recovery					Remove
Job Hold Timeout					
Job Retention	🚽 Add OXPd Device Functi	ions			? ×
Key Press Sound					
- Keyboard Layout					
Manually Feed Prompt	ID	Tit	le	Description	E dit
- Media Administration					
- Order Supplies % Level					
- Original Orientation	Ø Options				? ×
- Override A4/Letter - OXPd Accessory Record					
- DXPd Accessoly Recon	- Templates	COXPd Device Funct	tion Repository		
- OXPd Enabled	User Defined	Name.	Title	Description	Import
- PJL Configuration	PJL Repository Certificate Repository				
- Print PDF Errors	OXPd Device Functio				Delete
- Print PS Errors					Edit
Printer Wakeup					
	⊕ · Firmware				
- Resolution Enhancemer	E- Reports				
- Restore Modes	⊞- Supplies				
- Show Date and Time					
- Show Network Address					
- Size / Type Prompt					
Sloop //u/ako Timo					
<u></u>					
	-				
	Reset Page			OK	Cancel Apply

×

0

- 13 Click Import. In the Open page, search for your XML files. Device Model IP Address IP Hostname Port (Any) Severity Hardware Address 172.16.5.208 0 HP Color LaserJet 4730 MFF 172.16.5.130 NPI5BDA6 0014385BDA6 HP Color LaserJet 4730 MFP
 HP Color LaserJet CM6040 MFP 172 16 5 117 NPI1CB481 1 001B781CB481 🖪 Options ? × OXPd Device Function Repository Templates -User Defined Import. Title Description Name Status Config Ale Alerts
 Firmware
 Reports
 Supplies 🗇 Apply Template. Home Scre I/O Timeou Input Auto (Input Auto Jam Recov Job Hold Ti Job Betenti × Job Storag d Open 😋 🔵 - HP • WEBJETADMIN • WebJet_admin_HPCR • WebJetAdmin_XML_OZ Search WebJetAdmin_XML_OZ New folder = - 🔟 📀 Organize 🔻 Name Date modified Туре Size 👉 Favorites 🧾 Desktop 🕋 Fax 4/2/2012 2:46 PM XML Document 3 КВ 鷆 Downloads MvAccuRoute original 3/19/2012 10:23 AM зкв XML Document 🔚 Recent Places PersonalDistribution 4/2/2012 2:44 PM XML Document з кв PublicDistribution 4/2/2012 2:45 PM XML Document зкв 🔚 Libraries 🔮 RoutingSheet 4/2/2012 2:45 PM XML Document 5 KB Documents 🖭 ScanToMe 4/2/2012 2:46 PM J Music XML Document 3 КВ E Pictures Videos 💻 Computer 4 🙀 Network
 - 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.

-1	Options					?
	Templates		DXPd Device Funct	ion Repository		
	User Defined		Name 🗸	Title	Description	Import
	PJL Repository Certificate Repository		Fax Button	Fax	Send a Fax	Delete
	OXPd Device Functio					
tatus Config Ale	OXPd Accessory Rec.					E dit
Apply Template.	⊕- Alerts ⊕- Firmware					
	Reports					
— Home Scre — I/O Timeou	😟 Supplies					
- Input Auto (
- Input Auto						
- Jam Recov						
Job Hold Ti Job Retenti						
Job Storage						
Key Press S						
- Keyboard L						
Manually Fe Media Admi	I I I	_ ا لے				
- Order Supp	<u>↓</u>					
Original Orie	Reset Page				ок	Cancel Apply
- Override A4						

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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

Status	Config	Alerts	Troubleshoo	ot Gro	oups	Reports	Supplies	Storage	Solutions	Capabilities	Firmware			
🖉 App	oly Templ	late j	🕼 View Histor	ry 🖇	Cus	tomize	🔁 Refre	sh						
	1/0 Tim		End Print J	▲ 5		PdDevi	ce Functio	ons (Chai	nges Pendi	ng-Click 'A	pply' to con	tinue)		
	Input A Jam Re Job Hol Job Rel Job Sto Key Pre Keyboa Manual	uto Con covery ld Timeou tention rage Lim css Soun rd Layou ly Feed F	itinue Time ut it d Prompt			ID				Title		Description		Add Remove
	Order S Original	Administra upplies % Orientati e A4/Let	‰Level ion		A A	dd OXPc	Device F	unctions						? ×
	OXPd A OXPd E OXPd E Pll Cor Print PC Print PS Printer V Replace Resolut Resolut Resolut	Accessor, Pd Devi Enabled Infiguratic DF Errors Errors Wakeup e Supplie ion Enha	y Records ce Functio n n ss ancement			ID 23920	c5c-f3dd-4	42f-a56f-09	335deb09e	Title Fax		Description Send a Fax		E dit
	Show N Size / T) ate and letwork / jype Prop	Address mpt	.]	OK	Cancel

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).

Home Screen Language. ▲ HO Timeout to End Print J Input Auto Continue Time. Imput Auto Continue Time. Job Hold Timeout Job Hold Timeout Job Hold Timeout Add Removesy Second 442(+a56):0035deb03e Fax Send a Fax Remove Remove Up Traine Sound Fax Keyboard Layout Fax Media Administration Porende Addministration Orende Addministration Print PO Accessory Records Ør Prid Dexides Function Print PO E times Print PO E times Printer Wakeup Resolution Enhancement Resolution Enhancement Resolution Enhancement Resolution Enhancement Resolution Enhancement Pristore Modes Show Deleva and Time Fore Addministration	Status Config Alerts Troublesh	ory	📌 Cus	tomize 💋 Refres	h				
Replace Supplies Resolution Resolution Enhancement Restore Modes Show Date and Time Show Network Address Size / Type Prompt	Home Screen Language I/O Timeout to End Print J. Input Auto Continue Input Auto Continue Jan Recovery Job Hold Timeout Job Storage Limit Key Press Sound Keyboard Layout Manually Feed Prompt Media Administration Order Supplies % Level Original Orientation Override A4/Letter OXPd Device Functio OXPd Device Functio OXPd Enabled Pill Configuration Print PDF Errors Pint PD Errors	-	<i>⊉</i> 0X	Pd Device Functio	ns (Changes Pendi	Title	D		
Restore Modes Show Date and Time Show Network Address Size / Type Prompt	Replace Supplies Resolution								
Show Network Address									
- Size / Type Prompt									
	Sleep //u/aka Tima	-							

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

Configure Devices	2 ?
Confirm	J.
Settings	
Devices: 1	
Device settings:	
Item	Value
🔍 OXPd Device Functions	0
	< Back. Configure Devices Cancel

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

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

Configure Devices			? :
rogress			S
<u> </u>			
🕢 In Progress	•		
Summary			
Success:	0		
🔒 Warning:	0		
🖸 Error:	0		
 Information needed: 	0		
Pending:	1		
Pending:	1		

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

Success may Success: 1 Warning: 0 Error: 0			?
Imany Success: 1 Warning: 0 Error: 0 Information needed: 0	esults		E.
Imany Success: 1 Warning: 0 Error: 0 Information needed: 0	<u> </u>		
Success: 1 Warning: 0 Error: 0 Information needed: 0	🕗 Success		
Warning: 0 Error: 0 Information needed: 0	Summary		
Error: 0 Information needed: 0	Success:	1	
Information needed: 0	🚹 Warning:	0	
	🕃 Error:	0	
Pending: 0	Information needed:	0	
	🔀 Pending:	0	

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

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

CZ (1 of 3 Selected)							
🐱 🗌 Layouts 👻	🍸 Filters 🔹 🚺	2 a a a					
Device Model	IP Address	IP Hostname	Port (Any)	Severity	Hardware Address		
📰 HP LaserJet M4345 MFP	172.16.5.208	NPI822592	1	0	001708822592		
HP Color LaserJet 4730 MFP	172.16.5.130	NPI5BDA67	1	A	0014385BDA67		
HP Color LaserJet CM6040 MFP	172.16.5.117	NPI1CB481	1	Ā	001B781CB481		
Status Config Alerts Troubleshoot	Groups Reports	Supplies Storage	e Solutions Ca	apabilities Firm	ware		
🗇 Apply Template 🕼 View History	🛛 🎇 Customize	🔁 Refresh					
⊕-My Settings	Alternative Let	terhead Mode					
Device							
Alternative Letterhead Mo							
Asset Number	@ Off						
- Auto Cleaning Page	Asset Number						
Auto Continue							
Browser	Not speci	ified)					
Clearable Warnings							
- Company Name -	Auto Cleaning	Page					
- Contact Person	Auto clear	ning frequency: 2	000	-			
Control Panel Display Control Panel Language							
- Date and Time	Cleaning p	bage size:	etter (8.5x11 in)	-			
Date/Time Format							
- Daylight Savings Time	Auto Continue						
- Default Media Size	🗖 🔍 On						
Default Media Type	C Off						
Default Print Density							
Default Printer Copies	Browser						
- Device Certificates	Г						
- Device Location		ection timeout:	60 🔻 se	conds			
- Device Name	-						
Duplex Binding Duplex Blank Pages	Hespo	onse timeout:	300 ▼ se	conds			
- Duplex biarik Pages	Truste	d sites:					
- Economode		d onoo.					
- Fuser Modes							
- Home Screen Applications							
- Home Screen Language							
		Use semio	colons(;) to separa	ate addresses			

- 07 /4 - F2 C

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

OVD4 Excelled		Capabilities Firmware	_	_	_	
OVA Challenge Over Challenge Over Challenge Print PDF Errors Print PS Errors Print PS Errors Printer Wakeup Resolution Resolution Enhancement Resolution Enhancement Resolution Show Network Address Show Date and Time Show Nate work Address Size / Type Prompt Size / Type Prompt Size / Wake Time	ID 23920c5c-13dd-4421-a56i-0935deb09e 4cbfa532-6be8-4877-8917-2tbfa836df2a		Description Send a Fax Distribute document using	Add Remove		
 Stored Job Sort Order Supplies Status Message Suppress Blank Pages Time Zone Tray Administration Use Another Tray Use Requested Tray Copier Network Security Frax Embedded Web Server File System Digital Sending 						
				Save as Template	Schedule	Apply

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

Section 10: Testing

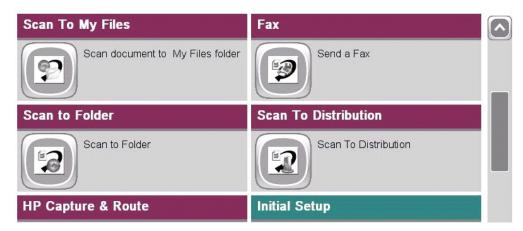
The following section provides a procedure for testing the Routing Sheet feature and the Device Administrator user interface. This will ensure that your installation is operational. This section includes:

Testing the Routing Sheet feature (10-1)

Testing the Device Administrator user interface (10-2)

Testing the Routing Sheet feature

- I 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 <u>Section 11: Troubleshooting</u>.

- 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 [6] 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 <u>Troubleshooting issues when the AccuRoute server cannot</u> 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

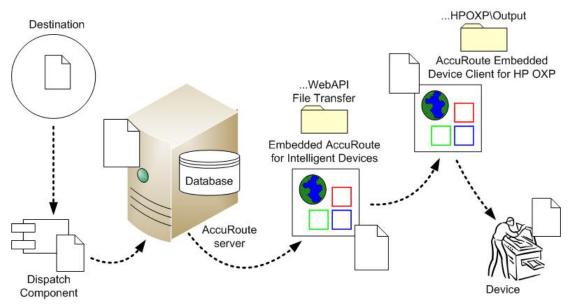
This section includes:

Detecting workflow issues (11-2) Troubleshooting the delivery mechanism (11-2) Troubleshooting messages on the AccuRoute server (11-3) Troubleshooting the Web server (11-5) Troubleshooting the multifunction device (11-5) Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd (11-5) Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster (11-6) Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet (11-6) Troubleshooting problems associated with applying all additional scan attributes (11-7) Troubleshooting problems when scanning large documents (11-7) Troubleshooting problems when scanning 100+ color pages (11-8) Troubleshooting an SNMP error (11-9)

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.

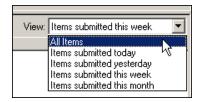
Troubleshooting messages on the AccuRoute server

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:

- I 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.



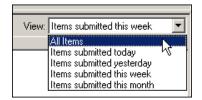
- c Sort all items by the date submitted.
- **d** Look for the message.
- Message found View the message journal to determine the current state and status of the message. Then monitor the components and confirm that the message is moving through the processing queues on the AccuRoute server. If the AccuRoute server stops processing the message (for example, the message seems to be stuck in a processing queue), restart all the Omtool services.

Recipient Properties					
ſ	General Attachments Re	cipient Sender Confirmations Journal			
ľ	Date	Journal Entry			
	10/05/2005 09:32:57 AM	Dispatch: Fax number normalized to +16038901			
	10/05/2005 09:32:57 AM 10/05/2005 09:32:57 AM	Dispatch: Matched rule All fax numbers to Telco Dispatch: Processing action for rule "All fax num			
	10/05/2005 09:32:58 AM	Compose: Started			
	10/05/2005 09:32:58 AM	Compose: (localhost - localhost) Document=cert			

• Message not found - Go to step 4 and look for the message in the History queue.

11-3

- 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.

Recipient Properties X					
General Attachments Recipient Sender Confirmations Journal					
	Date	Journal Entry			
	10/05/2005 09:32:57 AM	Dispatch: Fax number normalized to +16038901			
	10/05/2005 09:32:57 AM	Dispatch: Matched rule All fax numbers to Telco			
	10/05/2005 09:32:57 AM	Dispatch: Processing action for rule "All fax num			
	10/05/2005 09:32:58 AM	Compose: Started			
	10/05/2005 09:32:58 AM	Compose: (localhost - localhost) Document=cert			
	10/05/2005 09:33:07 AM	Compose: (localhost - localhost) Document=400			
	10/05/2005 09:33:20 AM	Compose: Completed			
	10/05/2005 09:33:21 AM	OmtoolConnector: Destination connector failed t			
	10/05/2005 09:33:22 AM	Dispatch: Fax number normalized to +16038901			
	10/05/2005 09:33:22 AM	Dispatch: Routing complete			

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 <u>AccuRoute v4.0 documentation page</u>.

If you cannot identify any issues with the Web server, troubleshoot the device. Continue to <u>Troubleshooting the</u> <u>multifunction device</u>.

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 vI.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 v3.5.1 before 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-spl-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 <u>AccuRoute v4.0 Server Installation Guide</u>.

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:

- I 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:

- I 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:

- I 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.

11-7

- 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.

- I 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.

- I 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.

- I 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.

Section 11: Troubleshooting

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.